

Tanium™ Threat Response User Guide

Autonomous IT. Unstoppable Business.

2025H2 Semiannual Release

Version 4.12

May 26, 2026

The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://help.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and services provided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved *supports* or *partially supports* for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.

Patents: https://www.tanium.com/patents

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2025 Tanium Inc. All Rights Reserved

© 2025 Tanium Inc. All rights reserved.

Table of contents

Threat Response overview **18**

Investigation 18

Detection 18

Containment 18

Tanium Autonomous IT Platform in Threat Response 18

Supported languages 18

Interoperability with other Tanium products 19

Tanium Connect 19

Tanium Data Service 19

Tanium Enforce 20

Tanium Impact 20

Tanium Investigate 20

Tanium Trends 20

Threat Response - Alerts 20

Threat Response - Stream STATS 20

Gaining organizational effectiveness with Threat Response **22**

Change management 22

RACI chart 22

Organizational alignment 30

Operational metrics 30

Threat Response maturity 30

Benchmark metrics 31

Threat Response requirements **35**

Core platform dependencies 35

Computer group dependencies 35

Solution dependencies 36

Tanium recommended installation 36

© 2025 Tanium Inc. All Rights Reserved

Import specific solutions ... 36
Required dependencies ... 36
Feature-specific dependencies ... 37
Client extensions and endpoint tools ... 37
Tanium™ Module Server ... 37
Endpoints ... 37
Disk space requirements ... 39
CPU and memory requirements ... 40
Tanium Driver ... 40
Host and network security requirements ... 40
Ports ... 40
Security exclusions ... 43
User role requirements ... 140
Installing Threat Response ... 153
Before you begin ... 153
Import Threat Response with default settings ... 153
Import Threat Response with custom settings ... 154
Manage solution dependencies ... 154
Upgrade the Threat Response version ... 154
Verify Threat Response version ... 155
Configuring Threat Response ... 156
Install and configure Tanium Endpoint Configuration ... 156
Manage solution configurations with Tanium Endpoint Configuration ... 156
Configure Threat Response ... 157
Configure the Threat Response action group ... 157
Set up Threat Response users ... 158
Select a language ... 160
Getting started with Tanium™ Threat Response ... 161
Evidence and telemetry ... 161
Profiles ... 162

© 2025 Tanium Inc. All Rights Reserved

Live Response 163
Alerting and detection 164
Extended detections 164
3rd party intel feeds 165
Endpoint isolation 165
Tanium default quarantine profile 165
Create quarantine profile 166
Incident response automation 166
Tanium default alert reactions 166
Endpoint reactions 166
Automate playbooks 166
SIEM integration 167
Send stream data to SIEM 167
Send alerts to SIEM 167
Send Audit Logs to SIEM 167
Adding intel 168
Signals 168
Signals do not always evaluate with the recorder database 169
Intel safeguards 169
Configure intel sources 171
Connect to the Tanium Signals feed 171
Configuring Tanium Signals feed in an airgapped environment 173
Connect to iSIGHT Partners ThreatScape 173
Connect to a TAXII server 175
Set up Connect and Wildfire 177
Use a local directory or remote share 177
Delete an intel source 179
Configure process injection 179
Reputation data 181
Configure reputation data in Tanium Connect 181

© 2025 Tanium Inc. All Rights Reserved

Add Signals ... 182
Import and export Signals ... 183
Export Signals ... 184
Import Signals ... 184
Upload intel documents ... 185
Create intel documents ... 185
Create IOCs ... 186
Label intel ... 187
Apply a label ... 187
Manage existing labels ... 187
Configure YARA files ... 188
View orphaned intel documents ... 188
Assign a reaction to an intel document ... 188
Testing Intel for deployment ... 189
Creating reactions ... 190
Overview ... 190
Create a reaction ... 190
Assign a reaction to an intel document ... 192
Reaction statuses ... 193
Audit reaction data ... 194
Analyzing context ... 195
Overview ... 195
Examples ... 195
Analyze the context of artifacts ... 196
Export Context Analyzer results ... 197
Scanning endpoints ... 198
Background scans ... 198
On-demand scans ... 198
Creating configurations in Threat Response ... 201
Overview ... 201

© 2025 Tanium Inc. All Rights Reserved

Create detection configurations ... 201
Create index configurations ... 202
Create indexing exclusions ... 204
Create recorder configurations ... 204
Create stream configurations ... 207
Create filters ... 210
Import and export configurations and filters ... 229
Export configurations ... 229
Export filters ... 229
Import configurations ... 230
Import filters ... 230
Creating profiles in Threat Response ... 231
Overview ... 231
Tanium Managed profiles ... 231
Create a profile ... 232
Prioritize profiles ... 234
Deploy a profile ... 234
Deploy intel ... 235
Configure the intel deployment setting ... 235
Immediately deploy intel to endpoints ... 236
Direct connecting to endpoints and exploring data ... 237
Direct connect to an endpoint ... 237
Add to investigation ... 238
Capture a snapshot ... 238
Close the connection ... 239
Browse the file system on connected endpoints ... 239
Search for events ... 239
Manage snapshots ... 242
Export a snapshot from an endpoint ... 242
Download a snapshot ... 242

© 2025 Tanium Inc. All Rights Reserved

Upload a snapshot ... 242
Save files and events ... 243
Download a file ... 244
Create Enforce rules ... 244
Export events ... 245
Manage IOCs ... 245
Generate an IOC ... 245
Searching across the enterprise ... 246
Hunt across the enterprise ... 246
Enterprise hunting questions ... 247
Account Lockouts Security Event Log Search ... 250
AutoRun Files ... 250
AutoRun Program Details ... 251
Autoruns by Category ... 251
Certificate Search ... 252
Cleared Windows Security Event Log Search ... 252
Command Line of Process ... 252
Command Line with Hash Match ... 253
DLL Load Order Hijacking Search ... 253
Driver Details with Hash ... 253
Environment Variables ... 254
Established Connections with Hash ... 254
Explicit Logon Security Event Log Search ... 254
File Certificate Details ... 255
File Handle Details ... 256
File Handles Of Process ... 256
Has Incident Response ID Files ... 257
Has Scheduled Task ... 257
Hash Of File ... 257
Hosted Services Name Audit ... 258

© 2025 Tanium Inc. All Rights Reserved

iCloud Settings ... 258
Injected Threads ... 258
Is File Digitally Signed ... 259
Linux AutoRuns ... 259
Listen Ports with Hash ... 260
Loaded Modules Not Matching Whitelist ... 260
Loaded Modules Of Process ... 260
Loaded Modules with Hash ... 261
Logon Security Event Log Search ... 261
Mac AutoRuns ... 262
Mac Downloaded Files ... 262
Mac Firewall Settings ... 262
Mac Gatekeeper Settings ... 263
Mac Kext Details ... 263
MD5 Hash Of File ... 263
MD5 Hash Match Files Executing ... 264
MD5 Hash Single File Match ... 264
Mutex Details ... 264
Mutex Handles Of Process ... 265
Network Details ... 265
Non-Approved Established Connections with Hash ... 266
Original Filename ... 266
PowerForensics File Record ... 267
PowerForensics Master Boot Record ... 267
PowerForensics Prefetch ... 267
PowerForensics Recently Opened Office Files by User ... 268
PowerForensics Shim Cache ... 268
Process Details ... 268
Processes Using Module ... 269
RDP Client History ... 269

© 2025 Tanium Inc. All Rights Reserved

Remote Desktop Event Log Search ... 270
Run Command History ... 270
Running Processes With Filename Mismatch ... 270
Running Processes with Hash ... 271
Running Processes with MD5 Hash ... 271
Scheduled Tasks ... 271
Semaphore Details ... 271
Service Module Details ... 272
Service Module Details with Hash ... 272
Service Process Details ... 272
Service Status with Hash ... 273
Service System Event Log Search ... 273
SHA1 Hash Match Files Executing ... 274
SHA1 Hash Single File Match ... 274
SHA1 Hash Of File ... 274
Shell History ... 275
SIP Settings ... 275
SSH Known Hosts ... 275
Trace DNS Queries ... 276
Trace Executed Process Hashes ... 277
Trace Executed Process Trees ... 277
Trace Executed Processes ... 278
Trace File Operations ... 280
Trace Image Loads ... 282
Trace Loaded Drivers ... 283
Trace Logon Events ... 284
Trace Network Connections ... 285
Trace Registry Keys or Values ... 286
Windows Audit Policy ... 288
Windows Credential Security Settings ... 288

© 2025 Tanium Inc. All Rights Reserved

WMI Event Consumers ... 288
Managing Threat Response alerts ... 289
View alerts ... 289
Decode encoded text ... 290
Assign a status to an alert ... 290
View alerts by intel document ... 291
Microsoft Defender alerts ... 291
Deep Instinct alerts ... 292
Investigate reputation data ... 293
Investigate alerts ... 293
Add alerts to an investigation in Tanium Investigate ... 294
Deploy an action to an endpoint ... 294
Initiate a Response Action from an alert ... 295
Remediate alerts in Tanium Enforce ... 295
Export alerts ... 297
Delete alerts ... 298
Suppress alerts ... 298
Suppress an alert ... 299
Edit and delete suppression rules ... 300
View the status of a retroactive task ... 300
Import and export suppression rules ... 300
Export specific suppression rules ... 300
Export all suppression rules ... 300
Import suppression rules ... 300
Manage the impact of lateral movement with Tanium Impact ... 301
Set up Tanium Connect forwarding ... 301
Managing response activity ... 303
Create a response action for an endpoint ... 303
Response Action: Download File ... 303
Response Action: Gather Snapshot ... 304

© 2025 Tanium Inc. All Rights Reserved

Response Action: Live Response ... 304
Response Action: Quarantine ... 306
Response Action: Unquarantine ... 306
Stop a response action ... 306
Collecting data from endpoints with Live Response ... 307
Destinations ... 307
Destination types ... 308
Azure Destinations ... 308
S3 Destinations ... 309
SSH Destinations ... 310
SMB Destinations ... 311
Generate known_hosts and test connections ... 312
Collections ... 313
File Collector sets ... 314
Script sets ... 327
Collect data from endpoints ... 327
Collect logs ... 328
Regular expressions and environment variables ... 328
Quarantining endpoints ... 331
Before you begin ... 333
Endpoint operating system requirements ... 334
Supported Windows versions ... 334
Supported Linux OS versions ... 335
Supported macOS versions ... 335
Create quarantine rules ... 336
Create a quarantine profile ... 336
Delete a profile ... 343
Duplicate a profile ... 343
Edit a profile ... 343
Export a profile ... 343

© 2025 Tanium Inc. All Rights Reserved

Export all profiles ... 343
Import a profile ... 343
Generate Quarantine Packages ... 344
Check that the IPsec Policy Agent service is running on the endpoints ... 344
Verify that endpoints are not using Network Manager ... 345
Test quarantine on endpoints ... 345
View quarantined endpoints ... 347
Remove endpoints from quarantine ... 347
Reference: Create custom quarantine rules ... 347
Reference: Custom rules and options ... 348
Custom rules format ... 348
Reference: Custom rules examples ... 349
Example for Custom Quarantine Rules field ... 349
taniumquarantine.dat sample file ... 349
Exporting audit data ... **351**
Tanium Connect ... 354
Before you begin ... 354
Create a connection ... 354
Test a connection and review audit data ... 355
Schedule the connection ... 355
Maintaining Threat Response ... **356**
Review and remediate Tanium Threat Response issues ... 356
Get Threat Response endpoint tools status and configurations ... 356
Monitor and troubleshoot Threat Response coverage ... 360
Monitor and troubleshoot mean time to investigate threats ... 360
Monitor and troubleshoot mean time to remediate threats ... 360
Troubleshooting Threat Response ... **361**
Collect logs ... 362
Collect troubleshooting information from the Threat Response service ... 362
Collect troubleshooting information from endpoints ... 362

© 2025 Tanium Inc. All Rights Reserved

View notifications ... 363
View task status ... 364
View and export log data ... 364
Remove Threat Response tools from endpoints ... 366
My device has no profile or the wrong profile ... 367
No alerts are generated ... 368
Too many alerts are generated ... 369
The lifetime of recorder events is too short ... 370
File, network, or security events are not displayed on Oracle Linux server ... 371
Identify Linux endpoints that are missing auditd ... 371
Start or stop the recorder ... 372
Configure client disk space use ... 372
Modifying client disk space thresholds ... 372
Files are not being hashed or indexed ... 373
Cannot establish a live connection ... 374
Test Live Response connections manually ... 374
Stream is not sending data ... 374
Stream is sending too much data ... 375
Configuration not available or not updated to the latest settings when deploying package ... 376
Action not running on endpoint ... 376
Artifacts not being copied to destination ... 376
Custom configurations are missing ... 377
Live Connections are not working while quarantined ... 377
Live Response is not working to copy files to the destination while quarantined ... 377
Verify endpoint tools ... 377
Uninstall Threat Response ... 377
Contact Tanium Support ... 377
Reference: Common health check issues ... 378
Fatal error loading subscriptions: auditd raw logging is enabled. Not loading rules. ... 378
Scan completion took longer than configured scan interval. Maybe under spec or subscription misconfigured? ... 378

© 2025 Tanium Inc. All Rights Reserved

Subscription has dropped events: <subscription name> ... 378
System minimum requirements not met to enable features: Single CPU detected. Not loading rules. ... 379
All configured audit rules did not load. Check rules for correctness. Recorder may not be seeing all events. ... 379
TaniumAuditPipe not running. ... 380
Failed to configure Tanium Driver provider. Check extensions log. Recorder may not be seeing all events. ... 380
Fatal error loading subscriptions: waiting for TaniumAuditPipe to be available. Not getting events. ... 380
Profile and/or Intel not fully resolved. ... 380
Reference: Alert data ... **382**
Finding ... 389
Finding.Whats ... 390
ArtifactActivity ... 391
IntraIdContext ... 391
ExternalSecurityEvent ... 392
ArtifactAction (relevant_actions) ... 392
Artifact ... 392
LocalSystemInfo ... 393
ProcessArtifact ... 393
ProcessArtifact.Handle ... 394
UserArtifact ... 394
FileArtifact ... 395
RegistryArtifact ... 395
RegistryArtifact.Value ... 395
RegistryArtifact.MultiSZ ... 396
WindowsEventLogArtifact ... 396
ServiceArtifact ... 397
DNSRequestArtifact ... 397
NetworkPortArtifact ... 398
DriverArtifact ... 398
ArtifactHash ... 399
AutomationEngine ... 399

© 2025 Tanium Inc. All Rights Reserved

ReactionStatusDetails 399
Step 399
StepResult 400
SignatureData 400
MicrosoftDefenderEventArtifact 400
WindowsPEInfo 401
WindowsPEInfo.Section 401
WindowsPEInfo.Exports 401
WindowsPEInfo.Import 401
WindowsPEInfo.Symbol 402
Reference: Set up the zone proxy service 403
Reference: Gateway examples for Threat Response 404
Threat Response example 404
Assign Resolved status to an alert (mutation.threatResponseAlertResolve) 404
Assign Resolved status to alert 404

© 2025 Tanium Inc. All Rights Reserved

Threat Response overview

Use Threat Response to expedite incident response actions from hours or days to minutes. Detect, react, and recover quickly from attacks and the resulting business disruptions.

Investigation

Threat Response continuously records key system activity for forensic and historical analysis. You can look for specific activity across every endpoint in an enterprise and drill down into process and user activity on individual endpoints in both real-time and historical views. You can investigate alerts from external sources such as Microsoft Defender and Deep Instinct to leverage the endpoint visibility provided by Threat Response.

Detection

Threat Response monitors activity in real time and generates alerts when potential malicious behavior is detected. You can configure threat intelligence from a variety of reputable sources such as TAXII and iSight. Use threat intelligence to search endpoints for known indicators of compromise and perform reputation analysis. The reputation data that Threat Response uses constantly compares activity such as all processes run, autorun related files, and loaded modules against known malicious hashes defined by user hash lists or other services such as Palo Alto Wildfire, VirusTotal, and ReversingLabs.

Containment

Threat Response includes sensors and packages that provide endpoint visibility and remediation. With the sensors, you can search endpoint data quickly for evidence of compromise. When you have discovered compromised endpoints, you can use Threat Response packages to isolate incidents and prevent additional compromise, data leakage, and lateral movement.

Tanium Autonomous IT Platform in Threat Response

- **Tanium Automate playbook steps**: Tanium Automate implements endpoint quarantine and quarantine removal in playbook steps. For more information, see , Tanium Automate User Guide: Building playbooks, and Tanium Automate User Guide: Reference: Steps.
- **Default configuration**: Threat Response provides common configuration workflows to expedite the time to value and to simplify the initial configuration experience. Configuration categories that target specific end-to-end scenarios decrease the number of steps required to operationalize Threat Response without having a comprehensive knowledge of all of the functionality of the module.

Supported languages

You can select one of the languages in the following table for user interface (UI) text in the Threat Response workbench and Tanium documentation. The language that you select for the workbench also sets the date and time format:

© 2025 Tanium Inc. All Rights Reserved

- **Dates**: In the table, the letters `dd`, `mm`, and `yyyy` represent the digits for day, month, and year respectively.
- **Times**: English (United States) times use the 12-hour clock in the format `hh:mm:ss [AM|PM] <time zone>`, where `hh`, `mm`, and `ss` represent the hour, minute, and second respectively. Other times use the 24-hour clock, where `GMT-<#>` indicates the offset from Greenwich Mean Time (GMT). For example, `GMT-7` indicates a time zone that is 7 hours ahead of GMT.

Supported languages with associated date and time formats

Language	Locale code	Date and time format
English (United States)	en-US	mm/dd/yyyy [AM|PM] *<time zone>*
French (France)	fr-FR	dd/mm/yyyy GMT-*<#>*
German (Germany)	de-DE	dd/mm/yyyy GMT-*<#>*
Japanese (Japan)	ja-JP	yyyy/mm/dd GMT-*<#>*
Korean (Korea, Republic of)	ko-KR	yyyy.mm.dd GMT-*<#>*
Spanish (Latin American)	es-LA	dd/mm/yyyy GMT-*<#>*

For information about language support, which types of text are translated, and the steps to select a language, see Tanium Console User Guide: Reference: Language support.

Interoperability with other Tanium products

Threat Response works with Tanium™ Connect, Tanium™ Data Service, Tanium™ Enforce, Tanium™ Impact, Tanium™ Investigate, and Tanium™ Trends for additional alerting, remediation, and trending of incident related data.

Tanium Connect

Configure a Connect destination to export Threat Response data outside of Tanium. Connect can send information to security information and event management (SIEM) products and services including Micro Focus ArcSight, IBM QRadar, LogRhythm, McAfee SIEM, and Splunk. For more information, see Connect User Guide: Configuring SIEM destinations. Threat Response sends hash information from saved questions to Connect and reputation service providers to elaborate on process hashes for an at-a-glance reputation status. You can also configure incoming connections from sources such as Palo Alto Wildfire to create threat data.

Tanium Data Service

Tanium Data Service (TDS) is a Tanium shared service that enables you to view stored sensor results for endpoints that are offline at the moment you issue a question. For more information about TDS, see Managing Tanium Data Service.

© 2025 Tanium Inc. All Rights Reserved

Tanium Enforce

Use Threat Response findings to create process and network rule policies for endpoints to prevent future incidents across the network. Failing to identify and address more fundamental vulnerabilities exploited during an incident leaves the organization with no net improvement to their security posture.

Tanium Impact

Use alert integration with Impact to take a data-driven approach to manage lateral movement impact within your organization by identifying, prioritizing and remediating access rights dependencies to reduce attack surface, prioritize actions, and scope incidents.

Tanium Investigate

From the sample details view in the context analyzer and the events grid on direct endpoint connections, you can add events to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

Tanium Trends

Threat Response features Trends boards that provide data visualization of Threat Response concepts.

THREAT RESPONSE - ALERTS

When a match to intel that you have applied on a computer group is detected, an alert is generated from the endpoint and reported back to Threat Response. The **Threat Response - Alerts** board features visualizations that illustrate patterns of alerts over time on the endpoints in an environment. The following panels are in the **Threat Response - Alerts** board:

- Mean Time to Investigate Alerts
- Mean Time to Resolve Alerts
- Lifetime Alerts Count
- Alerts by Status
- Alerts by Endpoint
- Alerts by Intel
- Alerts by Intel Type
- Alerts by Intel Source
- Alerts by Label

THREAT RESPONSE - STREAM STATS

The **Threat Response - Stream Stats** board features visualizations that show the status of stream data generation. The following panels are in the **Threat Response - Stream Stats** board:

© 2025 Tanium Inc. All Rights Reserved

- Data Sent This Month
- Data Sent Last Month

For more information about how to import the Trends boards that are provided by Threat Response, see Tanium Trends User Guide: Importing the initial gallery.

© 2025 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Threat Response

There are four key organizational governance steps to maximizing the value delivered by Threat Response to enable time to value:

- Develop a dedicated change management process. See Change management on page 22.
- Define distinct roles and responsibilities. See RACI chart on page 22.
- Track operational maturity. See Operational metrics on page 30.
- Validate cross-functional alignment. See Organizational alignment on page 30.

Change management

Develop a tailored, dedicated change management process to set up any incident response tools for a streamlined process using Tanium Threat Response.

- Update service level agreements and align activities to key resources for Tanium Threat Response where applicable. For example, see Maturity / Metrics and RACI
- Designate change or maintenance windows for various scenarios, where applicable. For example, setting up a Reputation source, integration with a SIEM, Log Solution, or SOAR solution.
- Identify internal and external dependencies to incident response process. For example, to achieve effective integrations with a SIEM, Log Solution, or SOAR Solution.
- Create a Tanium Steering Group (TSG) for discovery activities to expedite reviews and approvals of processes that align with SLAs / incident response processes, as applicable.

RACI chart

A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, and serves as a guideline to describe the key activities across the security, risk/compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against patch management. Use the following table as a baseline example.

© 2025 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Unstructured Threat Investigation	C/I	R/A	C/I	-	-	One of three starts to an investigation. For example, you have a hypothesis or are not sure of specific indicators to look for. You have not yet identified a problem and use Enterprise Hunting or other tools to investigate and understand a problem.
Known Target/Hypothesis	R/A	C/I	C/I	I	-	One of three starts to an investigation wherein a known target has been identified; for example, malware X or attacker Y uses this capability or technique for malicious intent in the environment. Use one of four techniques (Index, Incident Response Sensors, Live Connection, or Tanium Questions) to understand this known target. For example, use Tanium questions to show malware and what is relevant to that technique. You might not have a specific indicator or file you are looking for, but you know the attacker will put unusual things in outruns such as a technique - but not an indicator - and use for known target for questions.

© 2025 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Enterprise Hunting: Index, Incident Response Sensors, Tanium Questions, Live Connections	CI	R/A	R/A	-	-	Using Tanium questions to gather enterprise-wide data to establish a hypothesis and establish what is normal activity.
Establish what is normal activity	R/A	R/A	R/A	-	-	Use autoruns to establish normal activity from abnormal activity. For example, if a network has 10 devices that all demonstrate the same conditions, or establish that 9 out of 10 are normal. Something might only be available on one endpoint demonstrating a need for investigation. If you have identified what is normal or abnormal, go to establishing the hypothesis of the activity; for example, an attacker created an autorun.
Establish hypothesis of activity	C/I	R/A	R/A	I	-	When you have established what is normal versus abnormal, you can establish a hypothesis of the activity and conduct additional hunting for more information or establish suspicious activity to take action or remediation.

© 2025 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Additional hunting required	I	R/A	R/A	-	-	While working through what is normal versus abnormal activity, and establishing a hypothesis to perform actions or remediate, you might conduct additional hunting to understand the behavior.
Reputation and third-party validation	R/A	C/I	C/I	-	-	The reputation services provide the capability to compare information from the enterprise against lists of known bad at scale. The reputation service and Threat Response integrate to automatically search for relevant artifacts and then create IOCs from any malicious reputations discovered in the environment and then scan them to establish exposure.
Establish suspicious activity	R/A	R/A	R/A	I	I	When the suspicious activity has been established, decide on a course of action that might require further monitoring or investigation, or remediate the suspicious activity using Tanium and/or external tools.

© 2025 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Further Investigation: Live Connection	C/I	R/A	R/A	-	-	Further investigations might be required to establish the real cause of any activity discovered in the previous steps. This might be performed entirely in the Tanium platform or by gathering information for analysis in 3rd party applications.
Further Investigation: Live Response	C/I	R/A	R/A	-	-	Further investigations might be required to establish the real cause of any activity discovered on the previous steps. This might be performed entirely in the Tanium platform or by gathering information for analysis in 3rd party applications.
Further Investigation: Questions	R/A	R/A	R/A	-	-	Further investigations might be required to establish the real cause of any activity discovered on the previous steps. This might be performed entirely in the Tanium platform or by gathering information for analysis in 3rd party applications.
Select Action/Actions	R/A	R/A	R/A	I	-	Apply established process for further action or discuss and establish new course of action for previously undocumented activity.

© 2025 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Remediation: Operational Modules	C/I	C/I	C/I	-	-	When a suspicions activity has been established, and an action identified, remediation can be conducted using Tanium Operational Modules. This may often be outside of the realm of responsibility of the security organization who needs to hand off the requirement to the operations team or might involve some level of security team involvement in actions such as quarantining while further action is performed.
Remediation: Security/Risk Modules	R/A	C/I	C/I	-	-	When suspicious activity has been established, and an action identified, remediation can be conducted using Tanium Security Modules through Threat Response. For example, use built-in actions to kill processes, quarantine endpoints, delete files and folders, delete registry keys, or use Tanium Enforce for application allowlisting, firewall configuration, or security policy management.

© 2025 Tanium Inc. All Rights Reserved

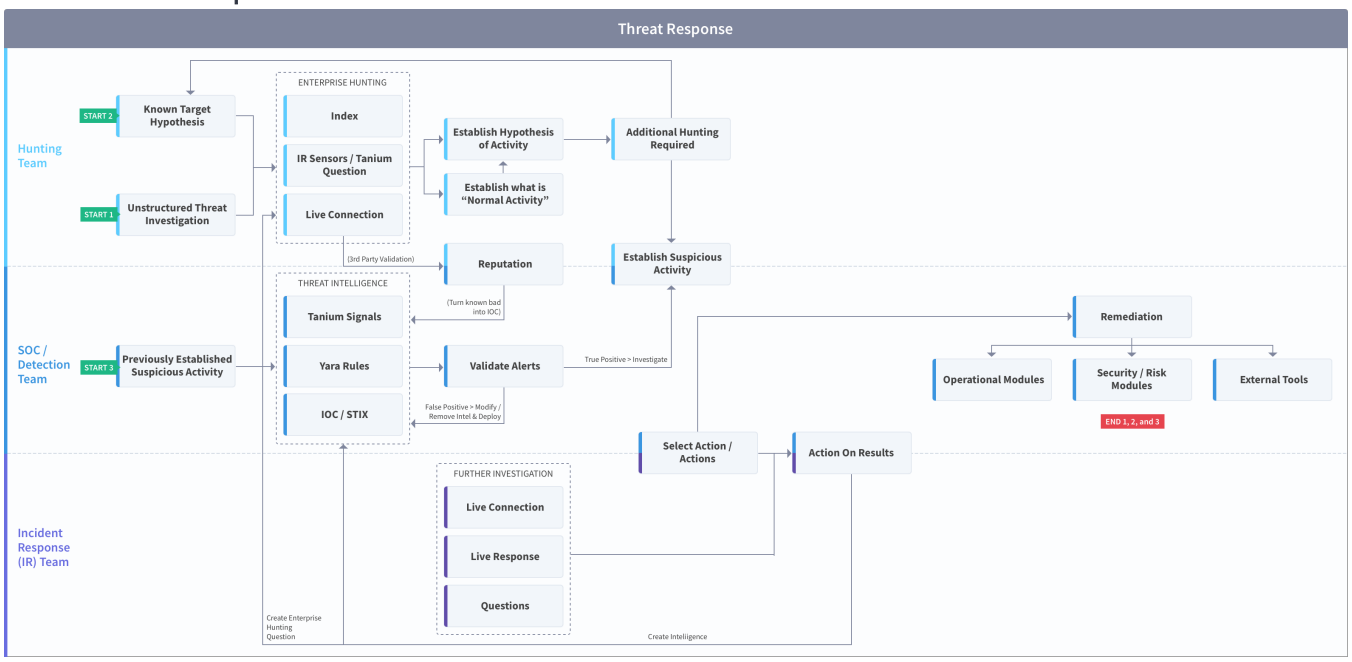
Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Remediation: External Tools	C/I	C/I	C/I	I/R/A	I	When suspicious activity has been established, and an action identified, remediation can be conducted using third-party capabilities and/or external organizations. This might often be outside the realm of responsibility of the security organization who need to hand off the requirement to the operations team or might involve some level of security team involvement in actions like quarantining while further action is performed.
Previously established suspicious activity	R/A	C/I	C/I	-	-	One of three starts to detection activity; for example, use Tanium Signals, YARA rules, and or IOC/STIX to validate alerts and identify true positives to further investigate and identify false positives to modify or remove intelligence and redeploy alerts.
Threat Intelligence: Tanium Signals	R/A	C/I	C/I	-	-	Install and deploy threat intelligence and then monitor systems for alerts from the environment.
Threat Intelligence: YARA Rules	R/A	C/I	C/I	-	-	Install and deploy threat intelligence and then monitor systems for alerts from the environment.

© 2025 Tanium Inc. All Rights Reserved

Task	SOC (Detection & Alerts) / L1	Hunting Team / L2	Incident Response (IR)	CISO	C-Level	Rationale
Threat Intelligence: IOC/STIX	R/A	C/I	C/I	-	-	Install and deploy threat intelligence and then monitor systems for alerts from the environment.
Validate Alerts: True Positive > Investigate	R/A	R/A	R/A	-	-	Activity that results as part of Threat Intelligence activities to validate an alert as a true positive and further investigate. This can result in escalation to higher levels.
Validate Alerts: False Positive > Modify/Remove Intelligence and Redeploy	R/A	R/A	R/A	-	-	SOC/L1 activity to analyze alert data and validate an alert as a false positive. This results in an action to modify or remove intelligence or to redeploy threat intelligence. Control of Threat Intelligence is often the responsibility of hunting or incident response teams.
Action on Results: Create Enterprise Hunting Question or Intelligence	C/I	R/A	R/A	I	-	Create alerts based on intelligence, hunting, or detection activities for automation. For example, Saved questions, alerts, or signals. Use the enterprise hunting dashboard to ask a saved question and have the results sent to SIEM or reputation tool.

© 2025 Tanium Inc. All Rights Reserved

Standard Threat Response workflow



Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk / compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions on how to manage software and hardware assets.

Operational metrics

Threat Response maturity

Managing an incident response program successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Threat Response program are as follows:

Process	Description
Usage	how and when Tanium Threat Response is used in your organization
Automation	how automated Tanium Threat Response is, across endpoints
Functional Integration	how integrated Tanium Threat Response is, across IT security, IT operations, and IT risk or compliance teams
Reporting	how automated Tanium Threat Response is and who the audience of Threat Response reporting is

© 2025 Tanium Inc. All Rights Reserved

Benchmark metrics

In addition to the key incident response processes, the three key benchmark metrics that align to the operational maturity of the Tanium Threat Response program to achieve maximum value and success are as follows:

Executive Metrics	Threat Response Coverage	Mean Time to Investigate Threats	Mean Time to Remediate Threats
Description	The percentage of endpoints that are running Threat Response tools.	The average number of days to perform analysis of threats.	The average number of days to remediate threats.
Instrumentation	The number of endpoints with an active Threat Response profile.	The time it takes from an Alert was received, to when remediation work on the detected alert begins.	The time it takes to author an Action or Enforce Remediation Policy status to resolve applicable Alerts.
Why this metric matters	If you are not including the entirety of your estate when searching for specific activity, then you are at risk.	The more quickly you can evaluate the risk associated with a given activity, the more quickly you can begin remediating a threat.	The more quickly you can remediate a threat, the more you can contain the associated damage.

Use the following table to determine the maturity level for Tanium Threat Response in your organization.

© 2025 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Threat Response installed; deployment profiles applied. Use of Threat Response questions and investigations. Components configured or in use: Index, Recorder, Detect.	Some Tanium Signals deployed; understanding of Tanium Signals syntax basics. Live Response Destinations configured and tested. Tanium IR Quarantine tested with default configuration. Components in use: Index, Recorder, Detect, Live Response, Trends.	Threat intelligence testing process created; tailoring Tanium Signals to the environment. Process injection alerting enabled. Multiple custom Live Response forensic data collection configurations created. Tanium IR Quarantine custom configuration setup and tested. Default Recorder filters implemented. Using Quick Scans and Background Scanning for Threat Response Intel. Components in use: Index, Recorder, Detect, Live Response, Trends, IR Content, Reputation.	Tuned deployment strategy for profiles and intel documents, including intel testing and promotion. Process injection alerting enabled and tuned. Creation of suppression rules for Tanium Signals to reduce false positives. Threat Response Alert triage and remediation using Response Actions Custom Recorder filters. Enables longer data retention, less noise when investigating events, and better performance of THR on endpoints. Components in use: Index, Recorder, Detect, Live Response, Trends, IR Content,	Proactive hunting for malicious activity (through Enterprise Hunting or Incident Response Sensors). Process injection alerting enabled and tuned. Generating custom YARA rules, IOCs, and Tanium Signals and sharing through the Threat Response community. Enables development and application of customized intel for given industry vertical and industry specific information sharing and analysis centers (ISACs). Components in use: Index, Recorder, Detect, Live Response, Trends, IR Content, Reputation, Connect, SIEM / Log Solution Integration, Tanium Enforce.

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Automation	Some intelligence applied and imported (For example, a few Tanium Signals, OpenIOC Intel, etc.)	Additional threat intelligence applied, and intel sources added. Ex: out of the box Tanium Signals, OpenIOCs, and a subscription to a TAXII source has been configured to automate searching for malicious behavior.	Tanium Reputation and Tanium Connect saved question configured to automatically feed hashes to Reputation Providers.	Automated Threat Response scanning of malicious hashes found via Reputation providers. Using the Threat Response API to automate tasks.	Integration with a SOAR Solution to automate evidence gathering, response actions, intel management (adding/removing/scanning), remediation, etc.)
	Functional integration	N/A	Trends Boards imported and / or integration with Reputation provider.	Threat Response is configured to surface alerts from Windows Defender and/or Deep Instinct.	Tanium Connect, SIEM / Log Solution integrated. Ex: Splunk and Yara rules set up or Splunk integration set up.	Creating remediation policies through Tanium Enforce and integration with a SOAR solution to automate data collection and performing actions.
	Reporting	Manual; through Threat Response workbench or dashboard for operators only.	Manual; Threat Response integration with Tanium Trends.	Automated; exporting data through file, email, or SQL to feed reports.	Automated; using SIEM / Log Solution; Ex: Splunk including the Tanium Splunk application.	Automated; using a SOAR solution for a holistic view of activity.

© 2025 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Metrics	Threat Response Coverage (% of Total)	0-60%	61-70%	71-85%	86-94%	>95%
	Mean Time to Investigate Threat (time)	>45 days	31-45 days	15-30 days	8-14 days	0-7 days
	Mean Time to Remediate Threat (time)	>45 days	31-45 days	15-30 days	8-14 days	0-7 days
	Historical Lookback Time	0 - 7 days	8 - 14 days	15 - 30 days	31 - 45 days	>45 days

© 2025 Tanium Inc. All Rights Reserved

Threat Response requirements

Review the requirements before you install and use Threat Response.

IMPORTANT

In Threat Response 4.0, the Detect and Event services have been deprecated and replaced by the Threat Response service. The integration with the Threat Response service and the Threat Response Client Extension on the endpoints provides performance improvements and provides a platform for future capability, intelligence, and workflows around intel and alerting.

Threat Response 4.0 includes API changes that require customers and partners to reconfigure API integrations. The API data format may be changed for many existing routes. Most of these changes have been made for consistency in what each API returns. From the Threat Response Workbench, click **Help > API > See API documentation** to review the Threat Response 4.0 API documentation to adjust your integrations appropriately.

For more information on the exact changes and required steps to ensure integrations work as intended, see Threat Response Version 4.0 API Changes.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Threat Response. For more information about how to get Threat Response, see Tanium Solutions & Bundles.
- **Tanium™ Core Platform server**
- **Tanium™ Client**:
  Any supported version of Tanium Client. For more information, see Tanium Client Management User Guide: Client version and host system requirements.
  If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

Computer group dependencies

When you first sign in to the Tanium Console after a fresh installation of Tanium Server, the server automatically imports the computer groups that Threat Response requires:

- `All Computers`
- `All Windows`
- `All Linux`

© 2025 Tanium Inc. All Rights Reserved

- All Mac

For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups. See Tanium Console User Guide: Create a computer group.

Solution dependencies

Other Tanium solutions are required for Threat Response to function (required dependencies) or for specific Threat Response features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.



Some Threat Response dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 36 and Feature-specific dependencies on page 37. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Threat Response requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Threat Response, the Tanium Server automatically imports all your licensed solutions at the same time. See Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Threat Response to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Threat Response, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Threat Response has the following required dependencies at the specified minimum versions:

- Tanium™ Client Index Extension*
- Tanium™ Client Recorder Extension*
- Tanium™ Connect
- Tanium™ Data Service (TDS)
- Tanium™ Reputation
- Tanium™ Investigate is required to add alerts to an Investigation
- Tanium™ IR Quarantine is required for isolating endpoints
- Tanium™ Direct Connect is required for live endpoint connections

© 2025 Tanium Inc. All Rights Reserved

- Tanium Trends
- Tanium Interact
- Tanium Default Content
- Tanium Endpoint Configuration
- Tanium™ System User Service
- Tanium™ RDB Service
- Tanium Secrets

*= The required version of this client extension is installed as part of Threat Response.

Feature-specific dependencies

If you select only Threat Response to import, you must manually import or update its feature-specific dependencies regardless of the Tanium Console or Tanium Core Platform versions. Threat Response has the following feature-specific dependencies at the specified minimum versions:

- Tanium™ Enforce is required for alert remediation.
- Tanium Impact is required to display Impact ratings for alerts.
- Tanium Trends is required to view visualizations that show current and historical data from endpoints.

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for Threat Response on endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For more information, see Security exclusions. For a list of all Client Extensions and tools, see Tanium Client Management User Guide: Reference: Client extensions used for Tanium solutions.

Tanium™ Module Server

Threat Response is installed and runs as a service on the Module Server host computer. The impact on Module Server host computer sizing is minimal and depends on usage. For more information, see Contact Tanium Support on page 377. As a best practice, 250GB to 1TB of disk space is recommended to ensure available storage for snapshots and other saved Threat Response evidence.

Endpoints

The following endpoint operating systems are supported with Threat Response. The endpoint requirements for Threat Response are consistent with those used for Tanium Performance and Tanium Integrity Monitor. Threat Response uses the Tanium™ Client Recorder Extension to gather data from endpoints.

© 2025 Tanium Inc. All Rights Reserved

Supported operating systems for Tanium Threat Response

Operating System	Version
Windows	A minimum of Windows 7 (SP1) or Windows Server 2008 R2 (with SP1) is required. Windows 8.1 provides DNS event recording capability. Windows XP, Windows Server 2008, and Windows Server 2003 are not supported. Live Response is not supported on Windows 7 (SP1) and Windows Server 2008 R2 endpoints. The ability to collect forensic evidence from Windows 7 (SP1) and Windows Server 2008 R2 endpoints using Live Response will be deprecated in an upcoming version of Threat Response. Windows 7 and Windows Server 2008 R2 operating systems must have the following Microsoft KBs installed: • KB3033929 - "Availability of SHA-2 code signing support for Windows 7 and Windows Server 2008 R2." For details regarding KB3033929, see https://support.microsoft.com/en-us/help/3033929/microsoft-security-advisory-availability-of-sha-2-code-signing-support. • KB4490628 - "Servicing stack update for Windows 7 SP1 and Windows Server 2008 R2 SP1." For details regarding KB4490628, see https://support.microsoft.com/en-us/topic/servicing-stack-update-for-windows-7-sp1-and-windows-server-2008-r2-sp1-march-12-2019-b4dc0cff-d4f2-a408-0cb1-cb8e918feeba. • KB4474419 - "SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008." For details regarding 4474419, see https://support.microsoft.com/en-us/topic/sha-2-code-signing-support-update-for-windows-server-2008-r2-windows-7-and-windows-server-2008-september-23-2019-84a8aad5-d8d9-2d5c-6d78-34f9aa5f8339. • KB4534310 or KB4539601 ◦ KB4534310 - "January 14, 2020—KB4534310 (Monthly Rollup)" For details, see https://support.microsoft.com/en-au/topic/january-14-2020-kb4534310-monthly-rollup-9ce32b1b-77ef-9a17-7ecb-2bcebcaa9ff5. ◦ KB4539601 - "January 31, 2020—KB4539601 (Preview of Monthly Rollup)" For details, see https://support.microsoft.com/en-gb/topic/january-31-2020-kb4539601-preview-of-monthly-rollup-1768e5a4-04bc-e964-a7a7-9509f91b0d1f. Windows 11 (Arm-based) endpoints running in emulation mode are supported. The following are areas where Windows 11 (Arm-based) running in emulation mode are not supported: • Deep Instinct alert integration. • Process Injection monitoring. • Live Response Memory collection may not be fully supported on Arm processors. Process injection monitoring is not supported on Windows 8.1 and Windows Server 2012 R2 and earlier. For Live Response, SSH destinations are not supported on Windows Server. SSH destinations are only supported on Linux and macOS. The recorder forces a vacuum if the database size becomes too large to ensure that a continual vacuuming does not exist. The recorder checks to only vacuum once per day and at least one hour after system startup to make sure vacuum operations do not interfere with system boot.

© 2025 Tanium Inc. All Rights Reserved

Supported operating systems for Tanium Threat Response (continued)

Operating System	Version
macOS	Same as Tanium Client support. Live Response Memory Collection is not supported on macOS endpoints that use M-series ARM chips.
Linux	Same as Tanium Client support with the exceptions noted below. See Tanium Client Management User Guide: Client version and host system requirements. Systemd is required for the Linux autorun sensor to collect data. The Client Recorder Extension does not support CentOS and Red Hat Enterprise Linux versions 5.3 and earlier. Endpoints require version 5.4 or later of CentOS or Red Hat Enterprise Linux. The Client Recorder Extension provides SELinux policies for the following distributions and versions: • Red Hat Enterprise Linux (RHEL) 5.4 and later, 6.x, 7.x, 8.x, and 9.x • CentOS 5.4 and later, 6.x, 7.x, 8.x, and 9.x • Amazon Linux 2 LTS (2017.12) At this time, SELinux is not supported on other Linux distributions. For Linux endpoints: • Install the most recent stable version of the audit daemon and audispd-plugins. For information on deprecated parameters in the audit daemon configuration, see Tanium Client Recorder Extension User Guide. See the specific operating system documentation for instructions. • Be aware that when using immutable "-e 2" mode, the recorder adds Tanium audit rules in front of the immutable flag. When using the -e 2 flag on Linux, the endpoint must be restarted after the recorder is enabled. • Be aware that when using the failure "-f 2" mode, the Linux kernel panics in the event that the auditd message is lost. The recorder does not add audit rules if this configuration is detected.

Disk space requirements

By default, the endpoint database for Threat Response is 1GB in size. On installation, 100MB is reserved on on disk, and the database increases in size to up to 1GB before event pruning occurs. 3GB is recommended. Free disk space is checked when a snapshot is requested.

If Indexing is enabled, space should also be reserved for the Index database. The size of the database depends on several factors, including the types of hashes recorded, the types and number of exclusions to indexing, and the number of files present on the volumes indexed. For planning, a general guideline is that the database size is 1MB per 1GB of files on disk.

© 2025 Tanium Inc. All Rights Reserved

CPU and memory requirements

The Client Recorder Extension does not start on endpoints with a single logical core without updating the **CX.recorder.EnableSingleCpuRequirement** configuration setting to 0. To update CX.recorder.EnableSingleCpuRequirement to 0, edit the **Recorder - Set Recorder Extension Setting [*OS*]** package to add a parameter with the configuration key `EnableSingleCpuRequirement` and a value of `0`, and deploy the package to appropriate endpoints. For more information about editing packages, see Tanium Console User Guide: Edit a Package. Alternatively, you can run the following command from the Tanium Client installation directory on endpoints to update this configuration setting:

- (Windows) `TaniumClient.exe config set CX.recorder.EnableSingleCpuRequirement 0`
- (Linux and macOS) `./TaniumClient config set CX.recorder.EnableSingleCpuRequirement 0`

A minimum of 4 GB RAM is recommended on each endpoint.

Tanium Driver

The Tanium Driver records process and command-line events on supported Windows endpoints. The Tanium Driver is included in initial installations and any subsequent updates of Threat Response. To record event data from Windows endpoints, the Tanium Driver must be installed.

If you are deploying the Tanium Driver to endpoints for the first time, a reboot of endpoints is not required for the driver to capture events, but a reboot is required to view complete process tree data.

Host and network security requirements

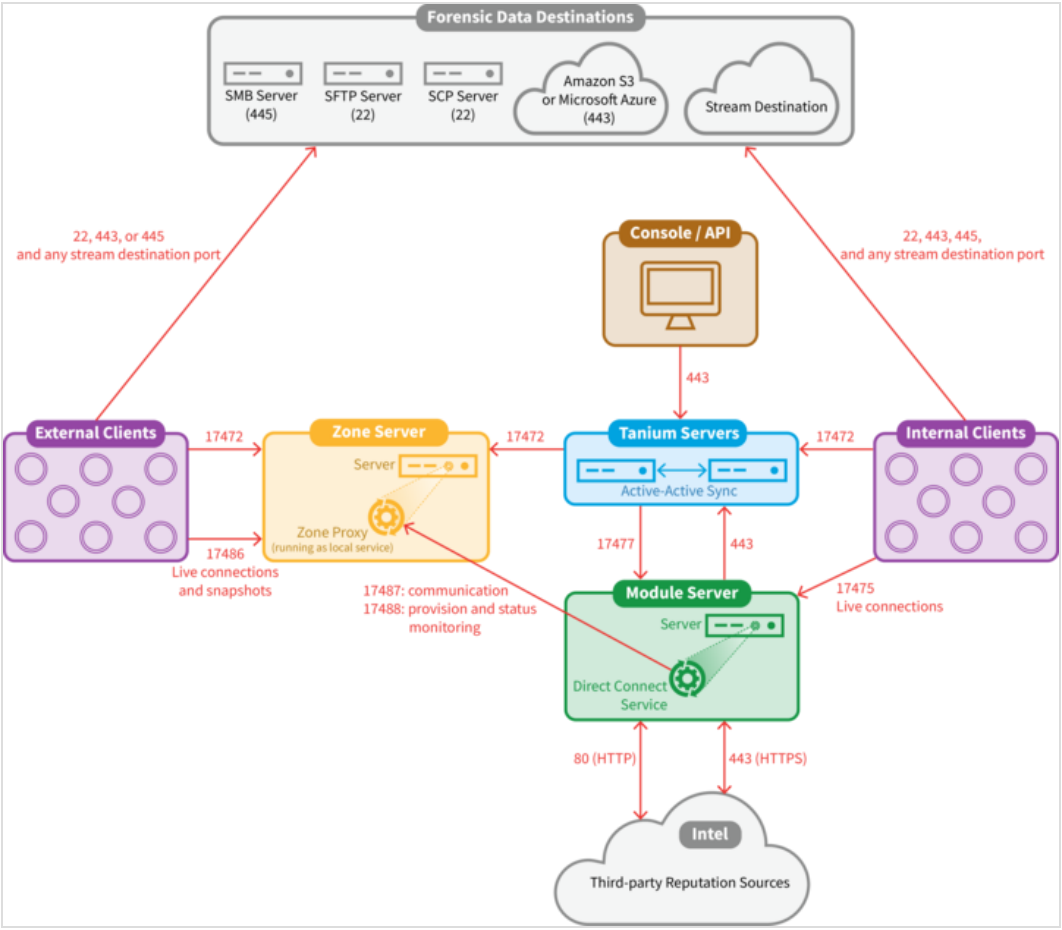
Specific ports and processes are needed to run Threat Response.

Ports

The following ports are required for Threat Response communication.

Required ports for Threat Response communication

© 2025 Tanium Inc. All Rights Reserved



© 2025 Tanium Inc. All Rights Reserved

Required ports for Tanium Threat Response communication

Source	Destination	Port	Protocol	Purpose
Module Server	Direct Connect Zone Proxy	17487 (Direct Connect communication port) and 17488 (Direct Connect provision and status monitoring port)	TCP	(Optional) Tanium Direct Connect connection to Direct Connect Zone Proxy
	Module Server (loopback)	17466	TCP	Internal purposes, not externally accessible
	Intel provider	80, 443	TCP	Integration of intel streams
Tanium Server	Module Server	17477	TCP	Tanium Server initiates connections to the Module Server on port 17477

© 2025 Tanium Inc. All Rights Reserved

Required ports for Tanium Threat Response communication (continued)

Source	Destination	Port	Protocol	Purpose
Tanium Client	Direct Connect	17475 (Direct Connect on Module Server) 17486 (Direct Connect Zone Proxy)	TCP	Connections to the Module Server or the Direct Connect Zone Proxy for live connections
	Live Response destination	443 (S3/Azure), 22 (SFTP/SCP), or 445 (SMB)	TCP	Outbound connections over ports depending on how the collected data is being transferred
	Stream configurations to external destinations	A TCP port for an external destination that you select in a Stream configuration. For Splunk destinations this is provided by a Splunk administrator. For Sentinel destinations this is 514 by default but is configurable.	TCP	Stream events from clients to external destinations that you specify in a Stream configuration.



Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

Security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as `fapolicyd` on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security

© 2025 Tanium Inc. All Rights Reserved

software. For more information about security exclusions to define across Tanium, see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions.



If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

Threat Response security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Tanium Module Server		Process	*<Module Server>*\services\threat-response-service\node.exe
		Process	*<Module Server>*\services\twsm-v1\twsm.exe
		Process	*<Module Server>*\services\endpoint-configuration-service\TaniumEndpointConfigService.exe
Tanium Zone Server		Process	*<Tanium Installation Directory>*\Tanium Direct Connect Zone Proxy\node.exe
		Process	*<Tanium Installation Directory>*\Tanium Direct Connect Zone Proxy\twsm.exe

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows x86 and x64		Process	`<Tanium Client>\Tools\IR\TaniumExecWrapper.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\Tools\IR\TaniumFileInfo.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\Tools\IR\TaniumHandle.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumIndex.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumIndex.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\Tools\recorder\TaniumRecorderCtl.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumRecorder.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumRecorder.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\SupportCX.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\SupportCX.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\recorder\proc.bin`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\recorder\recorder.db`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\recorder\recorder.db-shm`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\recorder\recorder.db-wal`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\index\index.db`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\index\index.db-shm`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\index\index.db-wal`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumStream.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumStream.dll.cfg`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumStream.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumExtras.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumExtras.dll.cfg`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumExtras.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x86 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverCtl.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x64 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverCtl64.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x86 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverSvc.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	x64 endpoints	Process	`<Tanium Client>\tools\driver\TaniumDriverSvc64.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\tools\driver\service\TaniumDriverSvc.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\tools\driver\TaniumProcessMonitor.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\tools\driver\TaniumProcessMonitor64.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumThreatResponse.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\TaniumThreatResponse.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\core\TaniumPythonCx.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\extensions\core\TaniumPythonCx.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Folder	`<Tanium Client>\extensions\stream`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\TaniumClientExtensions.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\TaniumClientExtensions.dll.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>\Tools\IR\TaniumPersistenceAnalyzer.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>\Tools\IR\PowerForensics\PowerForensics.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	1	File	`<Tanium Client>\Tools\IR\data\Action_*\PowerForensics.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	1	File	`<Tanium Client>\Tools\IR\data\Action_*\PSTaniumFileTransfer_64.dll`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	1	Process	`<Tanium Client>\Tools\IR\data\Action_*\taniumfiletransfer_32.exe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	1	Process	<*Tanium Client*>\Tools\IR\data\Action_*\taniumfiletransfer_64.exe
	1	Process	<*Tanium Client*>\Tools\IR\data\Action_*\TaniumHandle_32.exe
	1	Process	<*Tanium Client*>\Tools\IR\data\Action_*\TaniumHandle_64.exe
	1	Process	<*Tanium Client*>\Tools\IR\data\Action_*\winpmem_mini_x64_rc2.exe
		File	<*Tanium Client*>\Tools\IR\PSTaniumFileTransfer.dll
		Process	<*Tanium Client*>\Tools\IR\TanFileInfo.exe
		Process	<*Tanium Client*>\Tools\IR\taniumfiletransfer.exe
		Process	<*Tanium Client*>\Tools\Copy\taniumfiletransfer.exe
		Process	<*Tanium Client*>\Tools\IR\py\incident_response_deps_platform\38-cp38-win32\taniumfiletransfer\taniumfiletransfer.exe
		Process	<*Tanium Client*>\Tools\IR\py\incident_response_deps_platform\312-cp312-win32\taniumfiletransfer\taniumfiletransfer.exe
		Process	<*Tanium Client*>\Tools\IR\TaniumHandle.exe
		Process	<*Tanium Client*>\Tools\IR\TaniumListModules.exe
		Process	<*Tanium Client*>\Tools\IR\TaniumPersistenceAnalyzer.exe
		File	<*Tanium Client*>\TPython\TPython.bat
		Folder	<*Tanium Client*>\TPython312
		Folder	<*Tanium Client*>\python312
		Process	<*Tanium Client*>\python312\TPython.exe
		Process	<*Tanium Client*>\TaniumCX.exe
		File	<*Tanium Client*>\extensions\TaniumDEC.dll
		File	<*Tanium Client*>\extensions\TaniumDEC.dll.sig
		File	C:\Windows\System32\drivers\TaniumRecorderDrv.sys
		File	C:\Windows\SysWOW64\TaniumProcessMonitor.dll
		File	C:\Windows\system32\drivers\TaniumProcessMonitor.dll

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
Linux x86 and x64		Process	`<Tanium Client>/extensions/recorder/TaniumAuditPipe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/TaniumCX`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/Tools/IR/TaniumExecWrapper`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.so`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.so.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Folder	`<Tanium Client>/python312`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/python312/python`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/python312/bin/pybin`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/TPython/TPython`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Folder	`<Tanium Client>/TPython312`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.so`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.so.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libSupportCX.so`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libSupportCX.so.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumThreatResponse.so`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumThreatResponse.so.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumRecorder.so`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumRecorder.so.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/recorder/proc.bin`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/recorder/recorder.db`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>/extensions/recorder/recorder.db-shm
		File	<*Tanium Client*>/extensions/recorder/recorder.db-wal
		File	<*Tanium Client*>/extensions/recorder/recorder.auditpipe
		File	<*Tanium Client*>/extensions/index/index.db
		File	<*Tanium Client*>/extensions/index/index.db-shm
		File	<*Tanium Client*>/extensions/index/index.db-wal
		File	<*Tanium Client*>/extensions/core/libTaniumPythonCx.so
		File	<*Tanium Client*>/extensions/core/libTaniumPythonCx.so.sig
		File	<*Tanium Client*>/extensions/libTaniumDEC.so
		File	<*Tanium Client*>/extensions/libTaniumDEC.so.sig
		Folder	<*Tanium Client*>/extensions/stream
		File	<*Tanium Client*>/extensions/libTaniumStream.so
		File	<*Tanium Client*>/extensions/libTaniumStream.so.cfg
		File	<*Tanium Client*>/extensions/libTaniumStream.so.sig
		File	<*Tanium Client*>/extensions/TaniumExtras.so
		File	<*Tanium Client*>/extensions/TaniumExtras.so.cfg
		File	<*Tanium Client*>/extensions/TaniumExtras.so.sig
	1	File	<*Tanium Client*>/Downloads/Action_*/linpmem-*.bin
	1	Process	<*Tanium Client*>/Tools/IR/taniumfiletransfer
		File	<*Tanium Client*>/Tools/IR/linpmem_3.0rc2.bin
	1	File	<*Tanium Client*>/Downloads/Action_*/linpmem_3.0rc2.bin
		Process	<*Tanium Client*>/Tools/IR/py/incident_response/_deps/_platform/38-cp38-linux_x86_64/taniumfiletransfer/taniumfiletransfer
		Process	<*Tanium Client*>/Tools/IR/py/incident_response/_deps/_platform/312-cp312-linux_x86_64/taniumfiletransfer/taniumfiletransfer

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
macOS		Process	`<Tanium Client>/TaniumCX`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
	For macOS Universal only	Process	`<Tanium Client>/TaniumCX.app/Contents/MacOS/TaniumCX`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/Tools/IR/TaniumExecWrapper`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.dylib`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumIndex.dylib.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Folder	`<Tanium Client>/python312`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/python312/python`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/python312/bin/pybin`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	`<Tanium Client>/TPython/TPython`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Folder	`<Tanium Client>/TPython312`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.dylib`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/libTaniumClientExtensions.dylib.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumThreatResponse.dylib`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumThreatResponse.dylib.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumRecorder.dylib`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumRecorder.dylib.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/recorder/proc.bin`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/recorder/recorder.db`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/recorder/recorder.db-shm`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/recorder/recorder.db-wal`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/recorder/recorder.auditpipe`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/core/libTaniumPythonCx.dylib`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/index/index.db`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/index/index.db-shm`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/index/index.db-wal`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/core/libTaniumPythonCx.dylib.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		Folder	`<Tanium Client>/extensions/stream`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumDEC.dylib`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libTaniumDEC.dylib.sig`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	`<Tanium Client>/extensions/libSupportCX.dylib`

© 2025 Tanium Inc. All Rights Reserved

Threat Response security exclusions for endpoints (continued)

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<*Tanium Client*>/extensions/libSupportCX.dylib.sig
		File	<*Tanium Client*>/extensions/libTaniumStream.dylib
		File	<*Tanium Client*>/extensions/libTaniumStream.dylib.cfg
		File	<*Tanium Client*>/extensions/libTaniumStream.dylib.sig
		File	<*Tanium Client*>/extensions/libTaniumExtras.dylib
		File	<*Tanium Client*>/extensions/libTaniumExtras.dylib.cfg
		File	<*Tanium Client*>/extensions/libTaniumExtras.dylib.sig
		Process	<*Tanium Client*>/Tools/IR/taniumfiletransfer
	1	Process	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/libaff4.0.dylib
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/libpcre.1.dylib
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/libpcre++.0.dylib
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/libraptor2.0.dylib
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/libsnappy.1.dylib
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/liburiparser.1.dylib
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/libuuid.16.dylib
	1	File	<*Tanium Client*>/Tools/IR/data/Action_*/osxpmem.app/libs/libyaml-cpp.0.6.dylib
		Procress	<*Tanium Client*>/Tools/IR/py/incident_response/_deps/_platform/312-cp312-macosx_10_11_x86_64/taniumfiletransfer/taniumfiletransfer
		Process	<*Tanium Client*>/Tools/IR/py/incident_response/_deps/_platform/38-cp38-macosx_10_11_x86_64/taniumfiletransfer/taniumfiletransfer

© 2025 Tanium Inc. All Rights Reserved

[1] = Where * corresponds to the action ID or the version of linpmem.

User role requirements

Predefined roles grant the following permissions, which are required to use Threat Response functionality:

- Threat Response solution permissions on page 140
- Threat Response administration and platform content permissions on page 151: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Threat Response users on page 158.

Some Threat Response solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Threat Response. If you create custom roles for Threat Response users, be sure to assign all the solution permissions and content set permissions that are required for Threat Response functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role

NOTE

Do not assign the **Threat Response Service Account** and **Threat Response Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Threat Response solution permissions

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Access to the Threat Response workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Alert Deploy Allows for action deployment from a Threat Response alert	✓ ACTION	✓ ACTION	✓ ACTION	✗	✗
Threat Response Alerts Access to read and modify alerts	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response All Signals Suppression Rules Access to modify all signals suppression rules in Threat Response	✓ WRITE	✓ WRITE	✓ WRITE	✗	✗
Threat Response API Perform Threat Response operations using the API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Threat Response API Doc View and list API Docs	✓ READ	✓ READ	✓ READ	✓ READ	✗
Threat Response Audit Allows viewing and exporting Threat Response Audit data	✓ READ	✓ READ	✗	✗	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Configs Access to read and create configurations	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✓ READ
Threat Response Content Provides content privileges for Threat Response users	✓ USER	✓ USER	✓ USER	✗	✗
Threat Response Content Incident Response Provides content privileges for Threat Response Incident Response users	✓ USER	✓ USER	✓ USER	✗	✗
Threat Response Content Incident Response Administrator Provides content privileges for Threat Response Incident Response administrators	✓ ADMINISTRATOR	✓ ADMINISTRATOR	✗	✗	✗
Threat Response Content Incident Response Readonly Provides content privileges for Threat Response Incident Response read only users	✓ USER	✓ USER	✓ USER	✓ USER	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Content Index Provides content privileges for Threat Response Index users	✓ USER	✓ USER	✓ USER	✓ USER	✗
Threat Response Content Index Administrator Provides content privileges for Threat Response Index administrators	✓ ADMINISTRATOR	✓ ADMINISTRATOR	✗	✗	✗
Threat Response Content Readonly Provides content privileges for Threat Response Readonly users	✓ USER	✓ USER	✓ USER	✓ USER	✗
Threat Response Context Analyzer Provides content privileges to use Context Analyzer	✓ WRITE	✓ WRITE	✓ WRITE	✗	✗
Threat Response Data Collection Identify Allows the user to use the TDS Oracle service to get EIDs	✓ WRITE	✗	✗	✗	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Direct Connect Allows bypassing Direct Connect action approvals	✓ BYPASS	✓ BYPASS	✓ BYPASS	✗	✗
Threat Response Downloads Read and manage downloaded files from live connections	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Endpoint Configuration Enables approver privileges in Tanium Endpoint Configuration for Threat Response configuration changes	✗	✓ DISMISS REJECT	✗	✗	✓ APPROVE
Threat Response Enterprise Hunting View and list sensors for enterprise hunting	✓ READ	✓ READ WRITE	✓ READ	✓ READ	✓ READ
Threat Response Exports Create, view, and delete exported events	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Filters Access to read and create filters	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✓ READ

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Health Status Allows use of health status actions	✓ WRITE	✗	✗	✗	✗
Threat Response Intel Allows creating, viewing, and deploying Threat Response Intel	✓ DEPLOY READ WRITE	✓ DEPLOY READ WRITE	✓ READ	✓ READ	✗
Threat Response Intel Reaction Allows reading and modifying Intel reaction related attributes in Threat Response.	✓ WRITE	✓ WRITE	✓ WRITE	✗	✗
Threat Response Intel Safeguards Allows reading and modifying Intel Safeguard related attributes in Threat Response.	✓ WRITE	✓ WRITE	✗	✗	✗
Threat Response Labels Access to read and modify intel labels	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Live Connection Allows setting and viewing live connections to endpoints	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Live Connection File Allows deletion of a file on the endpoint during a live connection	✓ DELETE	✓ DELETE	✗	✗	✗
Threat Response Live Connections Filesystem Browse the filesystem on live connections	✓ BROWSE	✓ BROWSE	✓ BROWSE	✓ BROWSE	✗
Threat Response Live Response Collection Configs Access to read and create Threat Response Live Response Collection configurations	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Live Response Destinations Access to read and createThreat Response Live Response destinations	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Live Response File Collector Sets Access to read and create Threat Response Live Response file collector set configurations	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Live Response Modules Access to read Threat Response Live Response module configuration information	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Live Response Packages Access to create Threat Response Live Response packages	✓ GENERATE	✓ GENERATE	✗	✗	✗
Threat Response Live Response Script Sets Access to read and create Threat Response Live Response script set configuration information	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Threat Response Logs Allows viewing Threat Response logs	✓ READ	✗	✗	✗	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Notification Access to read and modify notifications	✓ READ WRITE	✓ READ WRITE	✗	✗	✗
Threat Response On Demand Scans [2] Access to run and read the results of on-demand scans	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Operator Settings Allows the operator to read and modify available settings	✓ READ WRITE	✓ READ WRITE	✗	✗	✗
Threat Response Operator Status Allows the operator to view the module status	✓ READ	✗	✓ READ	✓ READ	✗
Threat Response Override Scan Allows for overriding scan blockout windows on endpoints.	✓ BLOCKOUTS	✓ BLOCKOUTS	✗	✗	✗
Threat Response Profiles Access to read, create, and deploy profiles	✓ READ WRITE DEPLOY	✓ READ WRITE DEPLOY	✓ READ	✗	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Quarantine Packages Allows for the generation of Threat Response Quarantine Packages	✓ GENERATE	✓ GENERATE	✓ READ	✗	✗
Threat Response Quarantine Profile Allows users to read and write quaranting profiles and rules	✓ READ WRITE	✓ READ WRITE	✗	✗	✗
Threat Response Reputation Allows operations against Reputation	✓ READ INTEGRATIONS	✓ READ INTEGRATIONS	✓ READ	✓ READ	✗
Threat Response Response Actions Enables users to view, create, and stop response actions	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Saved Evidence View and save events from live endpoint connections	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✗	✗
Threat Response Settings Allows viewing and editing Threat Response settings	✓ READ WRITE	✗	✓ READ	✓ READ	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Snapshot Capture,view, and delete snapshots	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Sources 2 Access to read and modify sources	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Stats Allows viewing Threat Response stats	✓ READ	✓ READ	✓ READ	✓ READ	✗
Threat Response Status Allows the operator to view status information	✓ READ	✓ READ	✓ READ	✓ READ	✗
Threat Response Suppression Rules Create, edit, view, list, and delete suppression rules	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Threat Response Tasks Access to read Threat Response tasks	✓ READ	✓ READ	✗	✗	✗
Threat Response Trends Board Allows the user to view Trends data	✓ READ	✓ WRITE	✗	✗	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response solution permissions (continued)

Permission	Threat Response Administrator[1]	Threat Response Operator[1]	Threat Response User[1]	Threat Response Read Only User[1,3]	Threat Response Endpoint Configuration Approver[1]
Threat Response Visibility Bypass Enables users to view all alerts and saved evidence regardless of computer group membership	✓ READ	✓ READ	✗	✗	✗

[1]The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions.

[2] Requires permissions for other modules or solutions to complete all tasks in other modules and see all content; such as Protect (version 1.3.0 or later), Connect (version 4.3.0 or later), or Interact. You can assign a role for another product, or create a custom role that lists just the specific privileges needed.

[3] The Threat Response Read Only User role does not have the ability to create live endpoint direct connections. The Threat Response User role is required as a minimum for creating live endpoint connections.

Threat Response administration and platform content permissions

Permission	Permission Type	Threat Response Administrator[1]	Threat Response Operator	Threat Response User	Threat Response Read Only User	Threat Response Endpoint Configuration Approver
Action Group	Administration	✓ READ	✓ READ	✓ READ	✗	✗
Computer Group	Administration	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
User	Administration	✓ READ	✗	✗	✗	✗
Allowed URLs	Administration	✗	✗	✗	✗	✗

© 2025 Tanium Inc. All Rights Reserved

Threat Response administration and platform content permissions (continued)

Permission	Permission Type	Threat Response Administrator[1]	Threat Response Operator	Threat Response User	Threat Response Read Only User	Threat Response Endpoint Configuration Approver
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ WRITE	✗	✗
Dashboard	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Dashboard Group	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✓ READ	✗	✗
Package	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗
Sensor	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ	✗

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

© 2025 Tanium Inc. All Rights Reserved

Installing Threat Response

Use the **Solutions** page to install Threat Response and choose between automatic and manual configuration:

- **Automatic configuration with default settings**: Threat Response is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Threat Response, see Import Threat Response with default settings on page 153.
- **Manual configuration with custom settings**: After installing Threat Response, you must manually configure required settings. Select this option only if Threat Response requires settings that differ from the recommended default settings. For more information, see Import Threat Response with custom settings on page 154.

Before you begin

- Read the Release Notes.
- Review the Threat Response requirements on page 35.
- If you are upgrading from a previous version, see Upgrade the Threat Response version on page 154.
- If the Tanium Server uses a self-signed certificate, you must add localhost to the TrustedHostList.
- Assign the correct roles to users for Threat Response. Review the User role requirements.
    - To import the Threat Response solution, you must be assigned the Administrator reserved role.
    - To configure the Threat Response action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.

Import Threat Response with default settings

When you import Threat Response with automatic configuration, the following default settings are configured:

Default settings for Tanium Threat Response

Setting	Default value
Action group	• Restricted targeting disabled (default): `No Computers` computer group • Restricted targeting enabled: `No Computers` computer group

Tanium Signals are imported.

Tanium Managed profiles are provided that contain updated configurations. These profiles are the result of Tanium data and experience and have been designed to use settings that are considered safer and to provide more real-time visibility with Index and Recorder data. You cannot delete Tanium Managed profiles.

© 2025 Tanium Inc. All Rights Reserved

You can set the Threat Response action group to target the **No Computers** filter group by enabling restricted targeting before importing Threat Response. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Threat Response action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Tanium Console User Guide: Managing action groups. To enable or disable restricted targeting, see Tanium Console User Guide: Dependencies, default settings, and tools deployment.

To import Threat Response and configure default settings, be sure to select the **Apply Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Manage Tanium modules . After the import, verify that the correct version is installed: see Verify Threat Response version on page 155.

Import Threat Response with custom settings

To import Threat Response without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Threat Response version on page 155.

To configure the Threat Response action group, see Configure the Threat Response action group on page 157.

If Client Recorder Extension version 1.x exists on a targeted endpoint, you must remove it before you install Client Recorder Extension version 2.x tools. To target endpoints where Client Recorder Extension version 1.x exists, ask the question: `Recorder - Legacy Installed`. If the Supported Endpoints column displays **Yes**, you must remove Client Recorder Extension version 1.x from the endpoint before you install Client Recorder Extension 2.x tools. To remove Client Recorder Extension version 1.x, deploy the **Recorder - Remove Legacy Recorder [*Operating System*]** package to targeted endpoints.

Manage solution dependencies

When you start the Threat Response workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Threat Response are installed at the required versions. The Threat Response workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Threat Response, the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Threat Response and did not import all its dependencies, Tanium Console displays a banner that lists the dependencies and the required versions. For more information, see Solution dependencies.

Perform the following steps if a banner indicates any Threat Response dependencies are not installed:

1. Install the dependencies as described in Tanium Console User Guide: Import or update specific solutions.
2. From the Main menu, go to **Modules > Threat Response** to open the Threat Response **Overview** page and verify that Console no longer displays a banner to list missing dependencies.

Upgrade the Threat Response version

Upgrade Threat Response to the latest version by importing an update to the solution and migrating any existing intel.

© 2025 Tanium Inc. All Rights Reserved

IMPORTANT

In Threat Response , the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. When upgrading to Threat Response 4.0 it is only possible to upgrade from 3.8 or 3.10 to 4.0. Due to database schema changes during the migration, it is not possible to directly upgrade from Threat Response 3.7 (or earlier) to Threat Response 4.0. If you upgrade from 3.7 (or earlier) directly to Threat Response 4.0, the upgrade will fail, and you will need to recover Threat Response from a backup.

Before you upgrade, use Tanium Health Check to generate a report that you can use to resolve any issues or risks associated with the Tanium environment. Fix any issues reported by Tanium Health Check to mitigate problems that you encounter during an upgrade. You can also use this report to discover opportunities for improving the performance of the Tanium environment. For more information, see Tanium Health Check User Guide: Health Check overview.

For the steps to upgrade Threat Response, see Tanium Console User Guide: Managing Tanium solutions. After the upgrade, verify that the correct version is installed: see Verify Threat Response version on page 155.

If Tanium Reveal and Tanium Threat Response exist in the same environment, both solutions must be on a version that is running the same architecture of Tanium Index. Threat Response 3.4 and later must be installed in the same environment as Reveal 1.15 and later. Threat Response versions earlier than Threat Response 3.4 can be installed in the same environment as Reveal 1.14 and earlier.

When upgrading Threat Response, you can select to automatically upgrade the Threat Response tools package on all of the endpoints in an environment to ensure that the latest version of the Threat Response tools are distributed.

IMPORTANT

When Endpoint Change Management (ECM) is enabled, endpoint tools get upgraded according to upgrade workflows defined in Endpoint Change Management. When ECM is enabled, the option to control Threat Response tools deployment automatically or through Threat Response profile deployment is not available. Endpoint Change Management is enabled by default in Tanium Cloud and beginning with the 2024H1 Semi-Annual Release.

Verify Threat Response version

After you import or upgrade Threat Response, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Modules > Threat Response** to open the Threat Response **Overview** page.
3. To show version information, click Info .

© 2025 Tanium Inc. All Rights Reserved

Configuring Threat Response

If you did not install Threat Response with the **Apply All Tanium recommended configurations** option, you must enable and configure certain features.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.



For information about how to install Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Threat Response, see User role requirements on page 140. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.



For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings and select **Global**. For more information about action locks, see Tanium Console User Guide: Managing action locks.

For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to endpoints:

- Associating a response action with an alert
- Deleting profiles

© 2025 Tanium Inc. All Rights Reserved

- Deploying profiles
- Gathering snapshots
- Initiating on-demand scans

IMPORTANT

When Endpoint Change Management (ECM) is enabled, endpoint tools get upgraded according to upgrade workflows defined in Endpoint Change Management. When ECM is enabled, the option to control Threat Response tools deployment automatically or through Threat Response profile deployment is not available. Endpoint Change Management is enabled by default in Tanium Cloud and beginning with the 2024H1 Semi-Annual Release.

Configure Threat Response

Configure the Threat Response action group

Importing the Threat Response module automatically creates an action group to target specific endpoints. If you did not use automatic configuration or you enabled restricted targeting when you imported Threat Response, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Threat Response, configuring the Threat Response action group is optional.

Select the computer groups to include in the Threat Response action group.

BEST PRACTICE

Clear the selection for **No Computers** and make sure that all operating systems that are supported by Threat Response are included in the Threat Response action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Tanium Threat Response**.
3. Select the computer groups that you want to include in the action group and click **Save**.
   If you select multiple computer groups, choose an operator (AND or OR) to combine the groups.

When you have the **Threat Response Reputation Integrations** permission, you can auto-create Saved Questions and Connections for Tanium Reputation.

1. From the Threat Response overview page, click Settings .
2. Click **Service > Reputation** .
3. Click **Configure Reputation** to generate the saved questions and connections that are required to provide reputation intel to Threat Response.

When you click **Configure Reputation**, the following saved questions are generated:

© 2025 Tanium Inc. All Rights Reserved

- Reputation - Driver Details (SHA 256) [Tanium Default]
- Reputation - MS EXE Recently Changed [Tanium Default]
- Reputation - Windows AutoRuns (SHA 256) [Tanium Default]
- Reputation - Running Processes with Hash (SHA256) [Tanium Default]
- Reputation - Mac Autoruns (MD5) [Tanium Default]
- Reputation - Linux Autoruns (MD5) [Tanium Default]
- Reputation - Trace Executed Process Hashes (MD5) [Tanium Default]
- Reputation - Service Module Details (SHA256) [Tanium Default]
- Reputation - Loaded Modules (SHA256) [Tanium Default]
- Reputation - Recently Changed MACHO 32 Bit [Tanium Default]
- Reputation - Recently Changed MACHO 64 Bit [Tanium Default]
- Reputation - Recently Changed ELF [Tanium Default]

When you click **Configure Reputation**, the following Tanium Connect connections are generated to provide reputation intel to Threat Response:

- Reputation - Recently Changed MACHO 64 Bit [Tanium Default]
- Reputation - Recently Changed ELF [Tanium Default]
- Reputation - Recently Changed MACHO 32 Bit [Tanium Default]
- Reputation - Trace Executed Process Hashes (MD5) [Tanium Default]
- Reputation - Loaded Modules (SHA256) [Tanium Default]
- Reputation - Service Module Details (SHA256) [Tanium Default]
- Reputation - Linux Autoruns (MD5) [Tanium Default]
- Reputation - Mac Autoruns (MD5) [Tanium Default]
- Reputation - Running Processes with Hash (SHA256) [Tanium Default]
- Reputation - MS EXE Recently Changed [Tanium Default]
- Reputation - Windows AutoRuns (SHA 256) [Tanium Default]
- Reputation - Driver Details (SHA 256) [Tanium Default]

Clicking **Configure Reputation** does not recreate any existing connections or saved questions. If any connections or saved questions do not exist in the environment, they are created. Saved questions are recreated when the Threat Response service is restarted.

Set up Threat Response users

You can use the following set of predefined user roles to set up Threat Response users.

© 2025 Tanium Inc. All Rights Reserved

To review specific permissions for each role, see User role requirements on page 140.

IMPORTANT

On installation, Threat Response creates a **Threat Response** user to automatically manage the Threat Response service account. Do not edit or delete the **Threat Response** user.

For more information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

Threat Response Administrator

Assign the **Threat Response Administrator** role to users who manage the configuration and deployment of Threat Response functionality to endpoints.
This role can perform the following tasks:

- Configure Threat Response service settings
- Read and modify Threat Response configurations
- Take action on alerts
- Connect to remote endpoints
- Dismiss or reject approvals for Threat Response tasks in Tanium Endpoint Configuration

Threat Response Operator

Assign the **Threat Response Operator** role to users who manage the configuration and deployment of Threat Response functionality to endpoints.
This role can perform the following tasks:

- Configure Threat Response service settings
- Read and modify Threat Response configurations
- Take action on alerts
- Connect to remote endpoints
- Dismiss or reject approvals for Threat Response tasks in Tanium Endpoint Configuration

Threat Response User

Assign the **Threat Response User** role to users who work with alerts and performing analysis on remote endpoints.
This role can perform the following tasks:

- View service settings
- View and modify alerts and intel documents
- Suppress and take action on alerts
- Run and review on-demand scans
- Connect to remote endpoints and manage downloads from them, and read configurations and profiles

© 2025 Tanium Inc. All Rights Reserved

Threat Response Read Only User

Assign the **Threat Response Read Only User** role to users who need visibility into Threat Response data and Threat Response findings on endpoints.
This role can perform the following tasks:

- View service settings, alerts, and intel documents
- Review on-demand scans
- Read connections to remote endpoints
- Read configurations and profiles

Threat Response Endpoint Configuration Approver

Assign the **Threat Response Endpoint Configuration Approver** role to a user who approves or rejects Threat Response configuration items in Tanium Endpoint Configuration.
This role approves, rejects, or dismisses changes that target endpoints where Threat Response is installed.



Do not assign the **Threat Response Service Account** and **Threat Response Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Select a language

Select one of the supported languages for the Threat Response workbench and Threat Response user guide, as described in Tanium Console User Guide: Reference: Language support.

© 2025 Tanium Inc. All Rights Reserved

Getting started with Tanium™ Threat Response

Threat Response provides common configuration workflows to expedite the time to value and to simplify the initial configuration experience. Configuration workflows that target specific end-to-end scenarios ease the implementation of Threat Response without the need for comprehensive knowledge of the full functionality of the module. Initial configuration is not intended to replace existing workflows, but instead provide a path for configuring the operation of Threat Response as quickly as possible without having extensive Tanium experience or subject matter expert guidance. Configuration workflows also provide a sample of the functionality of Threat Response and the different types of scenarios that are possible.

The following read permissions are required to view the configuration workflows on the Threat Response overview page:

- Threat Response Profiles
- Threat Response Configs
- Threat Response Live Response Destinations
- Threat Response Quarantine Profile
- Threat Response Labels
- Threat Response Sources
- Threat Response Intel

These permissions are granted to Threat Response Administrators by default.



Configuration workflows only appear to new users of Threat Response. If you are an existing user, Click **Customize Page** at the top of the Overview page of the Threat Response workbench, select **Configuration**, and click **Save** to view the configuration workflows.

Threat Response provides configuration workflows for the following functional areas:

- Evidence and telemetry
- Alerting and detection
- Endpoint isolation
- Incident response automation
- SIEM integration

On the overview page, click **Next** to navigate through the provided workflows. After you navigate to any specific workflow, the navigation item becomes a link that you can use to go to the workflow directly. Click **Previous** to move to the previous workflow.

Evidence and telemetry

The evidence and telemetry section contains workflows for the configuration of Threat Response profiles and Live Response.

© 2025 Tanium Inc. All Rights Reserved

Profiles

Profiles are a collection of intel documents and settings that are distributed to endpoints. Threat Response uses a cascading model when deploying profiles to endpoints. For example, the profile with the highest priority targets endpoints with low resources, followed by more distinct categories of Windows domain controllers, servers, and workstations to ensure both broad coverage and optimal performance. The displayed profiles are Tanium Managed profiles. For more information on Tanium Managed profiles, see Tanium Managed profiles.

Live Response

Live Response enables you to collect specific information from endpoints to use for forensic analysis, data correlation, and to investigate potentially compromised systems with a customizable and extensible framework. You can specify a network location to transfer data that you collect.

Profiles



Initial configuration is not intended to replace existing workflows. For more information about profile configuration, see Profiles. The displayed profiles are Tanium Managed profiles. For more information on Tanium Managed profiles, see Tanium Managed profiles.

1. From the Main menu, go to **Modules** > **Threat Response** > **Evidence and Telemetry** > **Profiles**.
2. Select to **Enable** or **Disable** any displayed profile. If you disable a profile that is currently enabled, you must save and deploy the changes to the targeted endpoints. When you **Disable** a profile, the targeting for that profile is made such that it is not applicable to any endpoints. The targeted Computer Groups that you have assigned to that profile are not changed, however it is not deployed to endpoints that are included in those Computer Groups. For example, `Profile A` targets the `All Windows` Computer Group. If you disable `Profile A`, it still appears to target the `All Windows` Computer Group, but it is not deployed to those endpoints. Any endpoints that are targets of a disabled profile move to their next applicable enabled profile based on priority. Any configurations deployed by the profile before it was disabled are removed if no profile is currently applicable. If you switch a deployed profile from enabled to disabled you are prompted to deploy the profile so the change can take effect. Intel documents that are associated with a disabled profile are deployed along with intel documents that are associated with enabled profiles. If you make changes to the detection configuration that is assigned in a profile, and enable and deploy the profile, the previous set of intel is applied. When you deploy new intel, it becomes applied.
3. Click **Edit** to make changes to a profile.
4. In the Index Configuration section, you can select the hashes that you want to calculate for each file in disk to allow you to quickly search across all file systems, the frequency to receive updates for files in certain regions of the disk, the frequency to scan the entire disk on an endpoint, and the delay time after Index starts before starting the initial index scan.

   High Priority Path

   Use high priority path scanning to receive more frequent updates for files in certain regions of the disk. In addition to the baseline disk scan, you can specify high priority paths that use recorder events to update data. High Priority Paths are indexed more frequently. Performance impacts on the endpoint increase with the frequency of indexing

© 2025 Tanium Inc. All Rights Reserved

and the size of the path. Using the root directory as a High Priority Path is discouraged as this can quickly consume resources.

Scan Frequency

Threat Response uses Tanium Index to scan the entire disk on an endpoint at regular intervals that typically occur between once a day and once a week. Index does not use recorder events to update file data across the entire disk. Enter a value for how often the Index scan runs.

Scan Distribution

The delay time after Index starts before starting the initial index scan. This time is randomized over a 24 hour period.

For more information about Index configurations, see Index configurations.

5. In the Recorder Configuration section, you can add and remove the historical events Threat Response stores locally on the endpoint for triage and investigation. An exhaustive reference for event types is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click the help icon from the Threat Response overview page and click the **Recorder Security Event Details** tab. For more information on recorder configurations and events, see Recorder configurations.
6. In the Recorder Configuration section, you can view the number of active filters that are associated with the configuration. Click the number of filters to view all the existing filters to see which individual filters are applied. For more information on filters, see Filters.

Live Response



Initial configuration is not intended to replace existing workflows. For more information about Live Response, see Collecting data from endpoints.

1. From the Main menu, go to **Modules** > **Threat Response** > **Evidence and Telemetry** > **Live Response**.
2. In the Destinations row, click **Create** to create a destination. For more information on destinations and a procedure for creating a destination, see Destinations.

   You must create an external destination to use Live Response.
3. In the Collections row, click **Create** to create a collection. Collections are pre-defined common triage artifact captures. For more information on collections and a procedure for creating a collection, see Collections.
4. In the File Collector Sets row, click **Create** to create a file collector set. File Collector Sets enable you to use Live Response to capture any arbitrary file for your review. For more information on File Collector Sets and a procedure for creating a File Collector Sets, see File collector sets.

© 2025 Tanium Inc. All Rights Reserved

5. In the Script Sets row, click **Create** to create a Script Set. Script Sets enable you to use PowerShell and Python scripts to programmatically collect triage evidence. For more information on Script Sets and a procedure for creating a Script Set, see Script sets.

Alerting and detection

The alerting and detection section contains workflows for configuring intel documents and subscriptions to third-party threat intelligence data, and Tanium Signal Intel documents. Extended detections include intel documents for Deep Instinct, Microsoft Defender, Process Injection, and Reputation.

Extended detections



Initial configuration is not intended to replace existing workflows. For more information about Intel, see Intel.

1. From the Main menu, go to **Modules** > **Threat Response** > **Alerting and Detection** > **Detections**.
2. (Optional) For **Tanium Signals**, select to distribute the **Initial Set** or **All Signals**. The **Initial Set** of signals is a set of Tanium Signals that are curated and tested to ensure fewer false positive alerts. Tanium Signals in the **Initial Set** are assigned to the detection configuration in the profile that Threat Response deploys to endpoints and these signals have the **Tanium Initial Intel** label applied. Select **All Signals** to assign all Tanium Signals to the detection configuration in the profile that Threat Response deploys to endpoints. The **All Signals** option provides a more exhaustive set of alerts at the expense of more attentive analysis of the alerts that are generated. For more information on Tanium Signals, see Tanium Signals.
3. (Optional) For **Process Injection**, select **Enable** or **Disable**. Enable Process Injection to deploy the Process Injection intel document to endpoints that are targeted by the Threat Response profile. The Process Injection intel document provides a way to alert on incidents that involve techniques such as process injection and credential dumping. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select the profiles to which you want to apply Process Injection. For more information on Process Injection, see Process Injection.
4. (Optional) For **Reputation**, select **Enable** or **Disable**. Enable Reputation data to gain insight into which alerts might be good candidates to save for further analysis and action. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select the profiles to which you want to apply Reputation. For more information on Reputation, see Reputation. Reputation requires either a configuration with a reputation provider, or that malicious and non-malicious hashes be added to Reputation manually.
5. (Optional) For **Defender**, select **Enable** or **Disable**. Enable Microsoft Defender to gain visibility into common areas of Windows for changes which might have been caused by spyware, malware, and general security events. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select the profiles to which you want to apply Defender. For more information on Defender, see Defender. Defender requires Defender AV to be installed and running on the endpoint.
6. (Optional) For **Deep Instinct**, select **Enable** or **Disable**. Enable Deep Instinct to apply deep learning and adds next-generation AV capabilities to Threat Response by integrating the investigative abilities of Threat Response to Deep

© 2025 Tanium Inc. All Rights Reserved

Instinct alerts. If you select **Disable**, you can save and optionally deploy the changes to the profile to endpoints. Click Edit to select the profiles to which you want to apply Deep Instinct. For more information on Deep Instinct, see Deep Instinct. Deep Instinct must be installed and running on the endpoint.

3rd party intel feeds

1. From the Main menu, go to **Modules** > **Threat Response** > **Alerting and Detection** > **3rd Party Intel Feeds**.
2. Click **Create**. An intel source is a series of intel documents from an external source. Sources can be a vendor or a folder in your network. You can import sources manually or based on subscription settings.
3. Subscribe to 3rd party intel feeds. For more information on subscribing to 3rd party intel feeds, see Intel.
4. If you create one or more 3rd party intel feed subscriptions, you can click **View** to review the details of the subscriptions.

Endpoint isolation

The endpoint isolation section contains workflows for configuring the quarantine of a Windows, Linux, or Mac endpoint that shows evidence of compromise or other suspicious activity. When an endpoint is quarantined, traffic that is allowed on the quarantined endpoint is between the Tanium Client on the quarantined endpoint and Tanium Server over port 17472. Additionally, you can Direct Connect to the endpoint and use Live Response destinations.



Initial configuration is not intended to replace existing workflows. For more information about Quarantine, see Quarantining endpoints.

Tanium default quarantine profile

1. From the Main menu, go to **Modules** > **Threat Response** > **Endpoint Isolation** > **Tanium Default Quarantine Profile**.
2. Click edit to edit specific values in the Default Quarantine Profile.
3. Specify the allowances that you want to enable. The allowances that you select enable various types of traffic. You can select:
    a. **All DHCP** - Allows DHCP traffic to any destination.
    b. **DNS** - Allows DNS traffic to any destination when you select All. Allows DNS traffic only to the DNS servers currently configured on the endpoint being quarantined when you select **Current Only**.
    c. **Direct Connect** - Allows Direct Connect to access quarantined endpoints.
    d. **Live Response** - Allows Live Response to collect data from quarantined endpoints.
4. Click **Save and Deploy** to make any changes to the Tanium Default Quarantine Profile. For more information on the Tanium Default Quarantine Profile, see Quarantining endpoints.

© 2025 Tanium Inc. All Rights Reserved

Create quarantine profile

1. From the Main menu, go to **Modules** > **Threat Response** > **Endpoint Isolation** > **Create Quarantine Profile**.
2. Click **Create**. For a detailed overview of profile creation, see Quarantining endpoints.

Incident response automation

The incident response automation section contains workflows for managing and creating automated responses to alerts that result from an intel match. You can manage automated reactions to delete files, kill responsible processes, and quarantine endpoints. Additionally, you can create playbooks for Tanium Automate.



Initial configuration is not intended to replace existing workflows. For more information about reactions, see Creating reactions.

Tanium default alert reactions

1. From the Main menu, go to **Modules** > **Threat Response** > **Incident Response Automation** > **Tanium Default Alert Reactions**.
2. View the default reactions. Reactions automate one or more actions on an endpoint based on alerts from intel documents. For example, delete one or more files, kill a process, or quarantine an endpoint.
3. View the intel documents that are associated with each reaction. The associated intel documents are the documents that initiate the reaction if the intel definitions they contain are matched on an endpoint.
4. (Optional) Click **View** to view the reactions page in the Threat Response workbench to view all reactions.

Endpoint reactions

1. From the Main menu, go to **Modules** > **Threat Response** > **Incident Response Automation** > **Endpoint Reactions**.
2. Click **Create**.
3. The reactions page in the Threat Response workbench appears. For more information about creating reactions, see Creating reactions. After creating a new reaction, you must associate that reaction with an Intel Document.

Automate playbooks

1. From the Main menu, go to **Modules** > **Threat Response** > **Incident Response Automation** > **Automate Playbooks**.
2. Click **Create**.
3. The create playbook page in the Automate workbench appears. For more information about creating playbooks, see Tanium Automate User Guide: Building playbooks.

© 2025 Tanium Inc. All Rights Reserved

SIEM integration

The SIEM (Security Information and Event Management) integration section contains workflows for adding stream configurations to profiles that you can use to stream recorder data to external sources that includes process, network, file, driver events. You can use stream data to investigate incidents, enrich other workflows, or perform custom analytics. Stream configurations enable you to specify and filter recorder events for the endpoints in an environment, and provide instructions for exporting or streaming these events directly to an SIEM for analysis in JSON format. Additionally, you can create workflows to send alert and audit data to a SIEM using Tanium Connect.



Initial configuration is not intended to replace existing workflows. For more information about stream configurations, see Create stream configurations. For more information about setting up alert forwarding in Tanium Connect, see Set up Tanium Connect forwarding. For more information about sending audit logs to a SIEM, see Tanium Connect User Guide: Managing connections.

Send stream data to SIEM

1. From the Main menu, go to **Modules** > **Threat Response** > **SIEM Integration**.
2. (Optional) Click **Create**. For more information on creating Stream configurations, see Create stream configurations.
3. Once you have created one or more stream destinations, for each profile, select a Stream configuration to apply to the profile. The available configurations that you can add are listed in the dropdown list. To create a new Stream configuration, click **Create**. If you do not include a Stream configuration, no data is streamed to a destination outside of Tanium.

Send alerts to SIEM

1. From the Main menu, go to **Modules** > **Threat Response** > **SIEM Integration > Send Audit Logs and Alerts to SIEM**.
2. Click **Create**. For more information about setting up alert forwarding in Tanium Connect, see Set up Tanium Connect forwarding.

Send Audit Logs to SIEM

1. From the Main menu, go to **Modules** > **Threat Response** > **SIEM Integration > Send Audit Logs and Alerts to SIEM**.
2. Click **Create**. For more information about sending audit logs to a SIEM, see Tanium Connect User Guide: Managing connections.

© 2025 Tanium Inc. All Rights Reserved

Adding intel

Intel defines one or more conditions that might indicate malicious behavior on endpoints. Threat Response can leverage multiple sources of intel to identify and alert on potential threats in an environment. In addition to supporting third-party intelligence sources, Tanium provides threat intelligence called Signals. Intel documents and Signals, generally referred to as intel, interact with Threat Response to provide comprehensive monitoring and alerting.

Some intel document types, such as OpenIOC, STIX, CybOX, and YARA, search against existing or historical artifacts on the endpoint. There are a number of providers for these documents. You can upload them directly or configure source streams. Both the 1.0 and 1.1 versions of OpenIOC are supported. CybOX 2.1 is the currently supported version. The current supported version of STIX is 1.2. STIX 2.0 is required for TAXII 2.0 support. Consequently, TAXII 2.0 is not currently supported. YARA 4.5.0 is supported and support for the following default modules is provided: pe, elf, dotnet, hash, cuckoo, math, magic, macho, dex, string, and time.



Always use mutual (two-way) authentication and TLS encryption when connecting to intel feeds. Two-way authentication and data encryption provide additional privacy-related benefits, for example, ensuring that encryption keys that become compromised cannot decrypt TLS communications that were recorded in the past.

Signals

Signals provide real-time monitoring of endpoint telemetry events; for example, process, network, registry, and file events for malicious behaviors and methodologies of attack. Unlike other static forms of intel which focus on specific indicators, Signals are evergreen heuristics; they are perpetually relevant.

Signals interact with the engine differently; they can evaluate continuously with the recorder and match on live process events on endpoints. Signals help to identify malicious activity by correlating events and searching for behavior-based indicators that something is awry. You can use Signals as a source directly from Tanium, or you can write your own Signals. See Reference: Authoring Signals for more information.



Adding Signals to an intel configuration enables the recorder process on endpoints, and loads the Tanium audit rules. This happens even if you do not enable a recorder configuration.

When a Signal evaluates with the recorder database and an event matches, the resulting alert shows the context of the match. If you have filters for specific events in a recorder configuration, signals that match the events can still generate alerts. For a Signal to evaluate with the recorder database, you need to enable both intel and recorder configurations in an active profile.

The events of a Signal match are always written to the database, and override any filters that are included in a recorder configuration.

© 2025 Tanium Inc. All Rights Reserved

An exhaustive reference to Signals syntax - including supported objects, properties, and conditions - is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click from the Threat Response overview page and click the Threat Response Intel Support tab.

Signals do not always evaluate with the recorder database

There are times when Signals cannot be evaluated with the recorder database. For example, it is possible for the recorder to generate Signals, but not record them in the recorder database. Additionally, there are cases where events have been recorded, but one or more of the events in the Signal match occurred too far in the past that the event has been purged from the recorder database.

Threat Response integrates with third-party reputation services. Hashes are sent to the reputation service for assessment, then Threat Response enhances intel with the hash ratings. The **Definition** and **Engine Analysis** tabs on the Intel details page provide additional information about how the intel document is structured, which parts are applicable, and the hash rating.

Intel safeguards

Poorly tested or low-fidelity intel can cause a rapid influx of false-positive alerts that can be time consuming to review. By evaluating the fidelity of intel documents and disabling intel documents that generate high volumes of alerts, Threat Response can provide safeguards which help reduce false positive matches that overwhelm analysts. Intel safeguards provide the option to set thresholds across the environment for intel and to suppress intel that generates amounts of alerts that exceed the thresholds.

There are two types of thresholds that you can set; a per-endpoint alert rate before Threat Response disables the intel that initiated the alert, and a maximum percentage of disabled endpoints before Threat Response disables the intel document that initiated the alert.

Intel Safeguards is designed to only occur on Intel that is already being throttled. It only shuts down intel that is repeatedly and continuously throttled. Adjusting throttle settings impacts Intel safeguard settings.

1. From the Main menu, go to **Modules > Threat Response** . Click Settings .
2. Click **Service > Intel**.
3. In the **Intel Safeguards** section, enable or disable the **Intel Safeguards** setting. Enabling this setting causes intel documents that initiate a volume of alerts to become disabled. Default: Enabled.
4. In **Endpoint Safeguard Setting**, specify a number of throttle events that must occur in a time period for the intel document that is initiating the alerts to be disabled on the endpoint where alerts are being initiated. Default: 2 throttle events in 120 minutes. By default, individual endpoints throttle alerts for one hour if an Intel document alerts five times in five minutes. If this happens twice in a row, Intel Safeguards disables that intel document on that specific endpoint. Alerts from all other endpoints continue to be received.
5. In **Global Safeguard Setting**, set a threshold for continually throttled events across the enterprise that must occur for an intel document to be disabled. For example, if an intel document, at the service level, throttles 250 events consecutively, that intel document is disabled. Default: 250. By default, the service begins throttling alerts if an Intel document has more

© 2025 Tanium Inc. All Rights Reserved

than 100 alerts in 20 minutes. If the number of alerts continues above this level, and the service counts 250 additional continuously throttled alerts after the throttle is initiated with no break in the throttling, Intel Safeguards will shut down that intel document across the entire environment.

You can disable Intel Safeguards for individual intel documents of the following types: Open IOC, YARA, STIX, and Signals that are part of the Tanium Signal feed.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. In the **Advanced Settings** section, deselect **Set to Active**.

In the Intel page of the Threat Response workbench, you can filter for intel documents that have the following states of intel safeguards:

Enabled

This designation is assigned to any intel documents that are not assigned another state.

Reduced

This designation is assigned to intel documents that any single endpoint has disabled. The result of an intel document being assigned this designation is that it no longer provides the complete visibility expected from a high-fidelity intel document. A system notification appears in the audit browser to show which endpoints are in a reduced state.

Disabled

This designation is assigned to intel documents that are disabled enterprise-wide. Such intel documents have initiated alerts that have throttled over 250 times. 250 is a default value that you can configure to a more appropriate value for an environment. Intel documents with this designation require tuning and reevaluation to be effective.

Pending

This designation is for new or recently modified intel documents that have not been deployed and consequently have no basis for any other designation. If intel is deployed, but the intel document is not applicable to any endpoints, it continues to display as Pending indefinitely. Intel must be included in a Detection configuration to be applied to an endpoint. If an Intel document does not move to a Reduced or Disabled status, Intel remains in a pending state for up to two hours (by default) after Intel is deployed before moving to an Enabled state. This two hour timeframe is based on the Endpoint Safeguard Setting, which is 120 minutes by default.

No Safeguards

This designation means that automatic management of Enabled, Reduced, or Disabled states is turned off for an Intel document. This designation can be only for a specific intel document, or it could be turned off for the entire environment.



You can re-enable Intel documents after they have become disabled or reduced by updating the intel document and deploying to reset the state. Saving any changes to the name, any suppression rules, or edits to the definition, or labels associated with the intel document constitute a change. Alternatively, you can also turn

© 2025 Tanium Inc. All Rights Reserved

NOTE

off safeguards for an individual document and redeploy intel to re-enable a reduced or disabled document. To re-enable all disabled intel documents, disable the **Intel Safeguards** setting in the **Intel Safeguards** section from the Settings available from the Threat Response overview page.

Configure intel sources

An intel source provides a set of intel documents from an external source. Sources can be a vendor or a folder in your network. You can import sources manually or use sources that are based on subscription settings.

Intel sources are updated from the Threat Response service, which runs on the Module Server. If security software is deployed in the environment to monitor and block unknown URLs, your security administrator must allow the intel provider URLs on the Module Server.

Threat Response can use several data formats, with the following available source types:

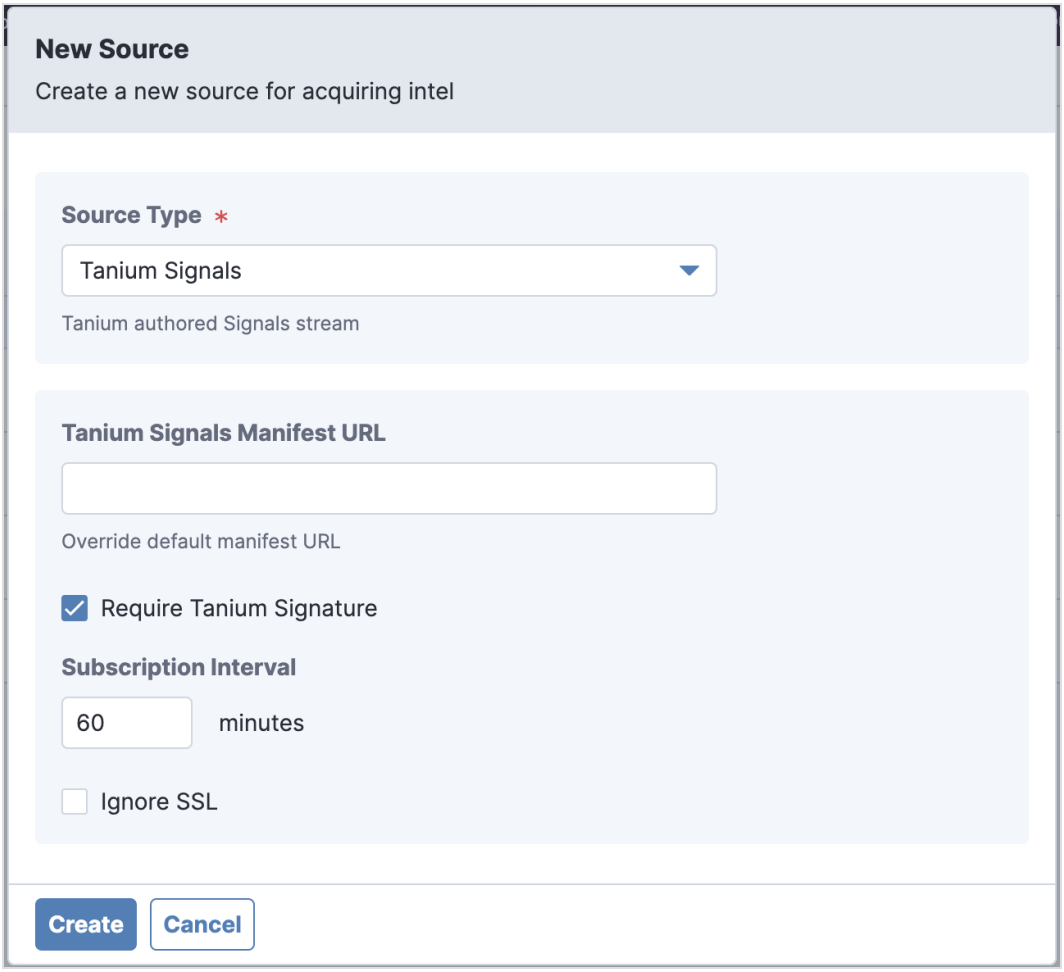
- Tanium Signals feed
- iSIGHT Partners ThreatScape
- Trusted Automated eXchange of Indicator Information (TAXII™)
- Palo Alto Networks Wildfire
- Folders on the Tanium Module Server

Connect to the Tanium Signals feed

The Tanium Signals feed provides a stream of regularly updated Signals that are designed to detect common patterns of attack on Windows endpoints. Each Signal is mapped to one or more categories in the MITRE ATT&CK Framework.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Threat Response > Intel > Sources** . Click **Create**.
2. From the **Type** drop-down menu, select **Tanium Signals**.



3. (Optional) If you do not want to use the default feed, enter a different content manifest URL. Use this field for testing beta Signals in non-production environments. If you require support for a different feed, see Contact Tanium Support on page 377.
4. Select **Require Tanium Signature** to only use Tanium-verified Signals.
5. Select the **Subscription Interval**, in minutes.
6. (Optional) Click **Ignore SSL** to skip the certificate validation.
7. Click **Create**.

When the Tanium Signals feed gets updated, system notifications get generated that include the release notes about the updates.

© 2025 Tanium Inc. All Rights Reserved

Configuring Tanium Signals feed in an airgapped environment

To configure the Tanium Signals feed in an airgapped environment on the Tanium Appliance, see Reference: Air gap support: Install or update Tanium Threat Response Signals.

If you are using one of the following versions of Threat Response, download Tanium Detect Signals v4:

- Threat Response version 3.10.59 or later 3.10 versions
- Threat Response version 4.0.1116 or later 4.0 versions
- Threat Response version 4.2.29 or later 4.2 versions
- Threat Response version 4.3.176 or later

If you are using Threat Response version 1.4 to any earlier 3.10, 4.0, 4.2, or 4.3 than listed above, download Tanium Detect Signals v3.

To deploy signals in an airgapped environment, navigate to https://content.tanium.com/files/misc/ThreatResponse/ThreatResponse.html and download Tanium Detect Signals from a computer that can access the internet. If you encounter a problem, see Contact Tanium Support on page 377.

When the download completes, host the .ZIP file on a Web server that is accessible by Threat Response. You can use the Tanium server to host this content. When this content is hosted, follow the instructions for connecting to the Tanium Signals feed.

For example, you can save the .ZIP file in a sub directory of the Tanium Server HTTP directory named `signals`. In this example, the URL to use when you create the signals feed is:

```
https://my.tanium.server/signals/DetectSignals.zip
```

In this scenario, content downloads directly from the Tanium Server, so the **Require Tanium Signature** option should be deselected. If the environment uses self-signed certificates select the **Ignore SSL** option.

All downloads of signals are logged on the module server.

Connect to iSIGHT Partners ThreatScape

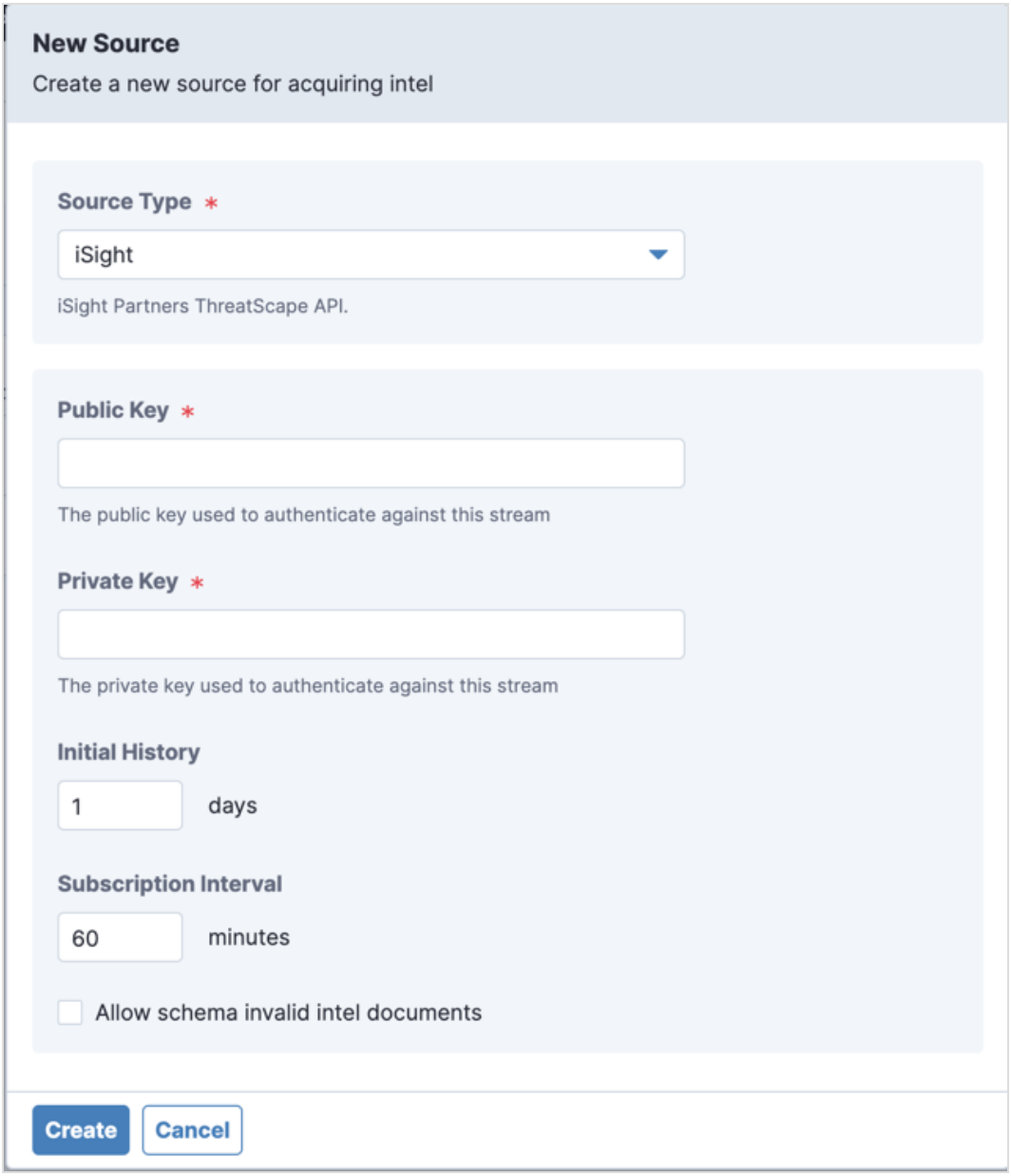
The iSIGHT intelligence is always in STIX format. You can have only one stream of this type at a time.



You must have an iSight subscription. The current supported version of STIX is 1.2. STIX 2.0 is required for TAXII 2.0 support. Consequently, TAXII 2.0 is not currently supported.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Threat Response > Intel > Sources**. Click **Create**.
2. From the **Type** drop-down menu, select **iSight**.



3. Paste the public and private key for your subscription.
4. Select the **Initial History** in days, and the **Subscription Interval** in minutes.
5. (Optional) Click **Allow schema invalid documents** to enable the import of intel that might be formatted incorrectly. Invalid documents show a warning next to their type on the individual intel page.
6. Click **Create**.

© 2025 Tanium Inc. All Rights Reserved

Connect to a TAXII server

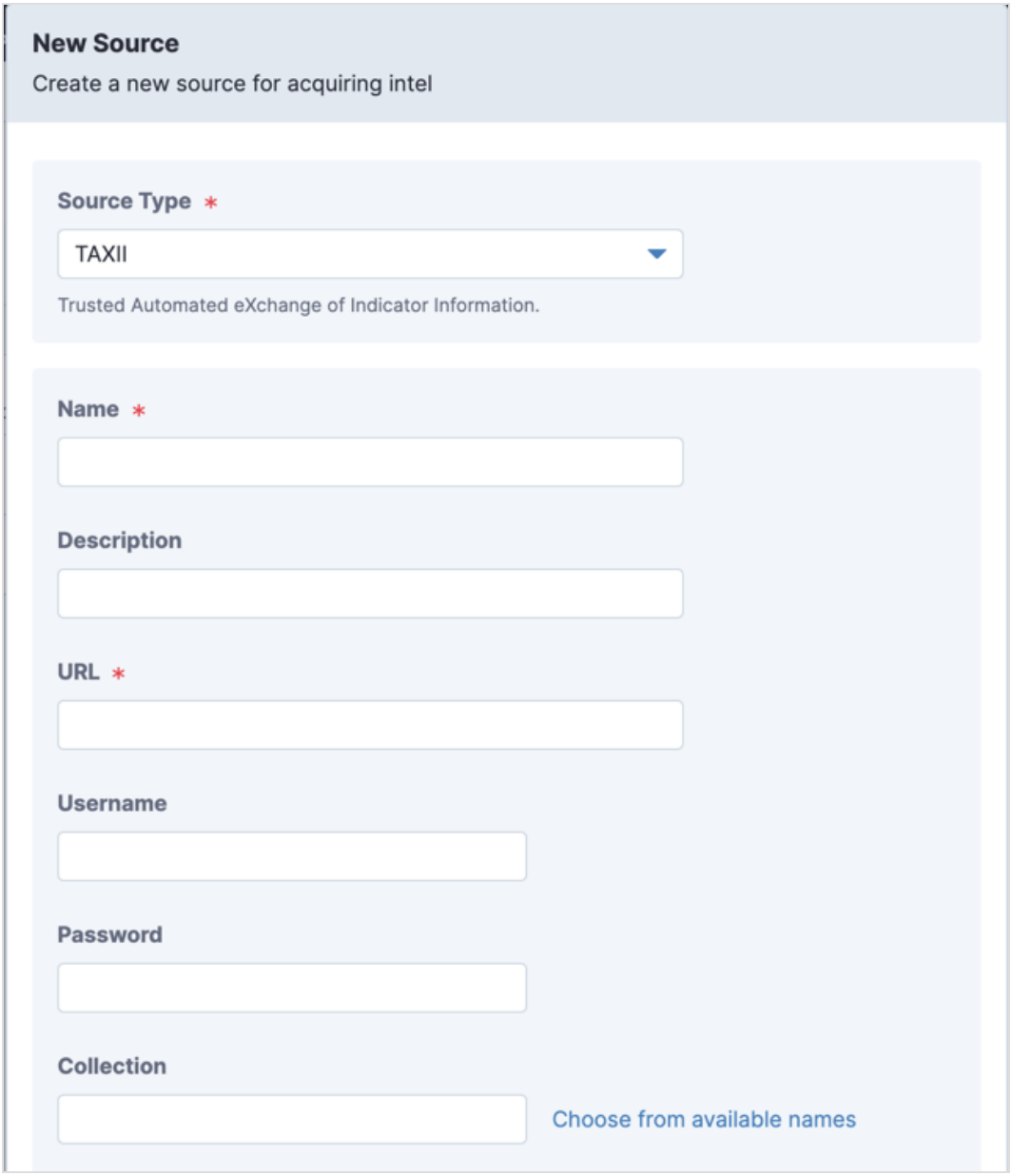
TAXII intelligence is always in STIX format. Unlike other streams, TAXII also sorts intel documents into collections, and a document only appears in one collection. Configure a source for each collection. Tanium does not support Subscription Based TAXII Servers; TAXII servers must be collection based.



The current supported version of STIX is 1.2. STIX 2.0 is required for TAXII 2.0 support. Consequently, TAXII 2.0 is not currently supported.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Threat Response > Intel > Sources**. Click **Create**.
2. From the **Type** drop-down menu, select **TAXII**.



3. Add a name and description.
4. Add subscription details including the URL, user name, and password. If you edit user name or password, you have to enter data for both fields.
5. Type in the case-sensitive collection name or select from available collections.
6. Select the **Initial History** in days, and the **Subscription Interval** in minutes.

© 2025 Tanium Inc. All Rights Reserved

7. Make optional security selections.
    a. If you want two-way SSL validation, paste the certificate and private key for your subscription.
    b. Click **Ignore SSL** to skip the certificate validation.
8. (Optional) Click **Allow schema invalid documents** to enable the import of intel that might be formatted incorrectly. Invalid documents show a warning next to their type on the individual intel page.
9. Click **Create**.

Set up Connect and Wildfire



The Palo Alto Networks Wildfire connection source is deprecated. Customers who need to integrate Palo Alto Networks WildFire and Tanium Threat Response should configure the Tanium Reputation source instead. For more information, see Tanium Reputation User Guide: Configure Palo Alto Networks WildFire reputation source.

For more information on configuring the reputation service, see Set up the reputation service.

Use a local directory or remote share

Stream intel from a set of local directories on the Module Server. The System Administrator for the computer where the Module Server is hosted must authorize a directory for streaming.

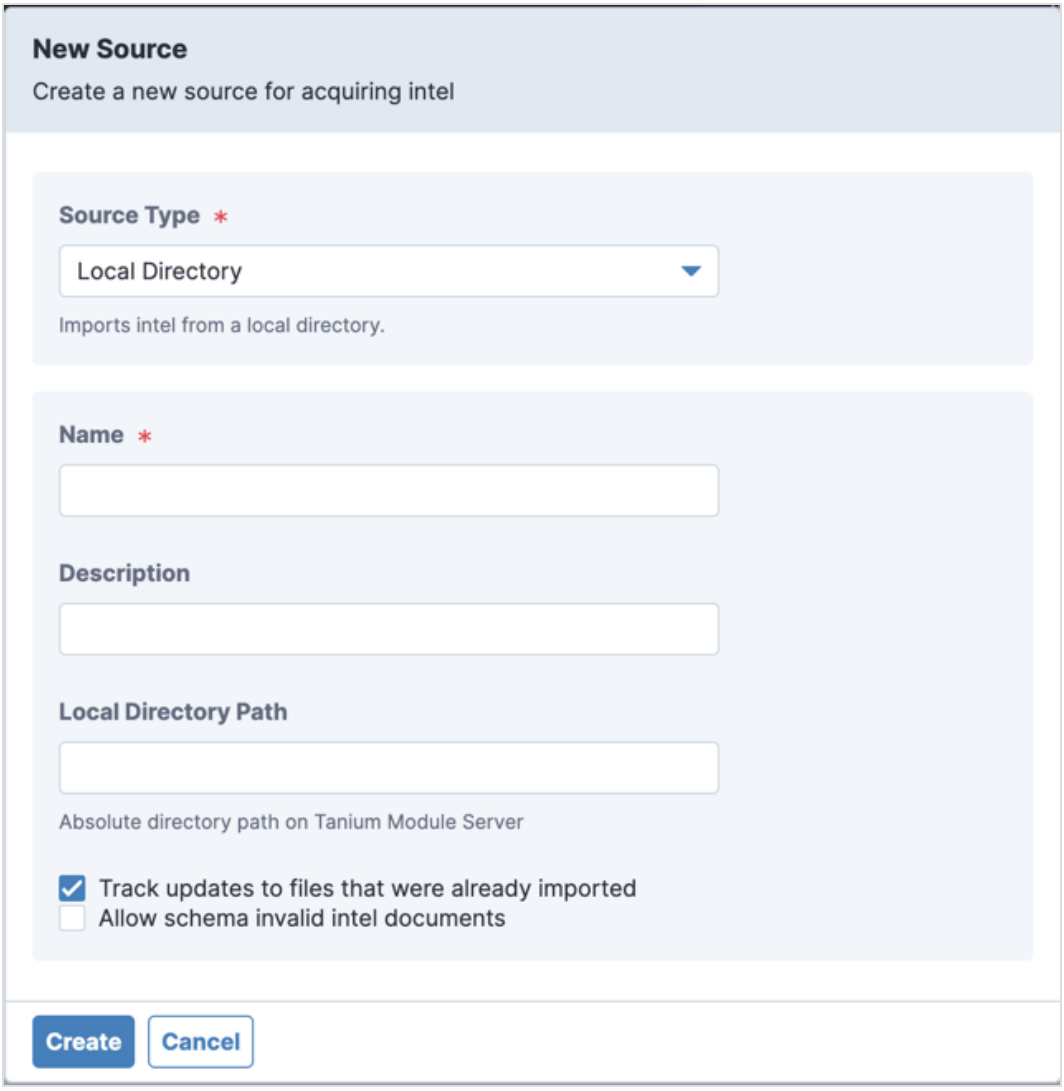


In Threat Response 4.0 and later, local directories on the Module Server are no longer stored in the `folder-stream-roots.conf` file. All directory content is stored in the Threat Response database and all paths in the database are editable by using API routes. The API routes to view, add, or replace paths are available to users with the Tanium Administrator role. Any existing paths in the folder-stream-roots.conf file will be migrated to the Threat Response database when upgrading to Threat Response 4.0 from earlier versions.

To view the allowed paths, use the `GET source-types/folder/allowed-roots` route. To add or replace paths use the `PUT source-types/folder/allowed-roots` route. Both routes are only available to users who are assigned the Tanium Administrator role. For more information on using the Threat Response API, click **Help > API > See API documentation** from the Threat Response workbench.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Threat Response > Intel > Sources**. Click **Create**.
2. From the **Type** drop-down menu, select **Local Directory**.



3. Add a name and description.
4. In the **Local Directory Path** field, specify the absolute directory path on the Module Server. The folder must be explicitly authorized for stream activity.
5. (Optional) Disable update tracking for imported files.
6. (Optional) Click **Allow schema invalid documents** to enable the import of intel that might be formatted incorrectly. Invalid documents show a warning next to their type on the individual intel page.
7. Click **Create**.

To mount a file share on a Tanium Appliance, see Tanium Core Platform Installation Guide: Server Proxy Settings. After configuring the Detect file share mount, use the absolute path value `/opt/mounts/detect` as the **Local Directory Path**.

© 2025 Tanium Inc. All Rights Reserved

If you edit an existing source, for example, by adding subscription choices, Threat Response indexes and downloads new intel documents every 60 seconds. The intel gets pushed to the endpoint during the next intel publication interval.

For more information about registry settings to use sources with a proxy server, see the Tanium Core Platform Installation Guide: Server Proxy Settings.

Delete an intel source

When you delete an intel source, all intel documents that are associated with the source are moved to the **Orphaned** source. The **Orphaned** source is not displayed on the sources page. To identify intel documents associated with the **Orphaned** source, you can filter all intel. Alerts that are associated with the intel from the source you are deleting are not deleted.

1. From the Main menu, go to **Modules > Threat Response > Intel > Sources**.
2. Click the intel source that you want to delete.
3. Click Delete. Confirm that you want to delete the intel source.

Any intel documents that were associated with the source you deleted are now associated with the **Orphaned** source. To manage intel in the **Orphaned** source, see View orphaned intel documents.

Configure process injection

The Process Injection intel document provides a way to alert on incidents that involve techniques such as process injection and credential dumping. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process can allow access to the memory of the process, system and network resources, and possibly elevated privileges. Process injection can also evade detection from security products since the execution is masked under a legitimate process. In the context of process injection, the actor identifies the process or file that performs the process injection. The target identifies the artifact that has been the subject of injection.



Process injection monitoring is not supported on Windows 8.1 and Windows Server 2012 R2 and earlier.

The Tanium Driver can monitor specific Windows API calls by injecting into user processes and kernel callbacks. The Tanium Driver can detect process injection and enable you to configure which process injection techniques result in an alert.

There are several techniques for process injection for which the Tanium Driver can monitor.

Process injection techniques

Technique	Description
Asynchronous Procedure Call	A process injection technique where an asynchronous procedure call executes memory that has potentially been created or modified in a malicious manner.

© 2025 Tanium Inc. All Rights Reserved

Process injection techniques (continued)

Technique	Description
Asynchronous Procedure Call Write	A process injection technique where an asynchronous procedure call writes to remote memory. For example, an asynchronous procedure call is queued to execute memset.
Atom Bombing	A process injection technique where an asynchronous procedure call is queued to write to memory through GetGlobalAtomName.
Callback Overwrite	A process injection technique that encompasses any method that modifies a function callback pointer in the target to potentially execute malicious code.
Ctrl Inject	A process injection technique where key combination processing (for example, CTRL+C) is used in a possibly malicious manner.
Exe Header Modification	A process injection technique that includes an executable showing in-memory header modification that could be intended to load a DLL or execute code in a malicious manner.
Image Section Replacement	A process injection technique that involves the removal of a mapped DLL or executable from memory and replaced with new memory in a possibly malicious manner.
Thread	A process injection technique where a new thread has been remotely created in a possibly malicious manner.
Thread Context	A process injection technique where the context of a thread context has been modified to execute in a possibly malicious manner. For example, SetThreadContext.
Unknown Asynchronous Procedure Call	A process injection technique where an asynchronous procedure call that was not detected as queued is about to execute. Such a situation could be indicative of something malicious running in the kernel and injecting into a process or it could be other security products performing their own injection. It could also be caused by the Tanium process monitoring DLL not being injected into the actor process that queued the APC.
Unusual Initial Thread	A process injection technique where the first thread in a process was created in an unusual manner. For example, the operating system did not create the thread, but instead a remote process.
Window	One of any process injection techniques that use various window manipulations to execute code in a possibly malicious manner. For example, SetWindowLongPtr or SetProp.

© 2025 Tanium Inc. All Rights Reserved

1. Select **Consume Process Injection Alerts** in a detection configuration to enable Threat Response to consume Process Injection alerts. For more information, see Create detection configurations.

   > NOTE
   >
   > By default this option is disabled in new detection configurations.

2. From the Main menu, go to **Modules > Threat Response > Intel > Extended Detections**.
3. Select **Process Injection**. It is not necessary to add the Process Injection intel document to any detection configuration or intel list to consume Process Injection alerts.
4. (Optional) From the **Techniques** tab, Click edit to select the techniques of process injection that you want to monitor. Click **Save**.
5. (Optional) Provide system filters to define the event information to record and add them to a recorder configuration. Ensure the **Consume Process Injection Alerts** setting is enabled in a deployed detection configuration. Apply system filters to exclude particular processes from having the Tanium Driver inject into them for process injection detection in a deployed recorder configuration. For more information, see Create filters.
6. (Optional) From the **Suppression Rules** tab, you can view the suppression rules that currently exist for process injection. Suppression rules define the criteria for filtering alerts based on information that you provide. Suppressing alerts for process injection is an effective way to reduce false positive matches and reduce noise in alerts. If you create a suppression rule for process injection it appears in the list displayed on this tab. For more information, see Suppress alerts.

You can view, investigate, and take action on alerts that are the results of matches to process injection criteria from the Alerts tab of the process injection intel document.

Reputation data

Reputation data provides more insight into which alerts might be good candidates to save for further analysis and action. Through a Tanium™ Connect integration, Threat Response uses the reputation data from third parties, such as VirusTotal. Blocklisted hashes are not included in the results unless the hashes are discovered by the saved question.

Threat Response detects if the reputation service is paused or stopped and in this event does not update reputation data. If after 24 hours the reputation service is disabled or deleted, Threat Response deletes the reputation source and any existing intel documents associated with the source are moved to the Orphaned source. If reputation is added again, the reputation source is created again.

The maximum database size for the reputation database is 10GB by default. You can increase this size as needed in the Reputation settings in the Reputation workbench. If the database exceeds this size, the reputation service is disabled.

Configure reputation data in Tanium Connect

In Connect, create a connection from a saved question source to the Tanium Reputation destination. This connection initiates a list of hashes to be sent from a saved question in Connect to Reputation. The detect service queries Reputation for all discovered malicious hashes including known bad hashes. Reputation data requires a Connect version from Connect 4.1 to Connect 4.10.5, or Connect 4.11 and Reputation 5.0. For more information on configuring the reputation service settings, see Tanium Reputation User Guide: Reputation overview.

© 2025 Tanium Inc. All Rights Reserved

For endpoints that use reputation data, any hashes found by the saved questions are sent to the third-party reputation service for assessment.

> **NOTE**
>
> Reputation Intel Source improvements (requires Reputation 5.0.0+) including Saved Questions for reputation hashes must now be configured and managed entirely within Tanium Connect. The naming convention of Reputation Intel has changed from `Malicious Files $Date:$Time` to `Reputation Malicious Files $Date:$Time`. Additionally, any Reputation intel that has existed before an upgrade is renamed with the date and time of the upgrade appended to the Signal name.

1. Select **Consume Reputation Alerts** in a detection configuration to enable Threat Response to consume Reputation alerts. For more information, see Create detection configurations.

   > **NOTE**
   >
   > By default this option is enabled in new detection configurations.

2. To view alerts that are specific to Reputation, from the Main menu, go to **Modules > Threat Response > Intel > Extended Detections**.
3. Select **Reputation Malicious Hashes**.

Add Signals

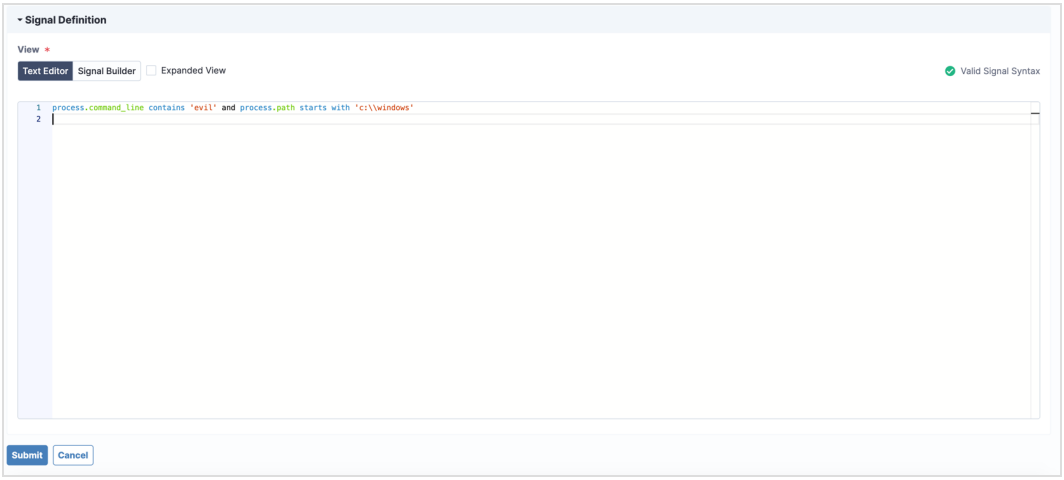
Signals are monitored by the recorder for live process, file, network, registry, and DNS event matching on the endpoint providing a recorder configuration is enabled in an active profile. If a recorder configuration is not enabled in an active profile, Signal matches still initiate alerts, however no specific information regarding the context of the Signal match appears in the resulting alert. You can write your own Signals. By default, each Signal can contain up to 55 terms.

> **IMPORTANT**
>
> An exhaustive reference to Signals syntax - including supported objects, properties, and conditions - is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click from the Threat Response overview page and click the Threat Response Intel Support tab.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Click **Create > Signal**.
3. Add a name and description.
4. Select the platforms for the signal to target.
5. (Optional) Select any available reactions to associate with the signal. For more information, see Create a reaction.
6. (Optional) In the Advanced Settings section, select Set to Active under Intel Safeguards to disable the signal when a high volume of alerts is initiated. For more information. see Intel safeguards.

© 2025 Tanium Inc. All Rights Reserved

7. Select a MITRE Technique ID. Selecting a MITRE Technique ID allows users to align with the MITRE Attack Framework and help map coverage to the different tactics and techniques. You can assign multiple technique IDs to a single Signal.
8. Configure the Signal. For more information, see Reference: Authoring Signals.



9. (Optional) Add a description.
10. Click **Save**.

IMPORTANT If the event is filtered (ignored), it cannot be matched against a Signal.

For Signals provided by Tanium, see Connect to the Tanium Signals feed on page 171.

You can use the Threat Response Import Signals API to import signals that contain comments in the signal definition. Comments in signals are denoted as // at the beginning of lines or after the signals content.

For example, you can use the Threat Response Import Signals API to import a signal that contains the following syntax:

```
//Description: Generic single line description
//MITRE: T1234
process.command_line contains "foo" and process.path contains "bar"
```

For more information on the Threat Response Import Signals API, click **Help > API** and see the API documentation from the Threat Response workbench.

Import and export Signals

Import and export Signals to move them from one platform to another. For example, you can export Signals from a test system and import them to a production system. Signals are imported and exported as JSON files and have a file size limit of 10 MB.

© 2025 Tanium Inc. All Rights Reserved

NOTE You cannot export OpenIOC, STIX, and YARA intel documents.

Export Signals

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Select the Signals you want to export and click the ellipsis and select **Export**. Any intel documents that are not Signals are omitted from the export.
3. For each Signal that you include in an export, select to **Include all Labels** and **Include all Suppressions** if you want to preserve the labels and suppression rules that you have associated with the Signal. Click **OK**. If you do not select to include labels or suppressions, the Signal is exported without any associated labels or suppression rules.

   NOTE When exporting a signal, only signal-specific suppression rules are included in the signal.
4. A JSON file is created for the export. Provide a name for the JSON file and click **Export**.

Import Signals

NOTE You can use the Threat Response Import Signals API to import signals that contain comments in the signal definition. Comments in signals are denoted as `//` at the beginning of lines or after the signals content.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Click **Upload Signal(s)**.
3. Browse to the JSON files that correspond to the Signals you want to import. Click **OK**. Click **Next**.
4. If the Signal already exists, or exists with different suppression rules or labels associated with it, select **Action > Skip** to not import the Signal. Click **Next**.
5. Review the list of the imported Signals and click **Finish**.

NOTE Exporting Signals that include MITRE technique IDs and importing them into an environment where the same Signals exist without associated MITRE technique IDs results in a new Signal with the same content and the addition of MITRE technique ID information. The result is that two Signals exist; one with MITRE technique information, and one without.

© 2025 Tanium Inc. All Rights Reserved

Upload intel documents

You can upload multiple intel documents at the same time, including YARA files. The size limit for uploading intel documents is 10MB for IOCs in XML format, such as STIX version 1.x, and Signals in JSON format.

BEST PRACTICE

Do not add more than 900 terms per type in a single IOC.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Click **Import IOC/YARA(s)** or **Import Signal(s)**.
3. Select intel files and click **Upload**.
4. Review the intel validation check. The intel XML schema validation check shows the documents that were successfully uploaded and any documents with errors.
5. Click **Close**.

Create intel documents

Create an intel document with a set of user-defined rules.

TIP

Quick IOC supports some types of defanged IP address formats that are found in threat intelligence documents, such as *10[.]1[.]1[.]1* or *10 . 1 . 1 . 1*.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Click **Create > Quick IOC**.
3. Type a name for the intel document. For long term usability, use a consistent naming convention.
4. From the **Detect when** drop-down menu, select a type of data.
5. Type the information to match. When you use the matches condition for any supported object, IOC uses regular expressions to evaluate resulting matches. You can include flags in the regular expression string to perform case sensitivity or insensitivity. You can use the `(?i)` flag around content in the regular expression for case insensivity. To end a section where you want to use case insensitivity, you can use the `(?-i)` flag.
   For example, `(?i)scvhost.exe(?-i)` matches include `ScVhOsT.eXe`, `scvhost.exe`, and `SCVHOST.exe`.
6. (Optional) Enable **Exact match required**.
7. In the **Advanced Settings** section, choose whether or not to enable Intel safeguards. Intel safeguards provide the option to set thresholds across the environment for intel and to suppress intel that generates amounts of alerts that exceed the thresholds. For more information on intel safeguards, see Intel safeguards.
8. Select a MITRE Techniques. Selecting MITRE Techniques allows users to align with the MITRE Attack Framework and

© 2025 Tanium Inc. All Rights Reserved

help map coverage to the different tactics and techniques. You can assign multiple techniques.

9. Select any applicable labels to add lables to the IOC.
10. Click **Create**.

Create IOCs

Use the IOC editor to create both simple and complex IOCs using AND/OR operators and understand the IOC objects and properties that Threat Response supports. You can edit IOCs that you import to the Threat Response workbench, remove any unsupported objects or properties, and add conditions to fine tune detections. The IOC editor ensures that the syntax is followed and validates that IOCs that you create feature supported terms. Imported IOCs might contain unsupported terms and therefore editing an IOC only enables you to add, modify, or delete terms supported by Threat Response, and to only delete non-supported terms.

Both the 1.0 and 1.1 versions of OpenIOC are supported.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Click **Create > IOC**.
3. Add a name and description.
4. (Optional) Select a reaction to associate with the IOC. Reactions automate one or more actions on an endpoint based on alerts from intel documents (for example, delete one or more files, kill a process, or quarantine an endpoint). For more information on reactions, see Creating reactions. By default, the reaction is set to Audit Mode. You can disable Audit Mode when you save the IOC.
5. In the **Advanced Settings** section, choose whether or not to enable Intel safeguards. Intel safeguards provide the option to set thresholds across the environment for intel and to suppress intel that generates amounts of alerts that exceed the thresholds. For more information on intel safeguards, see Intel safeguards.
6. Select a MITRE Techniques. Selecting MITRE Techniques allows users to align with the MITRE Attack Framework and help map coverage to the different tactics and techniques. You can assign multiple techniques.
7. Select any applicable labels to add lables to the IOC.
8. Use either the IOC Builder or Text Editor to provide the content of the IOC.
9. (IOC Builder) Select an object, property, condition, and value to use in the IOC. An exhaustive reference to IOC syntax - including supported objects and properties is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click  from the Threat Response overview page and click the Threat Response Intel Support tab. When you use the matches condition for any supported object, IOC uses regular expressions to evaluate resulting matches. You can include flags in the regular expression string to perform case sensitivity or insensitivity. You can use the `(?i)` flag around content in the regular expression for case insensivity. To end a section where you want to use case insensitivity, you can use the `(?-i)` flag. For example, `(?i)scvhost.exe(?-i)` matches include `ScVhOsT.eXe`, `scvhost.exe`, and `SCVHOST.exe`.

© 2025 Tanium Inc. All Rights Reserved

a. Click **Add Row** to add additional criteria to the IOC. When you have multiple rows, you can select whether the IOC evaluates all of the rows logically as AND or OR.

b. Click **Save**.

10. (Text Editor) Provide the IOC content using valid syntax. Threat Response validates the content and flags unsupported objects.

    a. Click **Save**.

Label intel

Use labels to organize intel into sets that are relevant for your environment. For example, you might want to sort intel by priority, incident case, or based on the applicable attack surface.

Create custom labels to control the promotion of intel in a production environment. The names of labels provided by Tanium are subject to change. Signals are generally updated automatically, creating a possibility that label changes could cause unintended consequences in a production environment. A best practice is to adopt a convention for naming custom labels that follows an organization's object naming guidelines. Intel documents that Threat Response provides by default, such as Defender, Deep Instinct, and Process injection do not support labels.

You can apply labels to the Reputation intel document, however if you want to add reputation intel for background scanning, you must add the reputation source in a Detection configuration. You cannot add the reputation intel document to a detection configuration as you would add other intel.

Apply a label

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Select the checkbox next to the intel documents or Signals. Click **Labels**.
3. Click **Add Label** and type in a new label or select an existing label.
4. Click **Save Changes**.

Manage existing labels

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Select the checkbox next to the intel documents or Signals. Click **Labels**.
3. Click **Manage Existing Labels** and select or deselect the labels you want to apply to the intel document or Signal. In the **Selection Preview** section, review the impact of making changes to intel documents.
4. Click **Save Changes**.

© 2025 Tanium Inc. All Rights Reserved

Configure YARA files

YARA files function like other intel documents, in regards to uploading, streaming from a folder, and labeling. However, Threat Response automatically assigns a scope to limit the evaluation scan; by default, all YARA files are set to scan live files. You can change the evaluation scope for any YARA file.



YARA 4.5.0 is supported and support for the following default modules is provided: pe, elf, dotnet, hash, cuckoo, math, magic, macho, dex, string, and time.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Click the intel name, then click the **Search Scope** tab.
3. Select the scope of evaluation scan.
    - **Live Files**: This instructs Threat Response to find the files for any running processes (executable and loaded library files) and then use the YARA rule to scan their file on disk. Limited to the running processes and their executable and library files.
    - **Memory**: Limited to the memory of all running processes.
    - **Paths**: Limited to the configured directory paths. The path search is recursive, up to six directories. When adding paths ensure that no duplicate entries or empty values are added.
4. Click **Save**.



On Mac OS 13.4+, YARA memory scanning is limited to processes without hardened runtimes only.

View orphaned intel documents

When the source for a piece of intel is removed, the intel moves into an orphaned state.

1. From the Main menu, go to **Modules > Threat Response > Intel > Documents**.
2. Expand the **Filter Results** section and set the **Source** to **Orphaned**.

Assign a reaction to an intel document

To cause the workflows that you define in a reaction to occur when an alert is initiated for an intel document, you need to assign the reaction to an intel document. For more information, see Creating reactions.

© 2025 Tanium Inc. All Rights Reserved

NOTE

When you duplicate an intel document, any reactions that you have assigned to the document that you are duplicating do not persist in the duplicate intel document.

Testing Intel for deployment

BEST PRACTICE

Test intel in a lab or test environment and deploy intel in a ring-based deployment before deploying to a production environment. Create the new Intel and use on-demand scans to test against endpoints to verify the intel matches on what you expect and that the intel does not match a high number of false positives. Evaluate intel safeguard settings.

When you are ready to promote the intel in a production environment, the following process is advised as a best practice:

1. Import or create the new intel in a production environment.
2. On-demand scan the intel against a computer group that contains a small number of endpoints that you have identified as appropriate for testing purposes. See Tanium Console User Guide: Create computer groups for more information. On-demand scans send a single piece of intel to the endpoints for immediate matching and alert reporting. You can use Signals, OpenIOC, STIX, YARA, or reputation intel in an on-demand scan. For more information, see On-demand scans. Verify the performance of the intel; for example, ensure it is matching and generating alerts for expected indicators of compromise.
3. On-demand scan the intel against a computer group that contains approximately 10-20% of the total endpoints the intel will ultimately target. Verify the performance of the intel. Modify the intel if necessary.
4. In addition to testing with on-demand scans, deploy intel in a ring-based deployment as a best practice. Modify the intel if necessary.
5. Deploy the intel to the production environment. Continue to verify the performance of intel and refine as necessary.
6. Review the settings you have specified for intel safeguards to evaluate the fidelity of intel documents and disable any intel documents that generate high volumes of alerts. For more information, see intel safeguards.

© 2025 Tanium Inc. All Rights Reserved

Creating reactions

Overview

Reactions help to automate actions to disrupt and respond to attacks for both on and off-network endpoints and help reduce the time to remediate issues from hours to seconds. Reactions automate one or more actions on an endpoint based on alerts from intel documents (for example, delete one or more files, kill a process, or quarantine an endpoint). This is different than a response action where a Tanium platform action (Live Response, Quarantine, Download File, Gather Snapshot) runs on a single endpoint after the alert is received by the service and a manual action is run. All reactions occur directly on the endpoint immediately after an intel match occurs. Reactions take place even if the endpoint is not connected to Tanium server.

Reactions reduce the risk of attack by providing a critical advantage in managing security incidents. Reactions help remediate known threats within seconds of identifying them, allowing workflows to be much more efficient and reducing a bad actor's capability of stealing data, causing damage, or intruding further into an organization. Automated workflows such as reactions provide capabilities that have become a regulatory requirement in many countries.

Reactions are defined in the Threat Response workbench and associated with an intel document. You can create a reaction to define a workflow that will occur when an intel match occurs on an endpoint. The intel document defines what to act on, and the reaction defines what action or actions to perform.



Reactions on detections inside ZIP files perform any relevant actions on the ZIP file itself.

Create a reaction

Create a reaction in the Threat Response workbench.



Creating reactions in the Threat Response workbench requires the **Threat Response Intel Reaction Write** permission.

1. Select **Intel > Reactions**. Click **Create Reaction**.
2. In the **Details** section, provide a name and description for the reaction.
3. In the **Steps** section, add steps that define the actions to perform when intel matches occur on an endpoint. You can create a step for each type of available action. You cannot create a reaction that contains multiple steps with the same action type. The available actions are:

   Kill Responsible Process

   This action type provides the ability to automatically kill a process when an alert is initiated for an intel match based on custom criteria including hash, name, command line, parent process, and ancestry. In response to an alert, the

© 2025 Tanium Inc. All Rights Reserved

action takes place immediately on the endpoint to allow the action to take place regardless if it communicating on the Tanium Server. **Kill Responsible Process** actions use the results returned as part of the Advanced Details for an alert to determine what artifact to act on, for example `processItem` in an IOC intel document.

When you select the **Kill Responsible Process** action, you can select to **Allow Signed Processes to be Killed** for either Windows or macOS endpoints. There are cases where killing a signed process is required. These settings are disabled by default to protect important processes such as `svchost`. **Allow Signed Processes to be Killed** enables you to create one reaction that does not kill OS signed binaries, and another version that you can use to kill OS signed binaries. For example, a **Kill Response Process** action does not kill a powershell.exe process in Windows unless you select this checkbox. Enable this setting for intel documents such as:

```
process.path ends with '\\powershell.exe' AND process.command_line contains '-ExecutionPolicy Bypass'
```

Kill Responsible Process actions act on all process items found in the intel document.

Quarantine Endpoint

This action type provides the ability to automatically quarantine an endpoint when an alert is initiated for an intel match. In response to an alert, the action takes place immediately on the endpoint to allow the action to take place regardless if it is communicating on the Tanium Server.



Before assigning quarantine actions, ensure that all endpoints that are targets of the intel document that the reaction is associated with meet the endpoint operating system requirements documented in Quarantining endpoints.

When quarantining an endpoint that has already been quarantined, the quarantine action respects the existing quarantine. In such cases a quarantine is not removed and reapplied.

Select the quarantine profile that you want to use. Changes to the profiles or rules after a quarantine has been applied on an endpoint has no effect on that endpoint unless it is unquarantined and requarantined.



Any alerts that had quarantine reactions associated with them from before the existence of quarantine profiles display as having a deleted quarantine profile.

Delete Files Identified by Intel

This action type provides the ability to automatically delete a file when an alert is initiated for an intel match. In response to an alert, the action takes place immediately on the endpoint to allow the action to take place regardless if it is communicating on the Tanium Server. **Delete Files Identified by Intel** actions use the results returned as part of the Advanced Details for an alert as the artifacts to act on. You can use the **Delete Files Identified by Intel** action type to delete empty folders, but not folders that contain files or other folders, even if the folder or folders it contains are also empty. **Delete Files Identified by Intel** actions act on all file items found in the intel document, including any `fileItem` artifacts that are returned as a child of a `processItem` artifact.

© 2025 Tanium Inc. All Rights Reserved

BEST PRACTICE

Use caution when you assign a **Delete Files Identified by Intel** action to an intel document that matches on `processItem` artifacts. Since `processItem` alert data contains a secondary `fileItem` artifact that specifies the location of the binary on disk, `processItem` artifacts with a **Delete File Identified by Intel** action match on the secondary `fileItem` and delete the binary from disk.

When you select the **Delete Files Identified by Intel** action, you can select to **Preserve Copy of Files** to save a copy of the file in such a way that endpoint users can no longer execute the file, read the contents of the file, modify, or delete it. Files are preserved in a ZIP file on the endpoint. On the endpoint, the path to preserved files assumes the form of `[Tanium Client]/extensions/threatresponse/data/restricted/[Intel ID][Guid]/reaction-[ID][Step Number].zip`

The file contents of the ZIP file is encrypted. Decrypt files that you download with the password `infected`.

IMPORTANT

Delete Files Identified by Intel actions that are associated with signals intel documents are not supported. If you need to delete specific files, use an OpenIOC or STIX intel document that alerts on a specific file name, or a YARA intel document that alerts on the contents of the file.

Delete Files

You can specify files to delete by pasting in a list of absolute paths that are separated by line breaks that you want to delete when an alert is initiated. You must specify file names as absolute paths. Quoting or escaping special characters is not required. Do not use quotes in these file paths unless they are actually part of the file name.

When you select the **Delete Files** action, you can select to **Preserve Copy of Files** to save a copy of the file in such a way that endpoint users can no longer execute the file, read the contents of the file, modify, or delete it. Files are preserved in a ZIP file on the endpoint. On the endpoint, the path to preserved files assumes the form of `[Tanium Client]/extensions/threatresponse/data/restricted/[Intel ID][Guid]/reaction-[ID][Step Number].zip`

The file contents of the ZIP file is encrypted. Decrypt files that you download with the password `infected`.

4. Click **Add Step**.
5. For each step that you add, provide a name and description for the step. Select an Action to perform, and select any additional settings that are available for the action.
6. When you have completed the workflow definition by adding steps to perform when an alert is initiated, click **Apply**.
7. Click **Create**.

Assign a reaction to an intel document

To cause the workflows that you define in a reaction to occur when an alert is initiated for an intel match, you need to assign the reaction to an intel document. Reactions continue to take action on endpoints even when alerts are throttled or intel is put into a reduced state on individual endpoints. The only way to disable a reaction is to delete the intel or remove the associated reaction

© 2025 Tanium Inc. All Rights Reserved

and re-deploy intel. Alternatively you can disable the intel at an enterprise level by intel safeguards.

1. Click **Intel > Documents** to locate an intel document that you want to assign a reaction to.
2. Select the intel document that you want to assign a reaction to and click **Edit**.
3. In the **Reaction** dropdown list, select the name of the reaction that you want to assign to the intel document.
4. Select **Set reaction to audit mode** to view the impact of the reaction without any of the actions you assign in a reaction actually occurring. Audit mode enables you to validate that any response actions that are initiated as part of a reaction do not have an unintended impact on an environment. When you create a new intel document and assign a reaction, **Set reaction to audit mode** is enabled by default to provide a safeguard against unintended or untested actions. To perform reactions, this setting must be deselected.

   NOTE

   When you run an on-demand scan for intel that is associated with a reaction that is set to audit mode, you can select **Override Audit Mode for Reaction** in the on demand scan to override audit mode and perform the reaction on endpoints.

5. Click **Save**.

Reactions that you assign to intel documents take effect when the intel is deployed to the endpoint. Intel must be included in a Detection configuration to be applied to an endpoint.

NOTE

When you duplicate an intel document, any reactions that you have assigned to the document that you are duplicating do not persist in the duplicate intel document.

An indepth overview of supported intel types and the specific intel artifacts that reactions act on, along with examples is available in the Threat Response Intel Support documentation. To access the Threat Response Intel Support documentation, click from the Threat Response overview page and click the Threat Response Intel Support tab.

Reaction statuses

The following reaction statuses for reactions are displayed in the Threat Response workbench for either intel documents or in the alerts results:

	For an intel document, this icon indicates the reaction is currently set to audit mode. For an alert, this icon indicates that the reaction was set to audit mode at the time an alert was initiated.
	For an alert, this icon indicates the reaction completed successfully.
	For an alert, this icon indicates that a reaction has multiple steps and indicates that some steps completed successfully, but at least one step in the reaction failed. For example, if the reaction features a Quarantine Endpoint step, but the endpoints that the reaction targets do not meet the endpoint operating system requirements, this step would fail. Other steps on the reaction could succeed.
	For an alert, this icon indicates that all steps in the reaction failed to complete successfully.

© 2025 Tanium Inc. All Rights Reserved

You can view details regarding any reaction success or failure including the status of each step in a reaction in the alert details of an alert that was initiated by a match on an intel document a reaction is associated with. For more indepth reaction detail data, you can view the endpoint logs. For more information, see Collect troubleshooting information from endpoints.

Audit reaction data

Audit mode provides a means for the endpoint to report back to the service if a reaction would have been initiated and what actions it would have taken without actually taking those actions. Audit mode enables you to validate that any response actions that are initiated as part of a reaction do not have an unintended impact on an environment.



Audit mode is specified at the intel document level. A reaction can be associated with multiple intel documents. By specifying audit mode at the intel document level, a reaction can be in audit mode for one or more intel documents, but not in audit mode for others.

© 2025 Tanium Inc. All Rights Reserved

Analyzing context

Overview

Use context analyzer to help determine what normal looks like in your environment. It provides a baseline that you can use to detect anomalies against. Use context analyzer to reduce false positives and benign investigative leads by determining the significance of a particular artifact. If a file or process is a common occurrence, it is likely benign. However, if it represents a rare occurrence, it might be indicative of an issue that requires further investigation. Context analyzer is the first step in helping you gather actionable data quickly and accurately about the normal state of an environment. By understanding the typical patterns in a digital environment, you can better focus on anomalies that might pose a true threat.

Context analyzer provides visibility into the most recent activity for processes, files, IP addresses, and process hashes across all online endpoints. Using file at rest (Index) and historical (Recorder Database) data, context analyzer displays a visual summary of the data followed by a searchable details grid. A sampling of the most recent data from each endpoint is provided, which attempts to prioritize outliers on each endpoint.

Context analyzer queries all files at rest and historical data across every online endpoint, visualizes that data and provides “context” for how an artifact appears in an environment. Such context helps answer questions such as: “Is this artifact normal in my environment?” “Does it exist across just a few or thousands of endpoints?”, “Which users are typically associated with this artifact?", "Does this artifact have the same hash everywhere, or are their many different hashes?", and "Are there any obvious outliers associated with this artifact?".

When you query an artifact, the endpoints that you target return the most recent data available for each artifact. Each endpoint provides responses grouped according to hash, path, operating system, endpoint, and user. Context Analyzer automates the searching for you and returns results received at 95% completion or a maximum of four minutes.

As context analyzer focuses on the most recent activity for an artifact it is important to understand that it works best at identifying the “normality” of an artifact in an environment, and when searching for unique outliers across an enterprise. Context analyzer is not suited for attempting searches such as finding the single outlier in 1000 similar events on a single endpoint. Live Connect and sensors are still often best for that type of analysis or investigation. Context analyzer does not take the place of deployed Intel documents when you need the assurance of artifact existence or non-existence across an entire environment.



Full file path searches are not currently supported.

Examples

Example (A): UserA was executing process svcapp-init.exe on this endpoint. Context analyzer can tell you if this process is common across the environment and which users are typically running it.

Example (B): A powershell executable is found in what looks like a non-standard directory. Context analyzer can show you if this path is commonly used anywhere else for this binary, does this binary have a hash in common with other powershell binaries or is this hash unique, is this associated with any particular operating system, if it is being run frequently across the enterprise, and which users are running it.

© 2025 Tanium Inc. All Rights Reserved

Example (C): You are creating a new Intel document to help you detect a potential threat. Using context analyzer, you can quickly determine how common a file, hash, process name, or IP address is in the environment and if it would cause an excessive amount of false positive alerts.

> NOTE
>
> Time filters can be very useful in the combined view; however, you might need a very short window due to the quantity of events.

Analyze the context of artifacts

1. Select artifacts to examine from the **Gather Samples** bar on the Threat Response **Context Analyzer** page. Select one of the following values, provide an artifact of interest, select the computer groups to examine and click **Search**.
   - **File Name** - File Name analysis supports any text, Full file path searches are not currently supported.
   - **Hash** - Hash analysis does not support special characters.
   - **IP Address**- IP Address analysis supports valid IPv4 or IPv6 address forms.
   - **Process Name** - Process Name analysis supports any text.

     > NOTE
     >
     > The search terms that you use are literal terms. Regular expressions and wildcards are not supported.
2. The Sampled Details section provides a list view of the endpoints on which a match has occurred. You can open a direct connection to the endpoint on which the match occurs. After opening a direct connection to an endpoint from a context analyzer result, the workbench displays all events that happened within one minute of the timestamp of the initially selected event.
3. (Optional) In the Sampled Details section, click **Add to an Investigation** in the Actions column to add the match to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

> NOTE
>
> Users who are assigned the **Threat Response Read Only User** role must have the **Interact Ask Dynamic Question** permission to use Context Analyzer. To add context analyzer data to an investigation, the **Investigate SHOW** and **Investigate Investigations WRITE** permissions are required.

You can decode encoded text in many places in the Threat Response workbench without having to copy and paste to a third-party tool. For example, you can decode all command line locations in the advanced details for a Threat Response alert.

© 2025 Tanium Inc. All Rights Reserved

1. For any encoded text item, click Decode .
2. Select the **Encoding Schema** of the encoded text.
3. Select the character encoding standard for output of the decoded text. You can select either UTF-8 or UTF-16LE. This option is not available for all encoding schemas.
4. Click **Decode**. The decoded results appear in the **Output** section of the page. You can copy the results to the clipboard.

> NOTE
>
> From any location in the Threat Response workbench, press `ALT + \` (Windows and Linux) or `Command + \` (macOS) to display the editor to decode encoded text. On some keyboards it is common for mappings to replace the / key (Scan Code 2B) with other characters, for example, the # character. On such keyboards, use the appropriate key combinations for the locale of the keyboard.

Export Context Analyzer results

1. From the Main menu, go to **Modules > Threat Response > Context Analyzer**.
2. Select one or more items in the Sampled Details grid to export.
3. Click **Export**.
4. Click **Copy to clipboard** to copy the selected data to the clipboard. Click **Export to CSV** to export the selected data to a CSV file that is saved in the downloads directory of the web browser.

© 2025 Tanium Inc. All Rights Reserved

Scanning endpoints

Threat Response scans each endpoint using the intel documents and Signals that you define. Scanning includes background scans, on-demand scans, and live Signals monitoring through the recorder. Background scans begin shortly after intel is deployed to the endpoint and continue on regular intervals. On-demand scans are initiated on demand, typically when you need to urgently locate all instances of a potential compromise.

A scan can have three possible results:

- **Match**: Identifies potential compromise and generates alerts.
- **No match**: None of the intel matched the data on the endpoints.
- **Inconclusive**: Generally, an indication that the scan did not complete for some reason.

When a scan finds a match, the alert is gathered from the endpoint and reported to Threat Response. From there, you can further investigate the endpoint.

The two available types of scans are background scans and on-demand scans. Background scans and on-demand scans are complementary; background scans are run on a schedule for all intel. On-demand scans are immediate; they are intended for scenarios such as testing or piloting new intel. In this way, you can test the results of specific intel with an on-demand scan and when the intel is revised appropriately to ensure it generates the intended alerts can be scanned on a routine basis through background scans.

Background and on-demand scans, regardless of the intel type, are throttled to ensure they do not overuse endpoint resources. All Tanium Client extensions in total consume no more than 5% of the available CPU resources on each endpoint.

On-demand scans that initiate endpoint throttling cause the endpoint to throttle background scan alerts for the effective period of the throttle, which is one hour by default.

Endpoint throttling does not initiate any system notifications. Server throttling continues to send notifications.

Background scans

Background scans run continuously against intel. Threat Response actively acknowledges alerts when they are received. Alerts are not duplicated for the same artifact on the same endpoint.

To edit a detection configuration, see Detection configurations.

On-demand scans

On-demand scans send a single piece of intel to the endpoints for immediate matching and alert reporting. You can use Signals, OpenIOC, STIX, YARA, or reputation intel in an on-demand scan. There is no size limit of the intel document you can use for an on-demand scan, but be aware of the network impacts of sending large amounts of data for scanning.

© 2025 Tanium Inc. All Rights Reserved

NOTE

Signals that use the `image` type with a `signature_subject` property (for example, `image.signature_subject contains subject`) are not supported in on-demand scans.

For Signals, you can use on-demand scans for a seven day historical query on the event recorder database. On-demand scanning on Signals is also useful when you are authoring Signals.

1. From the Main menu, go to **Modules > Threat Response > Intel**. Click an intel document.
2. From the intel document, click the three dots in the upper right and select **Start On-Demand Scan**.
3. Select **Override scan blockout windows** if you want the on-demand scan to ignore any configured scan blockout windows. Selecting this option forces the on-demand scan to execute on endpoints that are currently online. **Override scan blockout windows** requires the **Threat Response Override Scan** permission.
4. Select the computer groups you want the on-demand scan to target. Click **Start**.
5. When you run an on-demand scans for intel that is associated with a reaction that is set to audit mode, you can select **Override Audit Mode for Reaction** in the on-demand scan to override audit mode and perform the reaction on endpoints. For more information, see Create a reaction.
6. Click **Run**.
7. A new on-demand scan is initiated in the **On-Demand Scans** section of the intel document page. For each active on-demand scan you can view the number of alerts for the intel you are scanning for and the total number of online endpoints and the number of endpoints on which that the scan has completed. A completed scan indicates that the scan has been deployed to targeted endpoints and no additional endpoints will receive the scan. After a scan has completed, endpoints that the scan targets that might have been offline could come back online and report alerts. Each on-demand scan has an associated scan ID which is a six digit number. You can filter by scan ID on the **Alerts** tab of the intel document page to view alerts that are associated with the on-demand scan.

   NOTE

   Results are limited to endpoints that are online, have an active Threat Response profile deployed, and are present in one or more of the computer groups you have targeted for the on-demand scan.
8. When an on-demand scan is complete, the results of the scan are available on the **On-Demand Scan History** tab of the intel document page. You can view historical on-demand scans and their results and preserve this data for auditing purposes.

NOTE

On-demand scans are action-based and require an approver if action approval is enabled. You can add the Threat Response content set to action approval bypass to allow action bypass for on-demand scans.

© 2025 Tanium Inc. All Rights Reserved

CAUTION

On-demand scans of intel documents can generate a new alert for a condition or event that alerted in the past. This is expected behavior; each on-demand scan is a unique search activity. An example where this can occur is with Tanium Signals; if a signal is matched and alerts in real time, and the same signal document is later on-demand scanned, a second alert could be generated for the same event if the event falls within the seven day look-back period.

© 2025 Tanium Inc. All Rights Reserved

Creating configurations in Threat Response

Overview

Configurations are groups of settings that control the behavior of Threat Response components. You can create different configurations for each Threat Response component to control how it performs on specific groups of endpoints.

For example, you might want to apply and scan for specific intel on one group of endpoints, but not other groups. Or, you might want to apply a subset of Threat Response capabilities to a group of endpoints. Use configurations to customize which intel to apply, how and when to evaluate intel, how to index file systems, which events to record on all the endpoints in an enterprise, and what event data to stream to an external destination.

You can orchestrate configurations for detection, the recorder, index, and stream in a profile that is assigned to one or more computer groups. You can import and export configurations to make them easy to apply to target groups of computers. Threat Response provides example configurations that feature the most common configuration settings for specific operating systems.

Create detection configurations

Detection configurations provide directions for scanning endpoints for intel matches. To avoid scanning important endpoints or to limit when detection is active, you can include blockout periods to prevent scans during those times.

1. From the Main menu, go to **Modules > Threat Response > Management > Configurations**. Click **Create > Detection**.
2. In the **General Settings** section, provide a name and description for the detection configuration.
3. (Optional) In the **Engine Options** section, select **Use UTC instead of the local time on the endpoint when calculating Scan Blockout**.
4. In the **Engine Options** section, select the hours and days for the **Scan Blockout** period to stop scanning against available intel during the times you select.
5. Configure the **Settings**.
   a. (Optional) Select **Consume Deep Instinct Alerts** to enable Threat Response to consume Deep Instinct alerts and display alerts from Deep Instinct detection. Selecting **Consume Deep Instinct Alerts** requires the Deep Instinct agent to be running on the endpoint. By default this option is disabled.

   For the integration to work correctly, you must configure additional flags for the Deep Instinct Agent (D-Client) using the Deep Instinct CLI. For more information refer to the Deep Instinct documentation or contact Deep Instinct support.

   b. (Optional) Select **Consume Deep Instinct Alerts** to enable Threat Response to consume Deep Instinct alerts and display alerts from Deep Instinct on endpoints. By default this option is disabled.

© 2025 Tanium Inc. All Rights Reserved

c. (Optional) Select **Consume Defender Alerts** to enable Threat Response to consume Defender alerts and display alerts from Defender on Windows endpoints. By default this option is disabled.

d. (Optional) Select **Consume Process Injection Alerts** to enable Threat Response to consume Process Injection alerts. Selecting **Consume Process Injection Alerts** requires configuring the Process Injection intel document. See Process injection. By default this option is disabled.

e. (Optional) Select **Consume Reputation Alerts** to enable Threat Response to consume Reputation alerts.

f. Specify a value (in days) for **Initial Lookback**. The initial lookback value that you provide defines the number of days in the past to look in the Recorder database for matching.

6. (Optional) In the **Advanced Settings** section, specify a value for the **YARA File Size** or accept the default. This corresponds to the maximum size of file YARA can scan. (Default: 32 MB). YARA File Size and YARA Process Size do not apply to On-demand Scans. The values you provide in these fields are used by detection configurations for continuous data scanning.

7. (Optional) In the **Advanced Settings** section, specify a value for the **YARA Process Size** or accept the default. This corresponds to the maximum size of the process YARA can scan. (Default: 256 MB). YARA File Size and YARA Process Size do not apply to On-demand Scans. The values you provide in these fields are used by detection configurations for continuous data scanning.

8. In the **Intel** section, click **Add Intel**. Select the intel you want to add. Click **Add**.

9. Select Intel that you have added to Threat Response. Click **OK**. Click **Save**.



Changes you make to the intel that is included in a detection configuration do not take effect until the next intel deployment.

After you have deployed detection configurations to endpoints, you can view and manage findings that result from intel matches. See Managing alerts.

Create index configurations

Use an index configuration to detect and report threat indicators for files at rest. Index creates an index of local file systems, computes file hashes, and gathers file attributes and magic numbers in an SQLite database on the endpoint. Index returns the files that are contained in zip archives. For information on Index configuration settings, see Client Index Extension User Guide.



To accommodate architectural changes made to Index, when upgrading to the latest version of Threat Response, existing Index exclusions and **Hash Types to Calculate** are migrated from each legacy Index configuration into a new Index configuration with a matching name. If legacy Index configurations were attached to a Threat Response profile, the corresponding new Index configurations are added to that profile.

Index configurations determine how file indexing and hashing occur on the local file systems of endpoints. Index is optimized to minimize endpoint resource use and work with journaled file systems, when available.

© 2025 Tanium Inc. All Rights Reserved

NOTE

Legacy Index versions must be removed from endpoints before you deploy new Index configurations. For information on removing legacy Index versions, see Upgrade the Threat Response version.

1. From the Main menu, go to **Modules > Threat Response > Management > Configurations**. Click **Create > Index**. Provide a name and description for the index configuration.
2. Select the **Hashes To Calculate**. Index can record any combination of three different hash types: MD5, SHA-1, SHA-256, or SHA512. Do not select any hash type to disable calculation of hashes.

   NOTE

   If legacy index configurations included the **Include Malicious Hash List** setting, you must add the new Reputation intel document to intel configurations. When you upgrade to Threat Response 3.4 or later, any malicious hashes that exist in the reputation database are added to the Reputation Intel document. All malicious hashes identified after upgrade are added to this same intel document moving forward. Open each detection configuration and ensure that the Reputation source is added anywhere you want endpoints to match against the malicious hashes.
3. (Optional) In the **Advanced Settings** section, change the default values for the following settings:

   High Priority Path Scan Fail-Safe Frequency

   Use high priority path scan fail-safe frequency to receive more frequent updates for files in certain regions of the disk. In addition to the baseline disk scan, you can specify high priority paths that use recorder events to update data. (Default: 24 hours). High Priority Paths are indexed more frequently. Performance impacts on the endpoint increase with the frequency of indexing and the size of the path. Using the root directory as a High Priority Path is discouraged as this can quickly consume resources.

   Index Scan Fail-Safe Frequency

   Threat Response uses Index to scan the entire disk on an endpoint at regular intervals that typically occur between once a day and once a week. Index does not use recorder events to update file data across the entire disk. Enter a value for how often the Index scan runs. (Default: 7 days).

   Index First Scan Distribute Over Time

   The delay time after Index starts before starting the initial index scan. (Default: 24 hours).
4. In the **High Priority List** section, select filters that you want to designate as high-priority paths. See Create filters for more information. Click **Manage Priority List** to select existing filters. Select any or all of the available filters. Only filters that have already been created are available to select. When you have selected the filters that you want to add to the configuration, click **Apply**. See Create filters for more information on filter methods. Click **Save**. You cannot add more than 24 filter definitions.
5. Click **Save**.
6. Click **Create**.

© 2025 Tanium Inc. All Rights Reserved

After you have deployed index configurations to endpoints, you can use sensors to query indexed files. See Using sensors to query indexed files.

Create indexing exclusions



Starting in Tanium Client Management version 1.12.132, you add Index exclusions that apply globally to all Tanium solutions that use Tanium Index. Exclusions that you add in Tanium Client Management are not visible in the list of exclusions that you set in Tanium modules; it is important to view the exclusions in both locations to understand the total exclusions that are applied to the Tanium environment. For more information, see Create and deploy an Index configuration.

Create recorder configurations

The recorder saves forensic evidence for each endpoint in a local database. With recorder configuration settings, you can restrict database volume by size and days of storage.

Adjust the settings for each endpoint database to suit a specific environment. Systems with different roles can generate a higher volume of certain types of events. For example, domain controllers typically generate more security events and network traffic than an average end-user workstation. You can build custom configurations that maximize event retention across an environment, while excluding unwanted activity. Starting in Threat Response 3.5, recorder configurations that target Windows endpoints require the Tanium Driver to be installed and enabled to record process and command line events. The Tanium Driver is installed as part of Threat Response and is upgraded when Threat Response upgrades are applied.

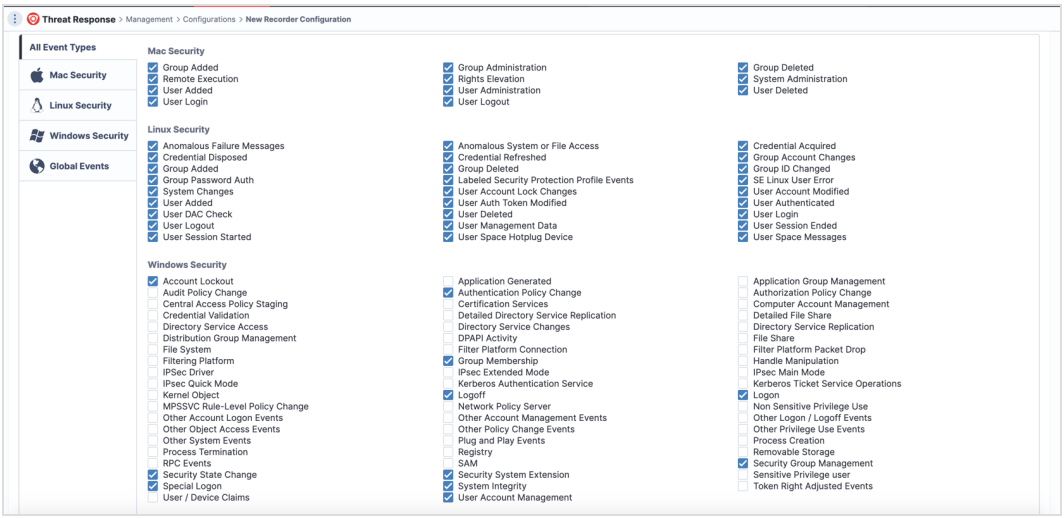
1. From the Main menu, go to **Modules > Threat Response > Management > Configurations**. Click **Create > Recorder**. Provide a name and description for the recorder configuration.
2. In the **Database Configuration** section, configure settings for the recorder database. The recorder database contains configuration data, signal match data, and configured event data. The events of a signal match are always written to the database, and override any filters that are included in a recorder configuration.
    a. Provide a **Maximum Database Size**. The endpoint purges events if the maximum database size is reached. If this database is larger than 2.5 GB, you cannot reimport the database if it is exported.
    b. Provide the **Maximum Days to Retain Events** to specify the number of days that events are retained. Older events are purged from the endpoint database. Entering 0 prevents events from being purged based on age.
    c. Select whether or not to **Record Tanium Client Processes**. Selecting this option includes all Tanium Client processes, and all child process of the Tanium Client in recorded events.
    d. Select whether or not to **Encrypt Database**. By default, the recorder database (recorder.db) is encrypted using AES 128 bit encryption. Deselect the database encryption setting if you do not want this data to be encrypted. Deselecting this setting does not revert any encrypted databases to a decrypted state. If changing an endpoint to a decrypted state, change the configuration, deploy the updated profile, and then deploy an action to the endpoints with `Recorder`

© 2025 Tanium Inc. All Rights Reserved

- Reset Database. After the reset action is complete, the recorder.db exists in a decrypted state.

> **NOTE** If encryption is enabled, a recorder database cannot be decrypted offline.

3. In the **Recorded Events** section, select the types of events to record for the current configuration.



Security Events

Security events include events such as authentication, privilege escalation, and more. This event type includes logon events, even if operating system logs have rolled. For Linux security events, see https://github.com/linux-audit/audit-userspace/blob/master/lib/libaudit.h for more information on specific event IDs. For Windows security events, see https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq for more information on specific event IDs. More information about event IDs is available in the Recorder Security Event Details documentation. To access the Recorder Security Event Details documentation, click from the Threat Response overview page and click the Recorder Security Event Details tab.

Global Events

Event types under global events do not apply the same across operating systems.
When a global event is disabled, events are not recorded unless they are associated with an applied signal. To preserve all intel alert context, even partial match events related to an intel document are recorded.

Database event filters do not apply for event types that are globally disabled. To filter recorded events associated with intel alerts, that event type must be enabled in the Threat Response Database configuration. For example, to prevent image load events from being recorded, you must enable image load events, and filter them appropriately.

© 2025 Tanium Inc. All Rights Reserved

Global events contain the following:

- **Registry**

  [Windows only] Changes to the registry, such as the creation or alteration of registry keys and values. Includes the associated process and user context.

- **Network**

  Network connection events, such as an HTTP request to an internet location, including the associated process and user context. Events are recorded for all inbound and outbound TCP connections.

- **Process**

  Process events, such as path, hash, command line, user information, ancestry, and the signed status of a process.

- **File**

  File system events, such as files written to directory locations on the endpoint. The associated process and user context are included. Examples: A malware file copied to a location that Windows Update uses, or content changes made to a file.

- **DNS**

  [Windows 8.1 or later and Linux endpoints where eBPF is enabled] Request information, including the process path, user, query, response, and the type of operation. On Windows and Linux endpoints where eBPF is enabled, DNS events are only recorded when you use the system DNS client. DNS events for applications that use their own DNS client are not recorded (for example, nslookup and Google Chrome).

- **Image Loads**

  [Windows only] Returns historical data from each endpoint regarding image loads; for example, the full path and hash, the entity that signed an image, or a designation of "Unsigned" if the image is not signed. A possible example is the loading of an unsigned DLL. If you do not select Image Loads, any signal that uses the image event type results in an Unmatched Events warning in the Alert Details. Selecting Image Loads filters for `image` and `process.path is not 'system'`. Selecting Image Loads does not apply filters for Linux or Mac endpoints.

  Note: The driver load view in recorder is categorized as an image load ending in `.sys` and originating from PID 4 (SYSTEM). Driver load events display in the image load event view and therefore image load events might be displayed on Linux and Mac endpoints. While there is no support for image loads on Linux and Mac endpoints, driver load events such as these are presented as image loads.

© 2025 Tanium Inc. All Rights Reserved

- **Driver Loads**

  Returns historical data from each endpoint regarding driver loads; for example, the full path and hash of a driver. By default, Driver Load events are not selected. Selecting Driver Loads on Windows filters for `image` and `process.path is 'system'`. Selecting Driver Loads on Linux or macOS filters for `image`.

- **HTTP headers**

  [Windows only] Returns HTTP header information from connections on endpoints including the time connections occurred, the connection ID of the connection, the remote (destination) address, and the header name and value.

  IMPORTANT

  When using HTTP headers as recorded events, be aware that CPU usage on endpoints is impacted; especially on servers. When capturing HTTP headers as recorded events, ensure that you are monitoring the performance impacts on the endpoints from which they are captured and tune their collection appropriately.

4. In the **Filters** section, click **Manage File Filters** to select existing filters. Select any or all of the available filters. Only filters that have already been created are available to select. See Create filters for more information on filter creation. When you have selected the filters that you want to add to the configuration, click **Apply**. In the **Filters** section, designate the method you want to apply for each set of filters. Select either **Include** or **Exclude**. See Create filters for more information on filter methods.
5. (Linux only) In the **Custom Audit Rules (Linux Only)** section, add **Custom Audit Rules**. Provide custom audit rules for use on Linux endpoints. Audit rules are provided to the auditd service and are in the following format: `-a exit,always -S adjtimex -S settimeofday -k time_change`. You can provide up to 500 custom audit rules.

   NOTE

   By default eBPF is enabled on supported endpoints. When eBPF is enabled, any custom auditd rules that you have added to a Recorder configuration are not used. To disable eBPF, use the CX.recorder.BPFEnableBPF configuration setting and set the value to "0". For more information, see the Client Recorder Extension User Guide.
6. Click **Save**.

After you have deployed recorder configurations, you can view events that occur on the endpoints where you have applied the configuration. See Direct connecting to endpoints and exploring data.

Create stream configurations

Stream provides the ability to send rich endpoint data from the recorder to an external destination. This raw data includes process, network, file, driver events that you can use to investigate incidents, enrich other workflows, or perform custom analytics. Stream configurations enable you to specify and filter recorder events for the endpoints in an environment, and provide instructions for exporting - or streaming - these events directly to an SIEM for analysis in JSON format. For example, you

© 2025 Tanium Inc. All Rights Reserved

can specify that all network events with one or more filters be streamed to Chronicle, Microsoft Sentinel, Splunk or Elastic. Tanium customers use this data to solve critical data gaps and Tanium Partners leverage this data to build their own security programs.

1. From the Main menu, go to **Modules > Threat Response > Management > Configurations**. Click **Create > Stream**. Provide a name and description for the stream configuration.
2. Select a **Management Method**. You can manually provide configuration parameters, or upload a JSON file with configuration parameters for a stream configuration. Select either **Manual** or **File Upload**. If you select **File Upload**, click **Browse for File** and select a JSON file to upload. The JSON file contains the configuration parameters for the stream configuration. If you select **Manual**, complete the following tasks.
3. In the **Configuration** section, select a **Destination Type**. The **Destination Type** you select determines the additional required configuration settings that you are prompted to provide. When you select a destination type and provide configuration information for that specific destination type, you cannot change the destination type.

   Chronicle

   - Namespace - A namespace consists of a label part and a UUID. If a namespace label does not exist, then using it will create a new namespace with that label and a random UUID.
   - Chronicle Configuration URL - The URL to configure Chronicle. The provided URL must be complete and begin with `HTTPS://`
   - API Key - The API key that is used to authenticate calls.
   - Customer ID - The Chronicle customer ID for your environment.

   ELK

   - URL - The URL for Logstash HTTP input.
   - Disable Certificate Validation (Less Secure) - Select to disable the validation of the certificate presented by the destination. By default certificate validation is performed.

   Microsoft Sentinel CEF

   - Host/IP - The hostname of IP address of the AMA log forwarder.
   - Port Number - The numeric value for the syslog port which must be less than or equal to 65535. Only numeric values are allowed.
   - Dry Run (Optional) - Select to collect statistics about the data that would be streamed to the destination but not actually send the data.
   - Filter Tanium Processes (Optional) - Select to filter all Tanium Client processes and all child processes of the Tanium Client in the recorded events.
   - Enable Transport Layer Security (TLS) (Optional) - Select Enable Transport Layer Security (TLS) to use a secure connection to transmit data using Syslog over TLS (Transport Layer Security) to the destination. This ensures that the data is encrypted and authenticated between the sender and the receiver. If you select Enable Transport Layer Security (TLS) you must provide the following details:

© 2025 Tanium Inc. All Rights Reserved

- Server Verification - Specify the type of authentication to use with the destination for TLS. Select one of the following:
  - Use Default Certificate - Select this option to use the default certificate.
  - Allow Self-Signed Certificate - Select this option to allow a self-signed certificate
  - Upload PEM File - Select this option to use a RSA key for authentication. Browse to a PEM file to upload to the destination.
- Client Verification - Specify the type of authentication to use for the client.
  - None - Select this option to not require client verification.
  - Upload Certificate and Key - Select this option to specify a certificate and key that are used to verify the identity of the client. If you select this option, browse to a certificate and a PEM file to upload to the destination and provide a passphrase that corresponds to the certificate.
- Message Severity - Select the logging severity that Stream uses for output data. You must configure the Microsoft Sentinel data collection rule to have a minimum logging severity level that is lower or the same as the value you specify.
- Message Facility - Select the logging facility that Stream uses for output data. You must configure the Microsoft Sentinel data collection rule to observe this facility.



For more information on message facilities, message severities, and data collection rules, see https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-ama?tabs=portal#select-facilities-and-severities.

Splunk HEC

- URL - The URL to access the Splunk REST API.
- Authorization Token - The authorization token to access your Splunk environment. Do not include the `Splunk` prefix in this token.
- Disable Certificate Validation (Less Secure) - Select to disable the validation of the certificate presented by the destination. By default certificate validation is performed.

Splunk TCP

- Host - The fully-qualified Splunk host domain name.
- Port - The port for the stream communication to the host.

Select **Dry Run** if you want to collect statistics about the data that would be streamed to the destination, but not actually send data.

© 2025 Tanium Inc. All Rights Reserved

BEST PRACTICE

By default, **Dry Run** is enabled when you create a stream configuration. Analyze the amount of event data that would be streamed to a destination before you deselect **Dry Run**. While this setting is enabled, no data is streamed to a destination; it must be disabled for data streaming to occur.

You can use the `Threat Response - Daily Stream Stats` sensor to gain an understanding of the amount of data that would be sent.

4. Select **Filter Tanium Processes** to filter all Tanium Client processes, and all child processes of the Tanium Client in the recorded events. For example, if the Tanium Client starts Python to run a sensor, this is filtered from the recorded events.
5. (Optional) If you want to use a proxy to provide a gateway, provide the host, port, and a username and password for the proxy. This setting is not available for all destination types.
6. In the **Event Types** subsection, select the event types that you want to stream. For more information on event types, see event types. At least one event type is required.
7. In the **Filters** section, click **Manage Filters** to add filters to use in the stream configuration. Only filters that have already been created are available to select. See Create filters for more information on filter creation. When you have selected the filters that you want to add to the configuration, click **Apply**. In the **Filters** section, designate the method you want to apply for each set of filters. Select either **Include** or **Exclude**. See Create filters for more information on filter methods.
8. Click **Save**.

Create filters

Filters provide a way to define the event information to record to reduce performance impacts and enable quick event identification. Filters are applied in high priority paths, recorder configurations, stream configurations and are created for specific types of recorder events. Threat Response provides a default set of filters for each type of recorder event that you can use in configurations. You can also create your own filters. You can either include or exclude filters. The **Include** method of filtering enables you to replace the default filter to only include the filters you specify to reduce performance impact and enable quick event identification. The **Exclude** method of filtering prevents events that match the criteria you provide from recording.

Filters are constructed in signals syntax. You cannot have more than 55 unique terms in a signal.

If a configuration enables process, file and network event types but an include filter only includes process events. No file or network events are recorded. When using an include filter for network events, the associated process events are automatically included.

1. From the Main menu, go to **Modules > Threat Response > Management > Filters**. Click **Create**.
2. Select a **Filter Type**.

   File

   File filters define criteria for files to record when path or operation values match.

© 2025 Tanium Inc. All Rights Reserved

High Priority Path

Threat Response uses Index to scan the entire disk on an endpoint at regular intervals that typically occur between once a day and once a week. Index does not use recorder events to update file data across the entire disk. It is common to want more frequent updates for files in certain regions of the disk. To provide this visibility, in addition to the baseline disk scan, Threat Response enables you to specify high priority paths that use recorder events to update data and also scans every 24 hours by default. To change the default setting:

a. From the Main menu, click **Modules >Threat Response** to open the **Threat Response Overview** page.

b. Click Settings and open the **Service** tab.

c. In the Misc section provide a value (in hours) for the **High Priority Path Scanning for Index Configurations (Hours)** setting.

d. Click **Save**.

A high priority path must include a `file.path starts with` clause in Tanium signal syntax. Escape backslash characters in paths. For example, use `C:\\Users\\Administrator` to make `C:\Users\Administrator` a high profile path.

- Supported: `file.path starts with 'C:\\Users\\Administrator'`
- Unsupported: `file.path starts with 'C:\'`

A high priority path, in addition to the `file.path starts with` clause, can additionally specify one or more `file.path ends with` clauses to narrow the file types to inspect.

- Supported: `file.path starts with 'C:\\Users\\Administrator' and file.path ends with '.dat'`
- Supported: `file.path starts with 'C:\\Windows\\System32' and file.path ends with '.dll' and file.path ends with '.exe'`
- Unsupported: `file.path ends with '.dat'`

Image

Image filters define criteria for image events to record when path, hash, or signature values match.

Network

Network filters define criteria for network events to record when a match is made for a defined IP address, port, or DNS query.

Process

Process filters exclude events based on criteria such as the process path, hash, user name, user group, or command-line to filter out a process. Process filters do not exclude child processes from being recorded. Use an ancestry filter statement to exclude child processes.

© 2025 Tanium Inc. All Rights Reserved

NOTE

If you have a process-based filter, but that process spawns child processes, it is expected that the process that matches the process filter will still be recorded to ensure complete process trees. However, events for the process (for example, file events) that match the process filter are not recorded.

Additionally, a process matching a process filter can also be recorded to ensure completeness of data, if there is a Signal match that contained the filtered process.

Registry

Registry filters define criteria for Windows registry events to record when specific key-value pairs match.

System (Windows and Linux only)

System filters provide paths of files to match or filter from the Linux audit daemon (auditd) logging. On Windows endpoints, system filters exclude particular processes from having the Tanium Driver inject into them for API monitoring and process injection monitoring. On Linux endpoints, system filters completely blind the recorder from any activity from the defined path, for example, process launches. When eBPF is enabled, any system filters that you have added to a recorder configuration are not used. To disable eBPF, use the CX.recorder.BPFEnableBPF configuration setting and set the value to "0". For more information, see the Client Recorder Extension User Guide. Since system filters filter content from auditd, other auditd consumers will also be blind to this path, not just the recorder.

3. Select an **Operating System**. Provide a name and description for the filter.
4. In the **Filter Definition** section, click **Filter Builder**.
5. Click **Row** or **Grouping** to add a filter definition using the filter builder. Select a type, a property, and condition. The available properties and conditions differ for each filter type. You can use properties and conditions to create logical patterns for matching specific events. You can add multiple statements to each filter. For each statement that you add, specify a logical and or a logical or to define the relationship of the statements in a filter. The following table provides a reference for properties and conditions for each filter type.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters

Type	Property	Supported Conditions	Comments
File	operation	`is` `is not`	One of `create`, `write`, `open_write`, `rename`, `permissions`, or `delete`.  NOTE `open_write` is only relevant on endpoints that rely on auditd.  NOTE The `rename` operation corresponds to the `move` operation in the recorder events view.

	path	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full path to the file.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

Process	path	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full path to the process executable. Process filters do not exclude child processes from being recorded. Use an ancestry filter statement to exclude child processes.
			
			NOTE If you have a process-based filter, but that process spawns child processes, it is expected that the process that matches the process filter will still be recorded to ensure complete process trees. However, events for the process (for example, file events) that match the process filter are not recorded. Additionally, a process matching a process filter can also be recorded, to ensure completeness of data, if there is a Signal match that contained the filtered process.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments
	hash	`is` `is not`	The MD5 hash of the process executable file.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	command line	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full command line of the process.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	user name	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The user name executing the process.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	user group	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The user group or domain of the user executing the process.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	parent path	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full path to the parent process file.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	parent command line	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full command line of the parent process.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	ancestry path	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full path to any of the parent processes.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments
	ancestry hash	`is` `is not`	The MD5 hash of any of the parent processes.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	ancestry command line	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full command line of any of the parent processes.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

	ancestry user name	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The user name executing any of the parent processes.

	ancestry user group	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The user group or domain of the user executing any of the parent processes.

	signature status	`is` `is not`	One of `verified`, `unverified`, or `no_signature`

	signature issuer	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The signature issuer of the process.

	signature subject	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The signature subject of the process.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

Network	address	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The IPv4 remote address.

	port	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			A direction-specific non-ephemeral port. Local on incoming, remote on outgoing.

	dns query	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The hostname requested for DNS resolution.

	operation	`isis not`	Network operations that include connect and accept.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

Registry	key path	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full path to the registry key, including the full hive name.

	operation	`is` `is not`	Registry operations that include create, set_value, delete, and rename.

	value name	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The registry value name.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments

Image	path	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The full path to the file.

	hash	`is` `is not`	The MD5 hash.
	signature status	`is` `is not`	One of `verified`, `unverified`, or `no_signature`

	signature issuer	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The signature issuer of the process.

	signature subject	`is`
		`is not`
		`contains`
		`contains not`
		`starts with`
		`starts with not`
		`ends with`
		`ends with not`
			The signature subject of the process.

© 2025 Tanium Inc. All Rights Reserved

Properties and conditions for filters (continued)

Type	Property	Supported Conditions	Comments
System	path (Linux)	`starts with` `starts with not`	The full path to the file.

	actor path (Windows)	`is`
		`is not`
		`starts with`
		`starts with not`
			The full path to the process or file that performs the process injection.
			NOTE When using `is` or `is not` filter construction, the filter must match a file and not a folder. For example, `process_injection.actor_path is C:\\exclude\\` is invalid construction.

Property values can be an integer, a simple alphanumeric string, or they can be more complex and include other characters, such as spaces, backslashes, and hex-encoded values. Property values do not support regular expressions or wildcards. On Windows platforms, case is not sensitive for provided property values; for example, `TaniumClient` or `taniumclient` has the same effect. To create patterns for properties that start with, contain, or end with, use conditions and add additional statements to filters. For searches with non-alphanumeric values or spaces, enclose the value in single quotes. To escape special characters within the single quotes, the following sequences are supported:

- `\r` For carriage return
- `\n` For newline
- `\t` For tab
- `\\` For the backslash itself
- `\'` For a single quote within the quotes
- `\x` To allow a single-byte hex-encoded sequence. For example \x20 would translate to a single space.

NOTE The hex-encoding is required to handle UTF-8 characters outside of the single-byte character set. Any UTF-8 character can be added via the hex-encoding, if needed

The following sample expressions demonstrate combined expressions, precedence, and escaped special characters:

- `process.command_line contains 'evil' AND process.path starts with 'c:\\windows'`
- `(file.path starts with 'c:\\temp' OR file.path ends with '.evil.tmp') AND process.path contains cmd.exe`

© 2025 Tanium Inc. All Rights Reserved

6. (Optional) Click **Group**. Using a group indicates that you intend to match all conditions in the group against a single event. For example, to ensure that matches happen against the same file event, you should group those events. You can then include multiple groups to achieve matches against different events in time. You can use logical AND and logical OR to further refine group behavior.
7. Click **Save**.
8. In the **Filters** section of a Recorder or Stream configuration, click **Include** or **Exclude** next to any filter that you have added to designate the method you want to apply for each set of filters. The **Include** method of filters enables you to replace the default filter to only include the filters you specify to reduce performance impact and enable quick event identification. For example, for registry events, if you provide one or more registry filters as include, those replace the default include filter of 'registry'. The **Exclude** method enables you to effectively prevent events from recording. If a set of filters that you designate to **Include** contains a specific filter that has been designated to a set of filters to **Exclude**, a warning displays in the workbench.

Import and export configurations and filters

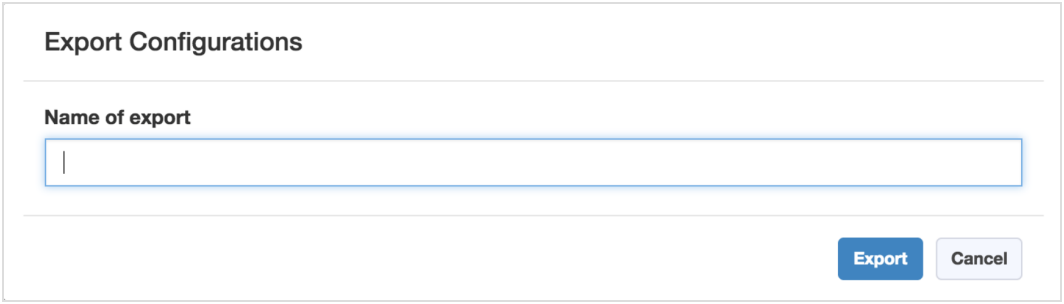
Import and export configurations and filters to apply them in a different Threat Response environment. For example, you can export configurations or filters that you have tested from a lab environment and import them into a production environment. With the exception of index configurations, both configurations and filters are imported and exported exclusively as JSON files.

Export configurations

1. From the Main menu, go to **Modules > Threat Response > Management > Configurations**.
2. Select one or more configurations to export. Click **Actions > Export** to export the selected configurations. To export all configurations, click **Export All**.
3. On the export page, provide a name and click **Export**. All of the configurations in the Threat Response environment are exported.

Export filters

1. From the Main menu, go to **Modules > Threat Response > Management > Filters**.
2. Click **Export All**.
3. On the export page, provide a name and click **Export**. All of the filters in the Threat Response environment are exported.



© 2025 Tanium Inc. All Rights Reserved

Import configurations

1. From the Main menu, go to **Modules > Threat Response > Management > Configurations**.
2. Click **Import/Export**. Select **Import JSON** and browse to a JSON file.
3. Click **Import**.

Import filters

1. From the Main menu, go to **Modules > Threat Response > Management > Filters**.
2. Click **Import**. Browse to a JSON file.
3. Click **Import**.

© 2025 Tanium Inc. All Rights Reserved

Creating profiles in Threat Response

Overview

Profiles combine configurations and apply them to one or more computer groups. Create and apply profiles to provide the most relevant Threat Response capabilities to specific groups of endpoints. For example, you can create profiles that apply configurations for such groups as:

- Endpoint type, such as servers or employee workstations
- Endpoint location, such as by country or time zone
- Endpoint priority, such as business-critical endpoints
- Endpoint configuration needs, such as VDI endpoints

The Profiles page displays all the profiles that are available to use with Threat Response. Threat Response provides default profiles that feature commonly used configurations as examples. For each profile, you can view a description and the computer groups that have the profile assigned. Profiles display as Deployed, New, Updated, or Deploying.

Deployed

Indicates that the profile is currently in use on one or more computer groups and that no changes have been made to the profile settings

New

Indicates that the profile has never been deployed to endpoints

Updated

Indicates that the profile is in use but there are pending changes that cannot take effect until the profile is deployed again

Pending

Indicates that the profile is in the process of being deployed to endpoints

Warning - Deleted Computer Groups

The profile targets computer groups that have been deleted. Ensure that the intel documents contained in the profile all target valid computer groups.

Tanium Managed profiles

Tanium Managed profiles are provided that contain updated configurations. These profiles are the result of Tanium data and experience and have been designed to use settings that are considered safer and to provide more real-time visibility with index and recorder data. You can not delete Tanium Managed profiles. Tanium Managed profiles are intended to be a starting point

© 2025 Tanium Inc. All Rights Reserved

that you can build off of or expand and are initial starting points that are based off of Tanium best practices. No existing profiles are changed when you install a version of Threat Response that provides Tanium Managed profiles. This is a new point of departure to accelerate the time for configuring the operation of Threat Response as quickly as possible without having extensive Tanium experience or subject matter expert guidance.

[Tanium Managed] Low Resource Assets

The **[Tanium Managed] Low Resource Assets** profile is intended for endpoints with limited CPU and memory resources. Includes less than 8 GB of memory and 4 logical processors/cores.

This profile is supported for Linux, MacOS and Windows endpoints.

[Tanium Managed] Windows Domain Controllers

The **[Tanium Managed] Windows Domain Controllers** profile is intended for Windows domain controllers with specific recorder filters assigned to optimize the retention of recorder data.

[Tanium Managed] Servers

The **[Tanium Managed] Servers** profile is intended as a set of best practices based on Tanium data for Servers.

This profile uses a two day **Index Scan Frequency**, and a **High Priority Path Scanning** interval of 12 hours.

The `All Linux` and `All Windows Servers` computer groups are intended targets for this profile.

[Tanium Managed] Workstations

The **[Tanium Managed] Workstations** profile is intended as a set of best practices based on Tanium data for Workstations.

The profile uses a one day **Index Scan Frequency**, and a **High Priority Path Scanning** interval of 12 hours.

The `All Windows Workstations` and `All Mac` computer groups are intended targets for this profile.

Create a profile

Create a profile to manage configurations for deployment to one or more computer groups.

1. From the Main menu, go to **Modules > Threat Response > Management > Profiles**. Click **Create Profile**. Provide a name and description for the profile.
2. Select to **Enable** or **Disable** the profile. When you **Disable** a profile, the targeting for that profile is made such that it is not applicable to any endpoints. The targeted Computer Groups that you have assigned that profile are not changed, however it is not deployed to endpoints that are included in those Computer Groups. For example, `Profile A` targets the `All Windows` Computer Group. If you disable `Profile A`, it still appears to target the `All Windows` Computer Group, but it is not deployed to those endpoints. Any endpoints that are targets of a disabled profile move to their next applicable enabled profile based on

© 2025 Tanium Inc. All Rights Reserved

priority. Any configurations deployed by the profile before it was disabled are removed if no profile is currently applicable. If you switch a deployed profile from enabled to disabled you are prompted to deploy the profile so the change can take effect.

3. In the **Computer Groups** section, click **Select Computer Groups** to add the computer groups to which you want to deploy the Threat Response configurations. Computer groups that you have associated with custom tags provides advantages over common Computer Groups, such as `All Computers`, or `All Windows`. By using Custom Tags, you can take advantage of the profile prioritization in Threat Response without needing to make any changes to the profiles themselves, for example, needing to re-deploy the profiles after changes are made.

   Manual computer groups are not supported.

4. In the **Detection**, **Index**, **Recorder DB**, and **Stream** sections, select an available configuration. A summary of the configuration is available to preview. If you need to make changes to the configuration, click **Edit**.

   When a detection configuration is not enabled, you can still perform on-demand scans. To fully disable detection from running on endpoints, create and enable a detection profile and configure a complete blockout window.

   If any component of an active profile is not configured, the implications are as follows:

Implications of unconfigured components of an active profile

Configuration	Implication
Detection	If the Intel component of an active Threat Response profile is not configured, intel documents are still updated on endpoints. However, intel is not used by Threat Response to generate alerts. On-demand scans are evaluated if the endpoint is part of a targeted group and is not within a blackout window. A detection configuration should be specified with a 24/7 blockout scan window to prevent on-demand scans from evaluating.

© 2025 Tanium Inc. All Rights Reserved

Implications of unconfigured components of an active profile (continued)

Configuration	Implication
Recorder	If the recorder component of an active Threat Response profile is not configured, the `TaniumClient` process continues running. However, the recorder does not record activity on endpoints in the action group. On Linux endpoints, the auditd and audispd processes restart when a configuration is added or changed. Ensure the Track Changes setting is not enabled in an Index Configuration or the recorder could become enabled.
Index	If the index component of an active Threat Response profile is removed, Index continues to be deployed to endpoints, however Threat Response does not perform Index tasks.
Stream	No data is streamed to a destination outside of Tanium.

5. (Optional) Specify a **TPA Scan Frequency** for Windows endpoints to configure how often the Tanium Persistence Analyzer runs on endpoints. Changing this setting affects the data that Threat Response sensors return.
6. Click **Save**.

Prioritize profiles

A computer group can have one assigned profile. However, an endpoint can be a member of multiple computer groups. If an endpoint is a member of multiple computer groups, the profile with the highest priority is applied to that endpoint. If another user updates profiles before the prioritization of profiles can complete, the prioritization is reset.

1. From the Main menu, go to **Modules > Threat Response > Management > Profiles**.
2. Click **Prioritize**.
3. Order the profiles in the order of their priority. The profile with the priority number of one (1) has the highest priority.
4. Click **Save**.

Deploy a profile

Deploy a profile to enable the functionality of Threat Response on all of the endpoints in the computer groups that the profile targets. A user must have management group rights to all computer groups in all profiles being deployed. When deploying profiles using the system user service, a user must have either unrestricted management rights, or rights to All Computers to deploy profiles.

© 2025 Tanium Inc. All Rights Reserved

NOTE

Confirm that all packages are cached before you deploy a profile. A ribbon appears on the profiles page if you attempt to deploy a profile prior to all packages being cached. Click the ribbon to view details about the state of package caching.

BEST PRACTICE

Track the deployment of Threat Response tools to the endpoints in an environment by viewing the Threat Response Coverage panel in Tanium Trends. The coverage of Threat Response tools across endpoints is important to measure; if you are not including the entirety of your estate when searching for specific activity, then you are at risk.

1. From the Main menu, go to **Modules > Threat Response > Management > Profiles**.
2. Select one or more profiles to deploy and click **Profile Actions > Deploy**.

   IMPORTANT

   Profile deployment is not part of a scheduled action. You need to deploy a profile in order for Threat Response capabilities to function on endpoints.
3. Enter your password to confirm the deployment. Click **OK**.

   IMPORTANT

   If the account of a Tanium Administrator who last edited a profile is disabled for any reason, the profiles that administrator edited become displayed as **Not Configured**. In such a situation you can enable the **Deploy as Service Account** setting. Click Settings > **Service** > **Misc** and select **Deploy as Service Account** to use the service account to deploy profiles. Selecting this setting causes Threat Response to ignore user permissions you have configured. Any user that can create or deploy profiles can deploy profiles to any computer groups.

Deploy intel

Before you deploy intel, ensure that you have thoroughly tested intel to verify that:

- The intel matches on what you expect
- The intel does not match a high number of false positives

See Testing Intel for deployment for more information.

Configure the intel deployment setting

© 2025 Tanium Inc. All Rights Reserved

1. From the Threat Response overview page, click Settings .
2. On the **Service** tab, click **Intel**. Make intel package selections:
    - **Intel Package Publication Interval**: Specifies how frequently the intel documents and labels are pushed to the endpoints (Default: 24 hours).
3. Click **Save**.

Immediately deploy intel to endpoints

Intel is automatically published to the endpoints on a regular interval. If a situation requires it, you can manually push the intel documents and Signals to the endpoints.

1. Click **Management > Profiles**.
2. Click **Deploy Intel**.



Assign the **Threat Response Intel Deploy Approval Bypass** permission to roles that deploy intel to bypass approvals for intel.

© 2025 Tanium Inc. All Rights Reserved

Direct connecting to endpoints and exploring data

You can review endpoint data with a direct connection or from an endpoint snapshot.

- Direct connection

  With direct connections, you can conduct analysis within seconds, without time-consuming data transfers or parsing. You can take multiple snapshots of the endpoint data, browse the file system, export events, and save evidence for remediation.

- Endpoint snapshot

  Snapshots capture the endpoint data for asynchronous investigation offline, preserving the recorder database for storage and collaborative analysis on the Tanium Module Server. With snapshots, you can export events, and save evidence for long-term analysis.

Threat Response supports direct connections using Tanium Direct Connect. Direct Connect provides a communication channel for other Tanium modules and a central location for configuring and administering direct endpoint connections across modules. Direct Connect replaces the mechanism for live endpoint connections that was used in previous versions of Threat Response to provide better performance and a consistent experience across Tanium modules. To install Direct Connect, see Tanium Direct Connect User Guide.

For new installations beginning with Threat Response 2.4, Direct Connect is enabled by default.

Direct connect to an endpoint

You can connect to endpoints that are registered with Tanium and are a member of a computer group that is accessible to you. You must have the IP address or computer name of the endpoint. If you do not have management rights to an endpoint, it appears offline.

You can make a direct connection to one or more endpoints.

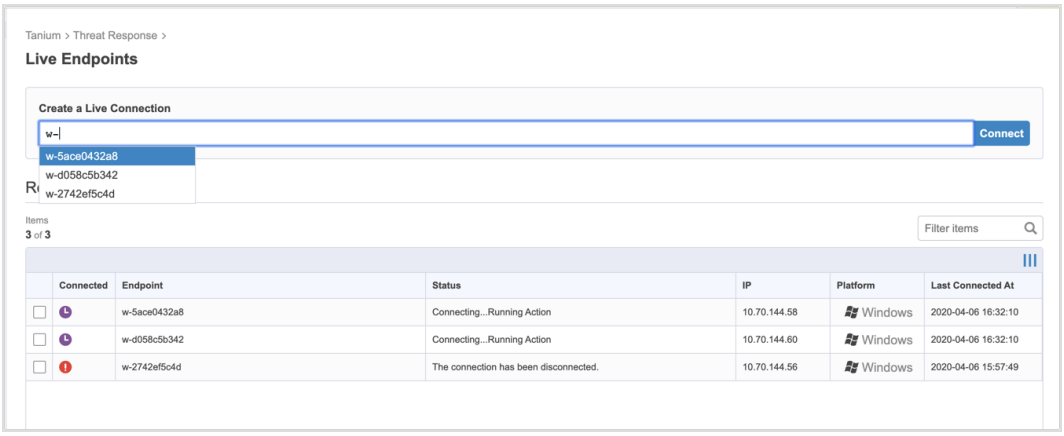
1. From the Main menu, go to **Modules > Threat Response > Direct Connect**.
2. Type the IP address or computer name of an endpoint that you want to add. Matching endpoints appear as you type.

   If the endpoint you want to add is not in the list, verify that the endpoint is a member of a computer group that you can access. An indicator next to the text field shows whether an endpoint is currently online.

© 2025 Tanium Inc. All Rights Reserved

3. Select one or more endpoints to add. Click **Connect**.



The live endpoint list displays endpoint connections that have been attempted, are connected, have failed, or where the connection has been closed. The history of connected endpoints is sorted by the last date on which endpoints were connected. Additionally, the date and a link to the last must gather package for the endpoint is provided. To download the most recent must gather package for an endpoint, click the link in the Last Must Gather column for the endpoint. If you do not see the Last Must Gather column, click the additional details icon at the top right of the grid and make sure to select Last Must Gather column to display this data. Live endpoint connection status appears next to the endpoint with the connection information. An endpoint remains on the Direct Connect list until the connection is manually closed, regardless of the connection status. The connection times out after ten minutes of inactivity.

Add to investigation

In the events grid on a live connection, click **Add to an Investigation** in the Actions column to add the event to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

Capture a snapshot

You can capture a snapshot of an endpoint database for offline analysis and detailed forensics.

> **NOTE** When you use Direct Connect to manage live endpoint connections, you cannot view snapshots of Recorder 1.x databases (monitor.db). This does not apply to Recorder 2.x databases (recorder.db).

1. From the Main menu, go to **Modules > Threat Response > Direct Connect**.
2. Click the computer name to go to the events grid. Click **Capture**.
3. Go to **Saved Evidence**.
4. View the snapshot progress by expanding the computer name.

To view endpoint name and the number of captures, go to the **Snapshots** menu. The snapshot name is the endpoint host name with a timestamp in a *YYYY_MM_DDTHH.MM.SS.mmmZ* format.

© 2025 Tanium Inc. All Rights Reserved

Close the connection

You can manually close a connection to one or more endpoints. Select the endpoints you want to disconnect on the **Direct Connect** page. Click **Delete**.

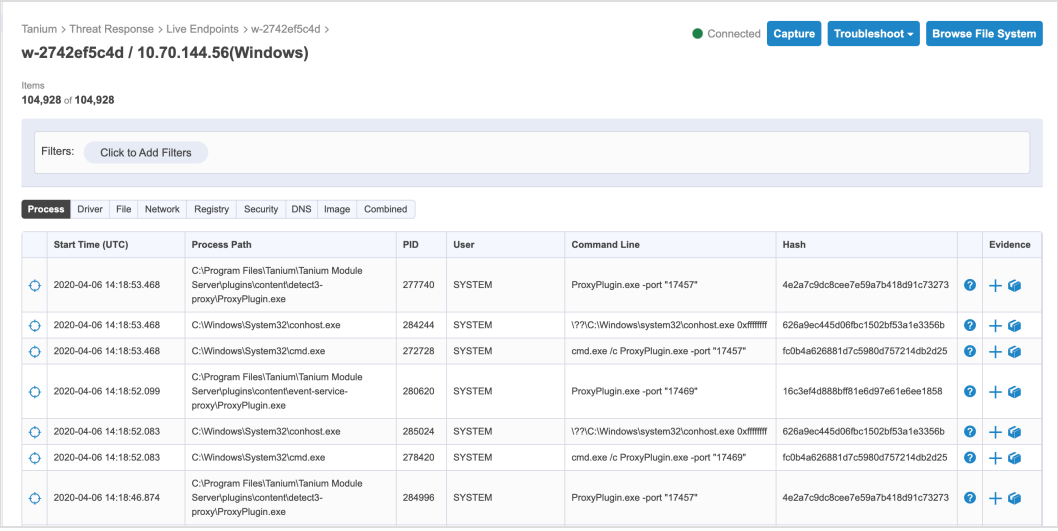
Browse the file system on connected endpoints

You can browse the file system on connected endpoints and download files that you want to keep as saved evidence. You can delete files on an endpoint if you have the Threat Response Administrator role.

1. Click an endpoint from the live endpoint list.
2. Click **Browse File System** to open a file browser at the root directory. On Windows endpoints the default location is `c:\`. On macOS and Linux endpoints the default location is `/`. Click a row in the results grid and click the folder icon in the process path column to open the file system to the directory that contains the file.
3. Navigate the file system by typing a path, or by clicking directories in the file browser of the breadcrumbs of the path. For each file in a directory you can view the size, creation date, modification date, and the permissions for the file. Symbolic links are visible while file browsing in a live connection.
4. Click one or more files to download as saved evidence. From the Main menu, go to **Modules > Threat Response > Saved Evidence > Files** to access the files that you download.
5. You can delete files and folders on an endpoint if you have the Threat Response Administrator role. To delete a file, ensure that you have the Threat Response Administrator role and click the delete icon at the end of the row. Click **Delete**. Deleting symbolic links requires Tanium Direct Connect 2.4 or higher.

Search for events

You can inspect and investigate endpoint data after you make a live connection or capture a snapshot. Search endpoint data for events using various parameters and operators. The search section displays all times in the UTC time standard.



© 2025 Tanium Inc. All Rights Reserved

1. Open the events grid on a live connection or snapshot.
2. Click an exploration button to search for events. Each exploration button is associated with a specific event type. The filter criteria for each event type changes based on the event type you select. For example, you can filter on such criteria as process path, IP address, operation, event type, hash, signature, key value, and more. For example, for file events you can sort on the following operations:

   Create

   An event that corresponds with the creation of a file

   Write

   An event that corresponds with writing to a file

   Delete

   An event that corresponds with the deletion of a file

   Move

   An event that corresponds with the moving of a file to a different location in the file system

   Permissions Changed

   An event that corresponds with changing the permission on a file

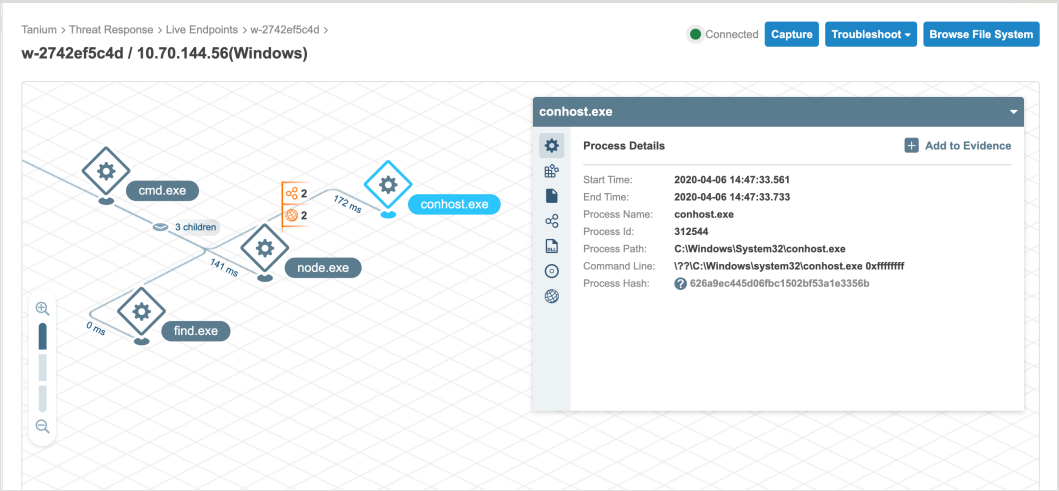
   Open

   An event that corresponds with the opening of a file by another process

3. Filter the search results to locate specific events that match criteria you provide. You can enter multiple sets of criteria based on various attributes of the event type. Less than three sets of filter criteria are treated as a logical `AND`. If you add more than two sets of filter criteria you can select to apply any or all of the criteria you have provided as a filter. The results are shown below the filters that you specify.
4. For most event types, the event grid features a column with a pivot icon. Click the icon to display questions that you can ask in Tanium Interact to gain further insight into the event.

Click a process to view additional details. The **Process Tree** visualization appears with focus on the process you selected. If a process is currently running, it displays the refresh icon. Drag the visualization in any direction to view peer or ancestor processes.

© 2025 Tanium Inc. All Rights Reserved



The **Process Tree** view displays all of the file, network, registry, and child process activity that was initiated by the current process. This page also provides the full process image path and arguments, user context, hash, and parent command line. A tree view of network processes display, including the current process, parent, children, and peer nodes. You can zoom in and out, click and drag, and click events to change the view. You can isolate one of the processes in the tree view and quickly focus on an artifact for analysis.

Hash information for each process is available from the events grid or from the **Process Tree** view for any specific process.

A hash can have one of the following ratings:

- Non-Malicious (Green)
- Malicious (Red)
- Unknown (Grey)
- Pending

You can decode encoded text in many places in the Threat Response workbench without having to copy and paste to a third-party tool. For example, you can decode all command line locations in the advanced details for a Threat Response alert.

1. For any encoded text item, click Decode .
2. Select the **Encoding Schema** of the encoded text.
3. Select the character encoding standard for output of the decoded text. You can select either UTF-8 or UTF-16LE. This option is not available for all encoding schemas.
4. Click **Decode**. The decoded results appear in the **Output** section of the page. You can copy the results to the clipboard.

© 2025 Tanium Inc. All Rights Reserved

NOTE

From any location in the Threat Response workbench, press `ALT + \` (Windows and Linux) or `Command + \` (macOS) to display the editor to decode encoded text. On some keyboards it is common for mappings to replace the / key (Scan Code 2B) with other characters, for example, the # character. On such keyboards, use the appropriate key combinations for the locale of the keyboard.

Manage snapshots

Snapshots show all the data from an endpoint. The database file contains historical event activity going back to the first moment of recording or to the configured limits. Snapshots are stored on the Tanium Module Server.

Export a snapshot from an endpoint

You can retrieve the endpoint database manually if an offline endpoint or a direct connection fails.

1. Log on to the endpoint with administrator credentials.
2. Stop the endpoint recorder by deploying a profile that does not contain a recorder configuration.
3. Copy the `recorder.db` file to a location accessible to the Tanium Console from the `<Tanium Client>/extensions/recorder` directory.

   NOTE

   Change the file name to include the host name and a timestamp in the format: *hostname_YYYY_MM_DDTHH.MM.SS.mmm*Z.db. The file name appears in Threat Response.
4. Start the endpoint recorder by deploying a profile with a recorder configuration.

Download a snapshot

You can download snapshots an endpoint databases for offline analysis and detailed forensics outside of Threat Response.

1. Go to **Threat Response > Saved Evidence**. Click **Snapshots**.
2. Select the snapshots that you want to download and click **Download**.
3. The snapshot downloads are managed through the web browser. Note the location to which the browser downloads the file. Multiple snapshots are added to a zipped file.

Upload a snapshot

1. (Optional) Install upload authentication certificates.
2. In the Tanium Console, go to **Threat Response > Saved Evidence** and click **Upload Snapshot**.
3. Browse to the saved snapshot.
4. Click **Upload & Connect**.

If you are having difficulty uploading a snapshot, see Troubleshooting Threat Response on page 361.

© 2025 Tanium Inc. All Rights Reserved

NOTE

You can view uploaded snapshots from users who are using the same active persona as the active persona that uploaded the snapshot. Additionally you can view uploaded snapshots if the current user is the same as the user that uploaded the snapshot. The Threat Response Administrator role has access to view all uploaded snapshots. To provide other roles visibility into all uploaded snapshots, assign the **Threat Response Visibility Bypass** permission to those roles.

Save files and events

While reviewing the event data from a direct connection, you can save files - including locked files - and events directly from the events grid as you investigate. You can save files of any type.

NOTE

You must have a direct connection to the endpoint to save file evidence. Saving evidence files from the endpoint is limited by available memory on the Tanium Module Server. You cannot save file evidence from snapshots.

1. Open the events grid.
2. Double-click an event row to open the **Process Details** page.
3. Select **Save Process Evidence**.

The file is saved under **Saved Evidence**.

NOTE

You can view evidence saved from endpoints that belong to computer groups for which you have permissions to access. For example, you can view evidence from endpoints for which the active persona belongs to at least one management rights group to which the endpoint belongs. If the current user belongs to at least one management rights group to which the endpoint is a member of, saved evidence for that endpoint is visible. The Threat Response Administrator role has access to view all saved evidence. To provide other roles visibility into all saved evidence, assign the **Threat Response Visibility Bypass** permission to those roles.

To toggle the visibility of one or more types of saved evidence for a user, add or remove the following permissions that correspond to the type of saved evidence for the user role:

Download: Threat Response Downloads READ
Export: Threat Response Exports READ
Event: Threat Response Saved Evidence READ
Snapshot: Threat Response Snapshot READ

If you remove the **Threat Response Downloads Read/Write** permissions for a user, the files tab is not available under saved evidence, however selecting **All** still displays files in the results.

© 2025 Tanium Inc. All Rights Reserved

NOTE

If an endpoint is offline for longer than the configured value of the **Max Endpoint Age (Days)** setting in Tanium Interact, only the users with the **Threat Response Visibility Bypass** permission can view alerts and saved evidence for the endpoint. If such an endpoint comes back online, alerts and saved evidence become visible to users with the correct permissions.

Download a file

Suspicious files might require more analysis or reporting to threat intelligence. After you save files from a direct connection as evidence, you can also download them from the **Saved Evidence** page in Threat Response. The file contents are in an encrypted ZIP format that is downloaded to the endpoint that is hosting the browser. Decrypt files that you download with the password `infected`. If you need to inspect the file without opening it, the ZIP headers are not encrypted. The file evidence encryption method is based on the file size. Files that are greater than or equal to 2^32 bytes are encrypted with aes256 encryption. Files that are less than 2^32 bytes are encrypted with ZIP 2.0 encryption. Some ZIP utilities that support ZIP 2.0 decryption may not support aes256 decryption.

You can select multiple items of saved evidence to download at one time. When you download multiple items of saved evidence each item is downloaded as a ZIP file that is nested in a container ZIP file. Each ZIP file in this container is encrypted with the password `infected`. You can download a single file of any size. When downloading multiple files the total size of the downloaded files cannot exceed a total size of 1GB. To download files that exceed 1 GB in total size, download them individually.

Select one or more files from the **Saved Evidence** page. Click **Download**. The files are saved in a ZIP file in the downloads directory for the Web browser.

Create Enforce rules

You can pivot from evidence on a single endpoint to create Enforce policies for multiple computer groups that contain Windows endpoints. You can add policies to existing process rule policies or create new ones from Threat Response, where you seamlessly complete the policy configuration in Enforce.

1. From the Main menu, go to **Modules > Threat Response > Saved Evidence**.
2. Click one or more saved events.
3. Click **Create Protection Policy**.
4. Confirm the evidence to use and click **Create**.
5. On the **Policy Selector** page, create a new policy or add the evidence to an existing policy.
6. Complete the information on the **Edit Policy** page.
7. Click **Create** or **Update** as appropriate.
8. Review the **Policy Summary** and add enforcements as needed.

© 2025 Tanium Inc. All Rights Reserved

Export events

You can export some or all of the events from an endpoint as a ZIP file that contains a CSV file. If you are exporting a large event database, take a snapshot and export the events from the snapshot to reduce the load on the endpoint.



Large exports might take a while to become available.

Select the rows in the events grid that you want to export, and click Export .

Manage IOCs

Indicators of Compromise (IOCs) are artifacts observed on an endpoint that indicate a breach of security. IOCs help you detect data breaches, malware infections, or other threat activities. IOCs include the following:

- Hash values of suspicious files
- IP addresses that are known to be malicious
- Domain names associated with malicious activities
- URLs that are used for phishing attacks
- Email addresses used to send spam or malware
- File paths of malicious software
- Registry keys modified by malware

As you examine the endpoint event data during an investigation, you might confirm that an event is malicious. You can save such events and files as evidence.

Generate an IOC

1. From the Main menu, go to **Modules > Threat Response > Intel**.
2. Select **Add > Evidence Based IOCs**.
3. In the IOC Normalized Tree drop-down menu, select **Item from saved evidence**. Add one or more items.
4. Select an indicator type and value from the drop-down menus.
   Threat Response populates the list information from the details of saved evidence.
5. Click **Generate**.

© 2025 Tanium Inc. All Rights Reserved

Searching across the enterprise

Use event data to locate suspicious activity on other endpoints. Evaluate the extent of an intrusion and take informed action at scale.

Hunt across the enterprise

You can use the Threat Response sensors to search for suspicious events on multiple endpoints across the network.

Queries for simple events, such as a process, registry key, or file, yield immediate results. You can search for “known-bad” events, and recognize and evaluate the “known-good” events. You might be encountering a set of evidence that seems suspicious, at first, but might actually be normal system activity.

1. From the Main menu, go to **Modules > Threat Response > Enterprise Hunting**.
2. (Optional) Narrow the list of sensors by clicking filters or typing in search terms. This limits the visible sensors and highlights the applicable Common Uses.
3. To review the sensor summary, click the caret to expand.
4. Click the sensor name to open the parameters configuration page and complete the fields as needed.

   NOTE If a sensor has no configurable parameters, the Interact results grid opens immediately.

   If you select **Common Uses** the parameter fields are automatically populated. Click **Ask Question**. The results are available in an Interact grid where you can also create a saved question. You must close the grid to select a different sensor. For more information, see the Tanium Interact User Guide: Results.
5. Select the results that need further investigation.
6. Open a live connection or take a snapshot of the endpoints and verify that the events are actually malicious.
7. (Optional) Quarantine or remediate the compromised endpoints.
8. Create an IOC to scan for this type of activity in the future.

To search for files on disk, see Tanium Client Index Extension User Guide: Reference: Index sensors.

To search historical activity, use the following sensors.

- Trace DNS Queries

  NOTE If this sensor returns `No Events`, ensure that DNS events are configured and the recorder is using eBPF.
- Trace Executed Process Hashes
- Trace Loaded Drivers

© 2025 Tanium Inc. All Rights Reserved

- Trace Executed Processes
- Trace Logon Events
- Trace Executed Process Trees
- Trace Network Connections
- Trace File Operations
- Trace Image Loads
- Trace Registry Keys or Values

Enterprise hunting questions

You can sort the enterprise hunting questions to display them for which attack phase they are relevant.

Data Theft

An attacker has obtained or is attempting to obtain account credentials or other sensitive information within your environment. Data exfiltration or some form of system impact may occur soon. Attackers may attempt to interrupt, manipulate, steal, or destroy critical assets. It is not uncommon for bad actors to use encrypted channels or stagger the transfers to avoid detection.

Initial Compromise

An attacker has gained access or is attempting to gain access to your environment. If successful, attackers may attempt to move to the next attack phase.

Lateral Movement

An attacker is expanding or attempting to expand the attack scope within your environment. Data exfiltration or some form of system impact can occur shortly after this happens. Attackers can interrupt, manipulate, steal, or destroy your assets.

Persistence

An attacker is attempting to maintain or increase access to your environment. If successful, attackers may attempt to load malicious payloads onto your environment, such as bots and malware, which may remain dormant in your environment even if the attacker stops.

The following list provides a reference for enterprise hunting questions:

- Account Lockouts Security Event Log Search
- AutoRun Files
- AutoRun Program Details
- Autoruns by Category

© 2025 Tanium Inc. All Rights Reserved

- Certificate Search
- Cleared Windows Security Event Log Search
- Command Line of Process
- Command Line with Hash Match
- DLL Load Order Hijacking Search
- Driver Details with Hash
- Environment Variables
- Established Connections with Hash
- Explicit Logon Security Event Log Search
- File Certificate Details
- File Handle Details
- File Handles Of Process
- Has Incident Response ID Files
- Has Scheduled Task
- Hash Of File
- Hosted Services Name Audit
- ICloud Settings
- Injected Threads
- Is File Digitally Signed
- Linux AutoRuns
- Listen Ports with Hash
- Loaded Modules Not Matching Whitelist
- Loaded Modules Of Process
- Loaded Modules with Hash
- Logon Security Event Log Search
- Mac AutoRuns
- Mac Downloaded Files
- Mac Firewall Settings
- Mac Gatekeeper Settings
- Mac Kext Details

© 2025 Tanium Inc. All Rights Reserved

- MD5 Hash Of File
- MD5 Hash Match Files Executing
- MD5 Hash Single File Match
- Mutex Details
- Mutex Handles Of Process
- Network Details
- Non-Approved Established Connections with Hash
- Original Filename
- PowerForensics File Record
- PowerForensics Master Boot Record
- PowerForensics Prefetch
- PowerForensics Recently Opened Office Files by User
- PowerForensics Shim Cache
- Processes Using Module
- RDP Client History
- Remote Desktop Event Log Search
- Run Command History
- Running Processes With Filename Mismatch
- Running Processes with Hash
- Running Processes with MD5 Hash
- Scheduled Tasks
- Semaphore Details
- Service Module Details
- Service Module Details with Hash
- Service Process Details
- Service Status with Hash
- Service System Event Log Search
- SHA1 Hash Match Files Executing
- SHA1 Hash Single File Match
- SHA1 Hash Of File

© 2025 Tanium Inc. All Rights Reserved

- Shell History
- SIP Settings
- SSH Known Hosts
- Trace DNS Queries
- Trace Executed Process Hashes
- Trace Executed Process Trees
- Trace Executed Processes
- Trace File Operations
- Trace Image Loads
- Trace Loaded Drivers
- Trace Logon Events
- Trace Network Connections
- Trace Registry Keys or Values
- Windows Audit Policy
- Windows Credential Security Settings
- WMI Event Consumers

Account Lockouts Security Event Log Search

Retrieves lockout events from the Windows Security Event log in a specified time period. Also retrieves attempts to authenticate with a locked-out account. Using this sensor requires enabling account lockout auditing.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Retrieve	Select either **Account Lockouts** or **Logon Attempts with Locked out Accounts**.
Look Back Hours (Max 168)	Enter the number of hours to look back.

This sensor returns data that provides the time of the lockout, the hostname, account name, account domain, logon type, status, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

AutoRun Files

Returns a subset of the AutoRuns data, specifically the name of each AutoRun file and the cryptographic hash of the file in MD5, SHA1, SHA256, or IMP format. This sensor uses cached data; you can use the **Incident Response - Generate Autorun Cache [Windows]** package to regenerate this data.

© 2025 Tanium Inc. All Rights Reserved

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to display in the results for each file. You can select MD5, SHA1, SHA256, or IMP.
Include Microsoft Entries	Select this option to include Microsoft entries in the results. Do not select this option if you want to exclude Microsoft entries from the results.

This sensor returns data that provides the filename, hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

AutoRun Program Details

Retrieves information about the Autorun applications found in the Windows Registry. This sensor uses cached data; you can use the **Incident Response - Generate Autorun Cache [Windows]** package to regenerate this data.

This sensor is available for Windows endpoints.

There are no parameters that you can edit for this sensor. This sensor returns data that provides information about the Autorun applications found in the Windows Registry is displayed in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Autoruns by Category

Retrieves Autorun data for the enabled auto-start extension points (ASEPs). Use parameters to specify the category and hash for each ASEP. Note: This sensor uses cached data; this cached data can be regenerated with the **Incident Response - Generate Autorun Cache [Windows]** package.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Algorithm	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, SHA256, PESHA1. PSHA265, or IMP.
Autoruns Category	Select the category of the autoruns applications in the results. You can select Logon and Authentication, Application, or System.
Include Binaries with Microsoft as Publisher	You can select this parameter to include binaries that identify Microsoft as the publisher. Be aware that it is possible for this designation to not be genuine.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides information about the Autorun applications found based on the provided criteria in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Certificate Search

Enables searching for installed certificates. You can search by SHA1 hash. The default is to return all installed certificates.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
SHA1 Hash	Enter the SHA1 hash that corresponds with the certificate you are searching for.
Certificate Name	Enter the name that corresponds with the certificate you are searching for.

This sensor returns data that provides information about the certificates found based on the provided criteria in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Cleared Windows Security Event Log Search

Retrieves events generated when the Windows Security Event Log has been cleared.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Number of Days to Look Back	Select the number of days to look back. The maximum is seven days.
Include Domain Controllers in Event Search	Select to include domain controllers in the results of endpoints on which the Windows Security Event Log has been cleared in the specified time.

This sensor returns data that provides information about the endpoints on which the Windows Security Event Log has been cleared based on the provided criteria in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Command Line of Process

Returns the command line of any process by process name.

This sensor is available for Linux, macOS, and Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Process Name (Regular Expression)	A regular expression that matches the process name.

This sensor returns data that provides information about command lines of processes that match the provided regular expression in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Command Line with Hash Match

Returns the following information for any running process matching the specified hash: process, command line arguments of the process, and the module used by the process.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, or SHA256.
Hash to Match	Enter the hash that corresponds to the value you selected in the **Hash Type** parameter.

This sensor returns data that provides information about the running process matching the specified hash including the process, command line arguments of the process, and the module used by the process in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

DLL Load Order Hijacking Search

Searches for instances where DLL search order hijacking might have occurred in currently running processes. False positives are possible, so you must manually verify the results.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Exclude Signed Libraries	Select this option to return only unsigned potentially hijacked DLLs. Be aware that it is possible for this designation to not be genuine; for example, the signature of a library is not validated to confirm any authenticity.

This sensor returns data that provides information about the process name, DLL path, DLL MD5 hash, whether or not the DLL is signed, the reason for determining that the DLL is hijacked, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Driver Details with Hash

Retrieves information about loaded device drivers, including a hash of each driver file.

© 2025 Tanium Inc. All Rights Reserved

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides information about the display name, state, path, version, hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Environment Variables

Retrieves environment variables.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Variable	The environment variable to search for; for example, HOME or PATH.

This sensor returns data that provides information about the corresponding value for the provided variable in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Established Connections with Hash

Retrieves information about established connections with the hash value of the connected processes.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each autorun application in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides information about the process, hash, name, and target IP in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Explicit Logon Security Event Log Search

Searches the Windows Security Event Log for explicit logon events.

This sensor is available for Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Subject User Name	This value represents the username of the account that performed the action logged by the event.
Subject Domain Name	This value represents the domain to which the subject is associated.
Target User Name	This value represents the user account or resource being acted upon. It represents the recipient or object of a specific system action. For example, in an access attempt or permission modification, the target username indicates which account or resource is being affected.
Target Domain Name	This value represents the domain being acted upon.
Target Server Name	This value represents the server being acted upon.
Include Logons to Localhost?	Select this value to include logons to localhost in the results.
Enable Output from Domain Controllers?	Select this value to enable details from domain controllers to be reported in the results grid.
Look Back Hours	Enter the number of hours in the past that you want to include in the results grid.

This sensor returns data that provides information about the subjects and targets in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

File Certificate Details

Provides details about embedded certificates in Unix PE and COFF format image files.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
PE/COFF Executable File to Examine for Certificates	The full path to the image file for which you want to view certificates.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides information about the filename of the executable for which you want to find certificates, the subject of an associated certificate, the serial number of the associated certificate, valid dates for the associated certificate, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

File Handle Details

Retrieves information about the specified file handle that matches the input string. When a file is opened by a process, a file handle is associated with it until either the process terminates or the handle is closed. The file handle is used to identify the file in many function calls.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
File Handle String to Match (Regular Expression)	Enter a PCRE regular expression that matches the file handle that you want to find.

This sensor returns data that provides information about the process that created the file handle, the PID of the file handle, the user associated with creating the file handle, the handle ID, and a path to the handle in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

File Handles Of Process

Finds the file handles that are currently open in the specified process. The parameter is a regular expression of the process name. When a file is opened by a process, a file handle is associated with it until either the process terminates or the handle is closed. The file handle is used to identify the file in many function calls.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Process Name to Match (Regular Expression)	Enter a PCRE regular expression that matches the process for which you want to find associated file handles.

This sensor returns data that provides information about the file handles created by the process in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

© 2025 Tanium Inc. All Rights Reserved

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Has Incident Response ID Files

Identifies the Incident Response ID files that exist on a machine. For example, "irsearch1234".

This sensor is available for Windows endpoints.

Legacy versions of Tanium Incident Response provided files that were deployed to endpoints that were used to search and gather artifacts.

This sensor returns data that provides information about the Incident Response ID files in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

Has Scheduled Task

Returns whether the specified scheduled task exists.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Scheduled Task Name	Enter the name of a scheduled task.

This sensor returns data that provides a boolean value that indicates whether or not a scheduled task exists and the number of findings for each returned scheduled task in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Hash Of File

Returns the hash digest in the chosen algorithm of a specified file path.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.
File to Hash	Enter the full path of the file you want to hash. For example, `c:\windows\notepad.exe`.

This sensor returns data that provides a hash value for each matching file in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

© 2025 Tanium Inc. All Rights Reserved

Hosted Services Name Audit

Returns the Windows Service Group Name and a sorted list of service names in each group.

This sensor is available for Linux, macOS, and Windows endpoints.

This sensor returns data that provides the service group to which the hosted service is associated, the list of hosted service names, and count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

iCloud Settings

Displays all iCloud settings for all users by default. You can search by user, iCloud setting, or both.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
User Name	The name of the user associated with the iCloud setting.
Setting	The name of the iCloud setting to search for. For more information about iCloud settings, see https://support.apple.com/

This sensor returns data that provides the user associated with the setting, the setting name, a boolean value that indicates if the setting has been set, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Injected Threads

Returns threads executing possibly injected code. This is determined by finding thread start function addresses not mapped to a file on disk.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Show PID/TID	By default is unchecked and will display [omitted] for both PID and TID. Check this box for both process and thread IDs to be displayed.
Show Omitted Results	By default believe false positives will be omitted from results. Select this setting to see all possible false positive results.

This sensor returns data that provides:

© 2025 Tanium Inc. All Rights Reserved

- The full path of the process. This shows mismatches found between process and kernel paths.
- The PID provided that the Process ID when Show PID/TID is selected.
- The TID provided the Thread ID when Show PID/TID is selected.
- The header which corresponds to the first 2 bytes of allocated memory region in hex.
- The mapped file which corresponds to the file mapped to this memory region or No Mapped File. The memory type which corresponds to the type of the pages in the memory region such as `MEM_MAPPED` or `MEM_PRIVATE`.
- Allocated Protection which corresponds to the protection of the memory region when allocated such as `PAGE_EXECUTE_READWRITE` or `PAGE_EXECUTE_WRITECOPY`.
- Page Protection which indicates if protection of the page in the memory region such as `PAGE_EXECUTE_READWRITE` or `PAGE_EXECUTE_WRITECOPY`.
- Start Address which indicates the Win32 thread function start address.
- Region size which indicates the total size of the allocated memory region the Win32 thread function start address is in. When no suspicious threads are found, "No injected threads found" is returned.

All data appears in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Is File Digitally Signed

Checks whether or not the specified file is digitally signed. Uses the Windows WinVerifyTrust API to verify the signature embedded in the file.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File to Check	Enter the full path of the file you want to check. For example, `c:\windows\notepad.exe`

This sensor returns data that provides boolean value that indicates if the file has been digitally signed, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Linux AutoRuns

Linux AutoRuns and their types, from known categories such as Systemd.

This sensor is available for Linux endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hash Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.

This sensor returns data that provides the path, name, executable, category, command line, hash and a number of findings of the autorun file in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Listen Ports with Hash

Identifies listening TCP ports, including the process listening to the port, the hash of the process, the display name of the process (if available), and the listening IP Address and port.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the process listening to the port, the hash of the process, the display name of the process (if available), and the listening IP address and port in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Loaded Modules Not Matching Whitelist

Lists the MD5 hash and fully-qualified path of any loaded modules that are not on the current MD5 whitelist.

This sensor is available for Linux, macOS, and Windows endpoints.

This sensor returns data that provides the path of the loaded module that does not match the whitelist, the MD5 hash of the module, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Loaded Modules Of Process

Lists the modules loaded by the specified process. The parameter is a regular expression of the process or module name.

This sensor is available for Linux, macOS, and Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Process or Module Name (Regular Expression)	Enter a regular expression that matches the process or module name.

This sensor returns data that provides the loaded modules of a process that matches the regular expression you provided and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Loaded Modules with Hash

Displays the fully-qualified path and hash of each loaded module.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the path and hash of the loaded module and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Logon Security Event Log Search

Searches Windows Security Event log and equivalent logging sources on macOS for logon events.

This sensor is available for macOS and Windows endpoints.

Sensor parameters

Parameter	Description
User Name	The user name that is associated with the events you want to search.
Domain	The domain you want to search.
Hours to Look Back (Max 168)	Select the number of hours to look back. The maximum is 168 hours.
Logon Type	Select the logon type to search for.
Include Domain Controllers in Event Search	Select to include domain controllers in the results of endpoints on which the Windows Security Event Log has been cleared in the specified time.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides the date of the logon security event, the user associated with the logon, the domain that was logged into, the type of logon, and an a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac AutoRuns

Mac AutoRuns and their types, from known categories such as launch agents, launch daemons, startup items, user login items, and kernel extensions.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
Hash Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
Include Apple Signed Items	Select this setting to include autoruns that are signed by Apple in the results.

This sensor returns data that provides the path to the autorun file, the name of the autorun file, the executable, category, command line, hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Downloaded Files

Queries the `~/Library/Preferences/com.apple.LaunchServices.QuarantineEvent*` file for downloaded files.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
User Name	Enter the user name of the user for which you want to search for download activity.
File Name	Enter a comma separated list that includes the file names that you want to search for to see if a user has downloaded them.

This sensor returns data that provides the user, file GUID, time stamp, identifier, app, URL, sender name, sender address, download type, origin title, origin URL, origin alias and count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Firewall Settings

Enumerate the firewall settings on macOS.

© 2025 Tanium Inc. All Rights Reserved

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
Setting	Enter the macOS firewall setting that you want to search for. For more information about macOS firewall settings, see https://support.apple.com/.

This sensor returns data that provides the setting name, the status of the setting, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Gatekeeper Settings

Enumerate the Gatekeeper settings on macOS.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
Setting	Enter the macOS Gatekeeper setting that you want to search for. For more information about macOS Gatekeepr settings, see https://support.apple.com/.

This sensor returns data that provides the setting name, any notes about the setting, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mac Kext Details

Allows you to find allowed kernel extensions on a macOS endpoint.

This sensor is available for macOS endpoints.

Sensor parameters

Parameter	Description
Team ID	The team ID that corresponds with the team for which you want to search Kext details.
Bundle ID	The bundle ID that corresponds with the bundle for which you want to search Kext details.

This sensor returns data that provides the path, team ID, bundle ID, boot UUID, create time, last seen time, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

MD5 Hash Of File

Returns the MD5 hash for a file at a specified path.

© 2025 Tanium Inc. All Rights Reserved

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File	Enter the full path of the file for which you want to see the hash.

This sensor returns data that provides the hash of the provided file in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

MD5 Hash Match Files Executing

Retrieves a fully-qualified path of an executable file for a running process that matches the specified MD5 hash. Results also indicate if the file is executing.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
MD5 Hash to Match	Enter an MD5 hash to match a process.

This sensor returns data that provides the process that matches the provided hash and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

MD5 Hash Single File Match

Indicates whether the file at the specified path matches the specified MD5 hash.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File	The full path of the file you want to seach for.
MD5	The MD5 hash of the file you want to match to the file you are searching for.

This sensor returns data that provides a boolean value that indicates if the file and hash match and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mutex Details

Returns details about a specified mutex object, including process, PID, user, handle ID, and mutex name.

This sensor is available for Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Mutex String to Match (Regular Expression)	Enter a PCRE regular expression that matches a process, PID, user, handle ID, or mutex name that matches a specific mutex you want to find.

This sensor returns data that provides the process, PID, user, handle ID, mutex and a count of findings of matches to the regular expression you provided in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Mutex Handles Of Process

Returns the open handles to file mutex objects for a specified process. The parameter is a regular expression for a process name.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Process Name to Match (Regular Expression)	Enter a PCRE regular expression that matches a process that matches a specific mutex you want to find.

This sensor returns data that provides the mutex handle and a count of findings of matches to the regular expression you provided in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Network Details

Enumerates verbose network connection details.

This sensor is available for Linux, macOS, and Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hostname or IP	The hostname or IP address of the network for which you want to view details.
Hashing Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the process name and ID, the parent process, the path to the process, the hash of the process, the protocol, local IP address and port, remote IP address and port, and the state in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Non-Approved Established Connections with Hash

Lists information about established connections that were opened by a prohibited process or to a prohibited destination. Returns the process responsible for the connection, the hash of the process, the display name of the process (if available), and the target IP Address and port. Processes and IP ranges can be excluded in the sensor definition.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the process, the hash of the process, the name of the process, and the target IP in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Original Filename

Gathers the original filename for that binary on disk. This is a potential indicator that someone has renamed a legitimate binary. For example, copying and renaming the `cmd.exe` binary to a different location in an attempt to avoid detection.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
File Path	Enter a full path to the file you want to investigate. For example, `c:\windows\notepad.exe`.

This sensor returns data that provides the file path, the original filename, the internal filename, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

© 2025 Tanium Inc. All Rights Reserved

PowerForensics File Record

Retrieves the Master File Table (MFT) modified, accessed, changed, and born times for a specified file name. Returns file name, STANDARD_INFORMATION (SI) time stamps, and FILE_NAME (FN) time stamps. All time stamps are returned in UTC format.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Specify the Path to a Folder or File	Enter the full path to a file of a folder. For example, `c:\windows` or `c:\windows\notepad.exe`.

This sensor returns data that provides the file name, SI modified time, SI accessed time, SI changed time, SI born time, FN modified time, FN accessed time, FN changed time, and FN born time in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

PowerForensics Master Boot Record

Retrieves the operating system name, enumerated through WMI, and the MD5 hash of the master boot record (MBR) code section.

This sensor is available for Windows endpoints.

This sensor returns data that provides the operating system of managed endpoints and the MD5 hash of the master boot record in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

PowerForensics Prefetch

Searches prefetch entries for previously executed applications with a provided file path.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Path	Enter a relative path to an executed application that you want to search for.
Volume Name	Enter the volume name you want to search. If a value is not entered the volume defaults to `%SystemRoot%`.

This sensor returns data that provides the name of the executed application and the path to the executed application in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

© 2025 Tanium Inc. All Rights Reserved

PowerForensics Recently Opened Office Files by User

Returns the path of any recently opened Office files by a user. Requires PowerShell 2.0 or later.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Username	Enter the username of the user associated any recently opened office files you want to seach for.

This sensor returns data that provides the name of any recently opened office files and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

PowerForensics Shim Cache

Retrieves executables that might have been run from entries in the Microsoft Application Compatibility section of the registry. If an Explorer window is opened to a location for a given executable, a shim cache entry might be created even if the executable was never run.

Example output: `C:\Windows\System32\cmd.exe^N/A Verbose`

Example output: `C:\Windows\System32\cmd.exe^2016-04-11 14:28.`

A common use case for this sensor is to search for shim cache AppData entries.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Path to Match	Enter a path to search for.
Verbose Timestamp	Select this setting to display the timestamps in the results grid in a verbose format.
Include Tanium Client Entries	Select this setting to include entries that are associated with the Tanium Client.

This sensor returns data that provides the path to executables that might have been run from entries in the Microsoft Application Compatibility section of the registry and their last modified time in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Process Details

Returns verbose details about running processes.

This sensor is available for Linux, macOS, and Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hashing Algorithm	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.
Hostname or IP	Enter a hostname or IP address for the endpoint on which you want to find details about running processes.

This sensor returns data that provides the process name and path, the user associated with the process, the process ID, parent process ID, hash, and command line of the process in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Processes Using Module

Lists processes that use a specified module.

A common use case for this sensor is to search for processes that are loading PowerShell automation DLL.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Module to Search For	Enter a module to search for to view a list of processes that use it in a results grid.

This sensor returns data that provides the process and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

RDP Client History

Returns local profile, RDP target name or IP, and remote logon name for a remote desktop client. Note that if an attacker starts the RDP client with the /Public option, then this information is not recorded in the user profile registry hive.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Account Searching String	Enter the account you want to search.
Host Search String	Enter the host you want to search.
Max Returned per Host	Select the maximum number of results to return per host.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides the local profile, the RDP target name or IP address, the remote logon account, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Remote Desktop Event Log Search

Retrieves the most recent RDP events from the Terminal Services Event Log.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Look Back Hours (Maximum 168)	Enter the number of hours to look back.
Include Domain Controllers in Event Search	Select to include domain controllers in the results.

This sensor returns data that provides the time, target hostname, account name, account domain, source IP address, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Run Command History

Lists the commands that were run from the Windows command prompt field on the Start menu.

This sensor is available for Windows endpoints.

This sensor returns data that provides the name of the user who ran a command, and the command that they ran in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Running Processes With Filename Mismatch

Gathers running processes and inspects the original filename for that binary on disk. If the running process and the binary original filename are different, results return. This is a potential indicator that someone has renamed a legitimate binary. For example, copying and renaming the `cmd.exe` binary to a different location in an attempt to avoid detection.

This sensor is available for Windows endpoints.

This sensor returns data that provides the name of the process, the original filename, internal filename, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

© 2025 Tanium Inc. All Rights Reserved

Running Processes with Hash

Lists the fully-qualified path and hash of each running executable.

This sensor is available for Linux, macOS, and Windows endpoints.

Parameter	Description
Hash Type	Select the hashing algorithm to use to display each matching file in the results. You can select MD5, SHA1, or SHA256.This sensor returns data that provides.

the path of the process, the hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.
For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Running Processes with MD5 Hash

Lists the fully-qualified path and MD5 hash of each running executable file.

This sensor is available for Linux, macOS, and Windows endpoints.

This sensor returns data that provides the path of the process, the hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Scheduled Tasks

Returns scheduled tasks on a system, created either with "at" or "schtasks". Time and frequency information is omitted to limit unique strings.

This sensor is available for Windows endpoints.

This sensor returns data that provides the task name, the command, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Semaphore Details

Returns details about a specified semaphore.

Example: `symphony.exe|2400|WIN764\Administrator|2B4|\BaseNamedObjects\daemon242861781sem`.

This sensor is available for Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Semaphore String to Match (Regular Expression)	Enter a PCRE regular expression that matches a semaphore that you are searching for. For more information on semaphores, see https://learn.microsoft.com/en-us/windows/win32/sync/semaphore-objects

This sensor returns data that provides the process, PID, user associated with the semaphore, handle ID, and semaphore in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Module Details

Lists services that are running at the time the Question is asked. The details include the path to the service executable (if it is a stand-alone service), the module (DLL) path (if it is a hosted service), and the loaded modules if the service implements a COM application.

This sensor is available for Windows endpoints.

This sensor returns data that provides the service name, service caption, image path, module path, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Module Details with Hash

Collects a comprehensive list of stand-alone services, hosted services, COM+ application components, and the selected hash (MD5, SHA1, and SHA256) of the binary.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the name, caption, image path, binary path, hash of the binary in the selected algorithm, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Process Details

Returns verbose details about running processes for services.

This sensor is available for Linux, macOS, and Windows endpoints.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters

Parameter	Description
Hostname or IP	Enter the host name or IP address of the endpoint that you want to search for service process details.

This sensor returns data that provides the name of the process, the display name, the process ID, the process path, the start type, the service type, the user associated with the process, the status of the process, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service Status with Hash

Provides information about each of the Microsoft Windows Services that are installed on the endpoint, including the hash and whether the service is running.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Hash Type	Select the hashing algorithm to use to display in the results. You can select MD5, SHA1, or SHA256.

This sensor returns data that provides the short name of the service, the long name of the service, the service status, the account associated with the service, the command line, hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Service System Event Log Search

Searches and stacks Windows service start, stop, or install entries in the System event log that occurred within a specified time period.

Common use cases for this sensor are searching to find if credential theft services or the PsExec service has been installed recently.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Service Name	Enter one or more | seperated services to search for. For example, `(wce|pwdump|cachedump|gsecdump|fgdump).`
Service State	Select a service status; Service Installed, Service Started, or Service Stopped.
Lookback Hours	Enter the number of hours in the past to look back.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides the date of the service state, the service name, service information, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SHA1 Hash Match Files Executing

Matches a specified SHA1 hash against files that are currently executing. Returns the paths to matching executing files, and "Yes", or "No" if no executing files match.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
SHA1 Hash to Match	Enter a SHA1 hash to search for.

This sensor returns data that provides the matches for the provided SHA1 hash, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SHA1 Hash Single File Match

Compares the file at a specified path to a provided SHA1 hash. Returns "Yes" if the file at the specified path matches the hash.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Full Path of File to Check	Enter the full path of the file to check. For example, `c:\windows\notepad.exe`.
SHA1	Enter the SHA1 hash of the file to check.

This sensor returns data that provides a boolean value that indicates whether or not the file exists with the matching hash in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SHA1 Hash Of File

Returns the SHA1 hash of a specified file path.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
File to Hash	Enter the full path of the file to hash.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides the matches for the provided file, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Shell History

Returns the requested command(s) from the shell history files of all users (if found), or only one user if specified.

This sensor is available for Linux and macOS endpoints.

Sensor parameters

Parameter	Description
User	Enter a user that you want to search the shell history of.
Command	Enter a command that you want to search the shell history of.

This sensor returns data that provides the user, commands, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SIP Settings

Returns the SIP settings on macOS endpoints. If all components are enabled, you see only one line "System Integrity Protection status: enabled." Otherwise, each component appears with a status.

This sensor is available for macOS endpoints.

This sensor returns data that provides the component, setting, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

SSH Known Hosts

Retrieves entries from the `.ssh/known_hosts` file for a user.

This sensor is available for Linux and macOS endpoints.

Sensor parameters

Parameter	Description
User	Enter the user for which you want to see the entries of the `known_hosts` file.
Hostname	Enter the hostname of the endpoint on which you want to see the `known_hosts` file.

This sensor returns data that provides the user, host, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

© 2025 Tanium Inc. All Rights Reserved

Trace DNS Queries

Returns historical data from each endpoint regarding DNS queries.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Process Path	The path of the process to be found. For example, `jane.smith\software.exe`.
Username	The username that executed the process.
Query	Enter the DNS query to search for.
Response	Enter the DNS response to search for.
Operation	Enter the DNS operation to search for.

This sensor returns data that provides the process name, the query, the response, the operation and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

© 2025 Tanium Inc. All Rights Reserved

Trace Executed Process Hashes

Returns the MD5 hashes of process executed within a specified time range.

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Max Results Per Host	Enter the maximum number of results to return from each host.

This sensor returns data that provides the MD5 hash for executed processes in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Executed Process Trees

Generates process trees from a process name (regex). With "As Parent" the specified process name appears at the top of the tree. With "As Child" it appears at the bottom.

Common use cases for this sensor are to search for:

- Adobe Reader as parent process - Search to discover if acrord32.exe is being used as the parent process responsible for initiating any child processes.
- Command Shell as child process - Search to discover if cmd.exe is the child process of any suspicious parent processes.
- Command Shell as parent process - Search to discover if cmd.exe has initiated any suspicious child processes.
- Net Command as child process - Search to discover if net.exe is the child process of any suspicious parent processes.
- Office application as parent process - Search to discover if any Microsoft Office applications (outlook.exe|winword.exe|excel.exe) has initiated any suspicious child processes.
- PowerShell as child process - Search to discover if powershell.exe is the child process of any suspicious parent processes.
- PowerShell as parent process - Search to discover if powershell.exe has initiated any suspicious child processes.
- PsExec Service as parent process - Search to discover if psexesvc.exe has initiated any suspicious child processes.

© 2025 Tanium Inc. All Rights Reserved

- Web Browser as parent process Search to discover if a web browser (firefox.exe|chrome.exe|iexplore.exe) has initiated any suspicious child processes.
- WMI Service as parent process = Search to discover if wmiprvse.exe has initiated any suspicious child processes.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Process Name	Specifies the process name.
Treat Inputs as Regular Expressions	Treat input strings as regular expressions. By default, this option is cleared, and input is treated as a simple case-insensitive substring match.
Use Full File Paths	Select this option to use full file paths in the results grid.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Process Context	Select one of the following values to specify where the process appears in the tree: "As Child" or "As Parent". By default, this value is set to "As Child".
Number of Events to Search	Specifies the number of events to search.
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
All Times UTC	Select this option to display all times in UTC format.

This sensor returns data that provides the executed processes and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Executed Processes

Returns historical data from each endpoint regarding process executions.

Common usse cases for this sensor are to search for:

- Adding user account with NET
- launching a Command shell by an unusual parent
- Decoding with Certutil

© 2025 Tanium Inc. All Rights Reserved

- Domain reconnaissance with NET
- JavaScript ran via rundll32 or MSHTA
- MacOS security_trampoline privilege escalation
- NET use to mount remote root share
- PowerShell spawned by script interpreter
- PowerShell suspicious command line arguements
- PowerShell version downgrade attack
- ProcDump dumping LSASS memory for credential stealing
- PsExec child processes
- Remote task creation with at
- Volume shadow copy deletion
- WinRAR encrypted archive creation
- WMI remote command execution

This sensor is available for Linux, macOS, and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters (continued)

Parameter	Description
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Process Path	The directory and file name of the executed process.
Parent Process Path	The directory and file name of the parent process.
Command Line	Arguments supplied to the executed process; might or might not include full path, depending on how the process was launched.
MD5 Hash	The hash of the process executable file.
Domain	The domain or system context for the user that executed the process, for example CORP.
Username	The username that executed the process, for example `joe.smith`.

This sensor returns data that provides the parent process path, the process path, command line, MD5 hash and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace File Operations

Returns historical data from each endpoint regarding filesystem activity.

Common use cases for this sensor are to search for:

- *nix persistence with SSH authorized_keys
- Creation or modification of user startup files
- Delete shell history
- Executable created by Java
- Executable created by PDF readers
- Files in recycle bin boot
- PowerShell profile modified or created

© 2025 Tanium Inc. All Rights Reserved

- Processes in AppData changing document files
- RAR file creation
- Script creation in web accessible folders

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
File Path	The full path to the file you want to search for.
File Operation	The operation on the file, for example CreateNewFile, Write, DeletePath, or RenamePath.
Process Path	The path of the process executing the operation, for example `system32\cmd.exe`.
Domain	The domain or system context for the user that executed the process responsible for the file operation, for example `CORP`.
Username	The username that executed the process responsible for the file operation, for example `joe.smith`.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides the file path, the process path, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Image Loads

Returns historical data from each endpoint regarding Image Loads.

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Process Path	The directory and file name of the executed process.
Image Path	The directory and file name of the image.
Image Hash	The MD5 hash of the image.
Image Signed	Indicates whether or not the image is signed.
Signing Entity	Indicates the signer of the image.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides the process name, the image path, the image hash, and the signing entity in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Loaded Drivers

Returns historical data from each endpoint regarding loaded drivers.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Driver Path	The Windows path and device driver filename, for example `windows\system32\driver.sys`.
Driver Hash	The hash of the specified driver file.
Driver Signed	Select one of the following values to specify whether the device driver is signed: "Yes", "No", or "Either". By default, this value is set to "Yes."
Signing Entity	The name of the vendor that signed the file.

© 2025 Tanium Inc. All Rights Reserved

This sensor returns data that provides the driver path, the driver hash, the signature of the driver, the signing entity and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Logon Events

Returns historical data from each endpoint regarding logon events.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Max Database Rows	Indicates the maximum number of rows to process when the sensor runs.
Domain	The domain to be searched for the process, for example `CORP`.
Username	The Active Directory username associated with the user account.
Source Host	The host name or IP address of one endpoint that is the target for sensor execution.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters (continued)

Parameter	Description
Logon Process	The file name of the executable that launched the logon process.
Logon Type Number	A number indicating the logon type. This must be one of the following options: 2: Interactive 3: Network 7: Unlock 10: Remote Interactive.
Logon Provider	The process associated with the logon event.

This sensor returns data that provides the source user, the source domain, the target user, the target domain, the login result, the logon type, the logon provider, the proces, the source host, the source IP address and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Network Connections

Returns historical data from each endpoint regarding network connections made by processes.

A common use case for this sensor is searching for PowerShell HTTPS connections.

This sensor is available for Linux and Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters (continued)

Parameter	Description
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Include 127.0.0.1 Traffic	Select to include network connections from the localhost. This option assumes that the localhost is the device running Tanium Console. By default, traffic from the localhost is included.
Local IP Address	If the sensor is targeted to a single host, the IPv4 address of the device.
Local Port	The port number from which the connection was made on the targeted host.
Remote IP Address	The IPv4 address of the destination.
Remote Port	The number of the port to which the connection was made.
Process Path	Use this option to specify the process path of the process to be found.
Domain	The domain to be searched for the process, for example `CORP`.
Username	The Active Directory username associated with the user account.

This sensor returns data that provides the process image path, the operation, the remote IP address, the remote port, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Trace Registry Keys or Values

Returns historical data from each endpoint regarding registry activity.

Common use cases for this sensor are searching for:

- Image file execution debugger value
- RDP tunnel configuration
- Run key changes
- Sdclt.exe UAC bypass

© 2025 Tanium Inc. All Rights Reserved

- Service dll changes
- Service imagepath changes
- UAC notification manipulation

This sensor is available for Windows endpoints.

Sensor parameters

Parameter	Description
Time Range	Returns historical results within the selected relative time range for each endpoint, by default from one hour ago until now, or uses the range set in the Absolute Time Range option only if that option is specified.
Absolute Time Range	Returns historical results within the selected Absolute Time Range for each endpoint, only if values are provided.
All Times UTC	Select this option to display all times in UTC format.
Treat Inputs as Regular Expressions	Select this option to use regular expressions in input fields.
Output only Yes or No	Select this option to have Yes and No returned for all matches to search parameters.
Max Results Per Host	Enter the maximum number of results to return from each host.
Remove Endpoint Name, Username, and Timestamps to Stack Results	Select this setting to omit columns that are likely to be unique per host.
Registry Key Path	The registry key path to search the target computer group for, for example `HKLM\Software\VendorName\`.
Registry Value Name	The key value to search the target computer group for, for example "Setting name" in `HKEY_CURRENT_USER\Software\Vendor's name\Application's name\Version\Setting` name.
Operation	The type of registry event, for example SetValueKey, DeleteKey, or DeleteValueKey.
Process Path	The path of the process to be found.
Domain	The domain to be searched for the process, for example `CORP`.

© 2025 Tanium Inc. All Rights Reserved

Sensor parameters (continued)

Parameter	Description
Username	The Active Directory username associated with the user account.

This sensor returns data that provides the registry key, the key value, the operation, the process path, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Windows Audit Policy

Retrieves the Windows Audit Policy; Trace records the operating system audit data typically seen in the Windows Security Event Log. This policy can be altered. However, if Group Policy is set, it might overwrite the log.

This sensor is available for Windows endpoints.

This sensor returns data that provides the category, subcategory, activity rating, audit status, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

Windows Credential Security Settings

Returns the results of 10 Windows configuration settings that affect security.

This sensor is available for Windows endpoints.

This sensor returns data that provides the setting name, the setting value, and the OS version in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

WMI Event Consumers

Lists Windows Management Instrumentation (WMI) event consumers. Returns script path for `ActiveScriptEventConsumers` and command for `CommandLineEventConsumers`.

This sensor is available for Windows endpoints.

This sensor returns data that provides the name, class, command line template, and a count of findings in a results grid. You can customize the columns that appear in the results grid, and export the data to a CSV file.

For any result, you can issue further Tanium questions to drill-down on the match, or deploy an action.

© 2025 Tanium Inc. All Rights Reserved

Managing Threat Response alerts

When Threat Response detects a match to intel that you have deployed to a computer group, an alert is generated from the endpoint and reported back to Threat Response. You can view alerts in the Alerts page or in individual intel documents.



You can view alerts that have been generated from endpoints that belong to computer groups for which you have permissions to access. For example, you can view alerts on endpoints for which the active persona belongs to at least one management rights group to which the endpoint belongs. If the current user belongs to at least one management rights group to which the endpoint is a member of, alerts for that endpoint are visible. The Threat Response Administrator role has access to view all alerts. To provide other roles visibility into all alerts, assign the **Threat Response Visibility Bypass** permission to those roles.

If an endpoint is offline for longer than the configured value of the **Max Endpoint Age (Days)** setting in Tanium Interact, only the users with the **Threat Response Visibility Bypass** permission can view alerts and saved evidence for the endpoint. If such an endpoint comes back online, alerts and saved evidence become visible to users with the correct permissions.

Background and On-demand scans, regardless of the intel type, are throttled to ensure they do not overuse endpoint resources. All Tanium Client extensions in total consume no more than 5% of the available CPU resources on each endpoint.

On-demand scans that trigger endpoint throttling cause the endpoint to throttle background scan alerts for the effective period of the throttle, which is one hour by default.

To ensure the performance and health of the database, Threat Response prunes the alerts table in the Threat Response database every five minutes. Pruning occurs when the `alert.pruning.shouldPrune` setting in the API is set. By default, this setting is disabled in on-premises environments. Tanium Cloud does not support disabling alert pruning. To toggle pruning on-premise, use a PATCH method request to `/plugin/products/threat-response/api/v1/settings/alert.pruning.shouldPrune` with the value set to `true` to enable.

Pruning removes all alerts except for the latest 100,000 alerts that are not assigned the status of **In Progress** or **Resolved**. Alerts that are assigned the status of **In Progress** or **Resolved** are never pruned. Threat Response then determines if there are any alerts that are not assigned the status of **In Progress** or **Resolved** that are older than 60 days, and prunes them from the database. Finally, Threat Response checks for any intel that has created the vast majority of alerts and deletes 90% of the oldest alerts for that intel and keeps only the newest 10%.

View alerts

From the Main menu, go to **Modules > Threat Response > Alerts**. At the top of the page all of the alerts across the endpoints in an environment display ranked by endpoint with most alerts, event type, the intel document that initiated the alert, the path to the file or process that initiated the alert, the status of the alert, and a range of dates were the alert was detected. Click any of the fields in the rankings to create filters that display alerts that match the criteria you selected.

© 2025 Tanium Inc. All Rights Reserved

Specify any additional criteria to filter Alerts. For example, create filters to display alerts based on endpoint, event type, path, intel name, label, or MITRE technique. Click Advanced Details to view more information about the endpoint on which the alert occurred, the process that caused the alert, and the intel document that matched the alert.

Decode encoded text

You can decode encoded text in many places in the Threat Response workbench without having to copy and paste to a third-party tool. For example, you can decode all command line locations in the advanced details for a Threat Response alert.

1. For any encoded text item, click Decode.
2. Select the **Encoding Schema** of the encoded text.
3. Select the character encoding standard for output of the decoded text. You can select either UTF-8 or UTF-16LE. This option is not available for all encoding schemas.
4. Click **Decode**. The decoded results appear in the **Output** section of the page. You can copy the results to the clipboard.

> NOTE
>
> From any location in the Threat Response workbench, press `ALT + \` (Windows and Linux) or `Command + \` (macOS) to display the editor to decode encoded text. On some keyboards it is common for mappings to replace the / key (Scan Code 2B) with other characters, for example, the # character. On such keyboards, use the appropriate key combinations for the locale of the keyboard.

An alert that results from a Signal that matches signature status can display the following signature status values:

- Unverified - The signature could not be verified.
- Verified - The signature was verified and passed policy requirements.
- No Signature - The file had no signature.
- Error - There was an error processing the signature. For example, an antivirus solution could be preventing access.
- Disallowed - The signature was explicitly disallowed by the operating system.
- Not Trusted - The signature was not from a trusted source.
- Not Trusted Policy - The signature was disallowed based on policy settings.
- File Does Not Exist - The file did not exist at the time the check occurred.
- Checking Disabled - Recorder was configured not to check signature for this file type.
- Timed Out - The request to check the signature timed out before it could complete.

Assign a status to an alert

© 2025 Tanium Inc. All Rights Reserved

Assigning status to an alert enables incident response efforts to identify alerts that are being investigated or remediated. For example if you encounter a suspicious alert and you begin to take investigative actions, you can change the status of an alert to **In Progress**. Similarly when you have completed the remediation of an alert, you can assign the **Resolved** status to the alert. The Available statuses for alerts are:

- **Dismissed**
- **In Progress**
- **Resolved**
- **Unresolved**



The more quickly you can evaluate the risk associated with a given activity, the more quickly you can begin resolving a threat. Develop a plan for investigating and resolving alerts and be diligent about assigning alert statuses. Alert status dispositions are used to calculate the mean time to investigation and mean time to resolution; both key success metrics for Threat Response.

You can track the mean time to investigate alerts and the mean time to resolve alerts key performance indicators in Tanium Trends under the **Threat Response - Alerts** board. The mean time to investigate alerts is the average amount of time alerts are in the **In Progress** state over the last 7 days. The mean time to resolve alerts is the average amount of time between when alerts are created to when they assigned the **Resolved** state over the last 7 days.

Additionally when an alert is suppressed by a suppression rule, the status of an alert is **Suppressed**. This status is removed from a suppressed alert when the suppression rule is removed.

View alerts by intel document

From the Main menu, go to **Modules > Threat Response > Intel**. To open a single piece of intel, click the name of the item. From the individual page, you can review alerts that are associated with the intel, the activity over the last 30 days, the MITRE technique ID, and you can edit the definition.

Each Signal can have one or more associated MITRE technique IDs. Technique IDs can categorize Signals to better align with the MITRE Attack Framework and help map coverage to the different tactics and techniques. You can filter alerts by technique ID.

You can also initiate on demand scans for intel documents from the intel page.

Microsoft Defender alerts

Microsoft Defender is an anti-malware component of Microsoft Windows. Use Windows Defender alerts to gain visibility into common areas of Windows for changes which might have been caused by spyware, malware, and general security events. Windows Defender integration requires enabling the **Consume Defender Alerts** setting in a detection configuration for a deployed profile. By default, this setting is enabled for new configurations. For existing configurations, this setting needs to be enabled.

© 2025 Tanium Inc. All Rights Reserved

To subscribe to Defender process actions, such as Event ID 1007, go to Settings and click **Service > Misc**. Select **Microsoft Defender Process Action**.

When Defender generates an alert on a Windows endpoint, an alert is generated in Threat Response that you can view in the alerts page. You can filter the alerts page for Defender alerts.

Deep Instinct alerts

Deep Instinct is a solution that applies deep learning to cybersecurity and adds next-generation AV capabilities to Threat Response by integrating the investigative abilities of Threat Response to Deep Instinct alerts. For example, you can use the quarantine, collection, investigation, and remediation capabilities from Deep Instinct Alerts in Threat Response. Deep Instinct alerts that are saved on the Deep Instinct cloud can leverage Tanium roles and permissions to control access to alert data, enabling customers to access Deep Instinct alert data in a GDPR compliant setting.

Deep Instinct integration is available on Windows and macOS endpoints. Deep Instinct integration requires enabling the Generate Deep Instinct Alerts setting in a detection configuration for a deployed profile. By default, this setting is disabled for new configurations. For alerts to be returned from endpoints, the Deep Instinct agent must be running on the endpoint. Deep Instinct alerts are throttled as to not cause performance issues on an endpoint.

When Deep Instinct generates an alert on an endpoint, an alert is generated in Threat Response that you can view in the alerts page. You can filter the alerts page for Deep Instinct alerts. Deep Instinct Alert details contain a **Deep Instinct** section that shows Event Type, Event Action, File Path, File Type, file Hash, and Signature where applicable.

> NOTE
>
> For the integration to work correctly, you must configure additional flags for the Deep Instinct Agent (D-Client) using the Deep Instinct CLI. For more information refer to the Deep Instinct documentation or contact Deep Instinct support.

Deep Instinct alerts feature a Deep Instinct section in the alerts details section of each Deep Instinct alert. Each alert shows one of the following event types from Deep Instinct:

- Deep Static Analysis – Detection
- Ransomware Behavior
- Arbitrary Shellcode
- Malicious PowerShell Command Execution
- Malicious JavaScript Command Execution
- Remote Code Injection
- Credential Dumping
- Suspicious Script Execution
- Reflective DLL Injection

© 2025 Tanium Inc. All Rights Reserved

- .Net Reflection
- AMSI Bypass
- Known Payload Execution



Threat Response does not generate alerts for Deep Instinct “Suspicious Events” events.

In addition to showing the Event Action that Deep Instinct took in response to the alert, You can view the file path and type of the artifact that caused the alert and the probability percentage that the detection was of several types of malware as calculated by Deep Instinct.

Investigate reputation data

Investigating reputation data requires the reputation service to be configured. See Reputation data on page 181 for more information.

For endpoints that use reputation intel, hashes found by the saved questions are sent to the reputation service for assessment. If this intel generates an alert, the hashes display with red or yellow status. Any known malicious matches automatically initiate an on-demand scan on targeted computer groups and generate an IOC for ongoing background scans. Each reputation IOC can contain up to 20 hashes. These IOCs are listed with **Reputation** as their source.

When the reputation for a hash changes, the intel is updated. For example, if a hash is no longer considered malicious according to reputation data, the associated intel document is updated so no further alerts are generated. If no malicious hashes exist in an intel document, the document is deleted.

1. To view more details about a hash, open the side panel. A hash can have one of the following ratings:
    - Non-Malicious (Green)
    - Malicious (Red)
    - Suspicious (Yellow)
    - Unknown (Gray)
    - Pending
2. Click a hash to view more details. For reputation data that comes from VirusTotal, you can expand the details and see a color-coded list of intelligence providers that have assessed the hash.

The Threat Response icon pulses while the on-demand scan is running. After the on-demand scan completes, you can use the Interact icon to view the detailed results of the scan. Alerts are generated and gathered asynchronously from the scan. Alerts might be displayed on the Alerts page before the scan completes.

Investigate alerts

If you have a suspicious alert, you can open a live connection to investigate further.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Threat Response > Alerts**. Select the alert that you want to investigate. You can investigate one alert at a time.
2. From the alerts results, click the name of the endpoint to which you want to open a live connection.
3. Click **Start live connection**.

The live endpoint page opens, with appropriate filtering for the type of alert you are investigating. Take a snapshot of suspicious endpoints for saved evidence.

Add alerts to an investigation in Tanium Investigate

Add to an Investigation in the Actions column to add the alert to an investigation in Tanium Investigate. With Tanium Investigate you can identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to issues more quickly. For more information, see Tanium Investigate User Guide.

Deploy an action to an endpoint

If you have a suspicious alert, you can deploy an action to a single affected endpoint directly from the alert.

1. From the Main menu, go to **Modules > Threat Response > Alerts**. Select the alert for which you want to deploy an action to remediate or perform other action.
2. Click **Actions > Deploy Action**.
3. The **Deploy Action** page appears and the targeted endpoint is identified.
4. Select the package that you want to deploy. Depending on the package that you select, you are prompted to provide parameters for the package. If you select a package for Live Response, you can specify the collection configuration and destination configuration you want to use for Live Response file collection.
5. Provide a unique name and description for the action.
6. If you do not want to deploy the action immediately, specify a start to create a scheduled action. The time refers to the system clock on the Tanium Server, not on the endpoint. For example, if you specify the action to deploy at 1:00 am, it deploys when the Tanium Server system clock time is 1:00 am.
7. Optionally specify an end time. This is important If you configure reissue intervals for the action, unless you are sure it is the type of action that you want to reissue indefinitely. If you are not sure, configuring the schedule to end in six months is better than running indefinitely.
8. You can schedule the action to repeat at intervals. Specifying to reissue an action creates a scheduled action. Specifying a reissue interval is appropriate when:
   - Action approval is enabled and you are not certain it will be approved before the action expires.
   - You want to be sure software or configuration updates are made not only to the clients currently online but also to those currently offline that will be predictably online within a window that the reissue interval defines.
   - The action is a continual hygiene practice. For example, you want to check periodically that a client service is running or a client configuration has a particular value.
9. Click **Deploy**. Confirm that you want to deploy the action.

© 2025 Tanium Inc. All Rights Reserved

Initiate a Response Action from an alert

If you have a suspicious alert, you can initiate a response action to a single affected endpoint directly from the alert. Initiating Live Response, Quarantine, or Gather Snapshot deploys a *response action*. A response action, unlike a scheduled action, runs once during a provided time range and ensures that if an endpoint is not online when you deploy the action, it runs when the endpoint comes online. Once deployed, from the Main menu, go to **Modules > Threat Response > Response Activity** to view the status or stop a response action.

1. From the Main menu, go to **Modules > Threat Response > Alerts**. Select the alert for which you want to deploy an action.
2. Click **Response Actions > Live Response**, **Response Actions > Quarantine**, **Response Actions > Gather Snapshot**, **Response Actions > Download File**, or **Response Actions > Unquarantine**.

   
   NOTE

   When you download a file as a response action, the file is saved as saved evidence. From the Main menu, go to **Modules > Threat Response > Saved Evidence > Files** to access the files that you download.
3. Provide parameters for the response action. For example, if you select the response action for Live Response, you can specify the collection configuration and destination configuration you want to use for Live Response file collection. For Quarantine response actions you must select the quarantine profile to use. Changes to the profiles or rules after a quarantine has been applied on an endpoint has no effect on that endpoint unless it is unquarantined and requarantined.
4. Click **Run**. Confirm that you want to deploy the response action.

You can select up to 100 alerts to assign quarantine and unquarantine response actions to at a time.

Remediate alerts in Tanium Enforce

You can create a remediation policy in Tanium Enforce, and specify conditions to enforce that policy from an alert. For example, a remediation policy defines specific actions to perform for an alert, and an enforcement defines the endpoints and schedule for performing the actions defined in the policy. Policies such as deleting files, killing a process, and performing registry tasks are available to perform when an alert is generated. By default, the remediation only targets the endpoint that generated the alert. To create remediation policies from an alert, Tanium Enforce must be installed . Additionally, to create remediation policies in Tanium Enforce, the **Enforce Create Enforcement** permission must be granted.

1. From the Main menu, go to **Modules > Threat Response > Alerts**. Select the alert that you want to remediate in Tanium Enforce.
2. Select **Actions > Remediate in Enforce**.

   
   NOTE

   If an instance Tanium Enforce is not installed, this option is not available from the Actions menu.
3. In the Policy Details section, provide a name and description for the policy.

© 2025 Tanium Inc. All Rights Reserved

4. In the Tasks section, click **Add Tasks** to perform as part of the remediation. You can select multiple tasks to add. Each task that you add to the remediation policy requires additional data that is by default populated with the data from the alert. Available tasks are:

   Delete file

   Provide a path to a single file to delete. By default, this path is populated with the data from the alert. Select to continue or exit if an error occurs.

   Kill process

   Select to use the Name, Path, or Hash of the process. Paths support wildcard syntax such as *, !, and ?. Group syntax is also supported. Hashes support an optional maximum file size. Provide any additional command line arguments for a process. Command line arguments support regular expression syntax such as `C:\^Win$\.*`.

   Provide a timeout value in seconds. If the number of seconds you specify is exceeded without killing the specified process, the kill process task fails. You can additionally provide a number of attempts for the task before the task fails.

   Select to continue or exit if an error occurs.

   Edit Registry Data

   Select a hive in which to edit the registry data:

   HKEY_CLASSES_ROOT
   HKEY_LOCAL_MACHINE
   HKEY_CURRENT_CONFIG
   HKEY_USERS

   Additionally provide the path relative to the hive you select. For example, System\CurrentControlSet\Hardware Profiles\Current

   Select the type of the data to edit and provide new data to use to replace the value of the existing data.

   Select if you want to create the value using the data you provided if no value matching the alert is detected. Select to continue or exit if an error occurs.

   Update Registry Value

   Select a hive in which to update the registry data:

   HKEY_CLASSES_ROOT
   HKEY_LOCAL_MACHINE
   HKEY_CURRENT_CONFIG
   HKEY_USERS

   Additionally provide the path relative to the hive you select. For example, `System\CurrentControlSet\Hardware Profiles\Current`

   Select to edit the value with data that you provide, or to delete the current value. Select to continue or exit if an error occurs.

© 2025 Tanium Inc. All Rights Reserved

Delete Registry Key

Select a hive in which to delete the registry key:

HKEY_CLASSES_ROOT
HKEY_LOCAL_MACHINE
HKEY_CURRENT_CONFIG
HKEY_USERS

Additionally provide the path relative to the hive you select. For example, `System\CurrentControlSet\Hardware Profiles\Current`

Select to continue or exit if an error occurs.

5. In the Enforcements section, click **Add Enforcement**. Select **Computer Group** to target the remediation to an entire computer group. Select **Individual Computers** to provide one or more endpoints for the remediation to target. Add the fully qualified host name of each endpoint you want the remediation to target. Comma delimit multiple endpoints. Provide a start and end time for when you want to perform the remediation. Select to distribute over time to balance resource use over a time duration that you specify. The duration of the Distribute over time setting must be at least 10 minutes shorter than the Issue time setting. Select if you want to repeat the action and how often.
6. Click **Remediate**. The remediation is available in Tanium Enforce. From the Main menu, click **Modules > Enforce > Policies > Remediations** to view and edit the remediation in Tanium Enforce.

Export alerts

Export alerts to a CSV file.

1. From the Main menu, go to **Modules > Threat Response > Alerts**. Select the alerts that you want to export.

   Note: You can export up to 10,000 alerts.
2. Click **Actions > Export to CSV**.
3. Alert data is exported to a CSV file with the following data (if available) for each alert:
   - Date
   - Endpoint
   - Event Type
   - Hash
   - Hash Type
   - Intel Name
   - Intel Source
   - MITRE Technique(s)

© 2025 Tanium Inc. All Rights Reserved

- Outbound Impact
- On-Demand Scan ID
- OS
- Path
- Platform
- Status

The CSV file download is managed through the web browser. All exports are exported to the downloads directory of the web browser that initiated the export.

Delete alerts

You can delete alerts any time. If an alert is matched again later, the alert is generated again.

Suppress alerts

Create suppression rules to prevent the creation of a Signal-based alert when an intel match occurs. Use suppression rules to reduce false positives for Signals that you cannot edit, such as those from the Tanium Signal Feed. You can also add suppression rules for custom Tanium Detection types, like Process Injection. Suppression rules are not intended for use as a substitution for properly crafted Signals; if you are suppressing alerts consistently due to a Signal not matching as intended, it is a good indication that the Signal should be revised to more accurately match. By thoughtfully analyzing alerts you can tune the Signals that generate them optimally. See Authoring Signals: Testing Signals for more information.

Suppressed alerts are removed from the database after seven days by default. You can edit the number of days to wait after an alert is suppressed before removing it from the database in **Settings** from the Threat Response overview page.

You can apply rules that suppress alerts that match Process Path, Process Command Line, Parent Command Line, Process Hash, Parent Process Path, Ancestry Path, Ancestry Command Line, and User.



All of the selected suppression fields are required to match before the alert is suppressed.

1. From the Main menu, go to **Modules > Threat Response > Intel > Suppression Rules** and click **Add Rule**.
2. Select the type of suppression rule to create. **All Signals** rules apply to all Signals where a match occurs. An intel-specific rule only applies to matches to a specific intel document that you specify. Select **All Signals** or **Intel-Specific**. If you select **Intel-Specific**, select an available intel type.
3. Provide a name and description for the suppression rule.
4. Select the fields that you want to use for suppression rules. For process injection suppression rules, specify artifacts that are both the actor and target process of process injection in the corresponding fields. The fields are identical for both the actor and target processes.

© 2025 Tanium Inc. All Rights Reserved

a. **Process Path**: The path in the file system to a specific process. For example, `c:\windows\notepad.exe`.

b. **Process Command Line**: Additional parameters that were provided for a process. For example, if a process is `wevtutil.exe`, a possible process command line is: `wevtutil cl Application`.

c. **Parent Command Line**: The full command line of the parent process.

d. **Parent Process Path**: The path in the file system to a parent process. For example, `c:\windows\system32\cmd.exe`.

e. **Ancestry Command Line**: Additional parameters that were provided for a parent process.

f. **Ancestry Path**: The path in the file system to a process more remote than a parent process.

g. **Process MD5/SHA1/SHA256**: A specific MD5, SHA1, or SHA256 hash value that corresponds to a process.

h. **User**: A specific user on the system that is associated with a process.



If a Signal has generated an alert, you can click the **Suppress Alert** link from an alert page to preview the expected values for each of the fields.

5. Specify how you want to compare the field to the alert. You can choose to suppress an alert if a field is a direct match, contains a value, or matches a pattern specified by a regular expression.

   a. Select **Is** to suppress an alert when a direct match occurs. For example, a specific hash value or user name matches.

   b. Select **Contains** to suppress an alert when a subset of the alert criteria matches. For example, a path that contains "Windows".

   c. Select **Matches** to suppress an alert when a pattern matches the criteria. A regular expression needs to match the whole string. If you want to match `Win` and `Windows`, the regular expression needs to be `.*Win.*`. By default, regular expressions in suppression rules are case insensitive. Use of ^ and $ and flags are not supported.

6. Select **Retroactive** to run the suppression rule against all existing alerts that have not been resolved. If unselected, the rule does not apply to existing unresolved alerts, but applies to future Signal matches.

7. Click **Preview** to view a list of existing unresolved alerts that match the criteria you specify in the suppression rule. Threat Response evaluates 1000 alerts at a time until all applicable alerts have been evaluated, or until 10,000 alerts have been evaluated. Click **Save**. **Preview** is not available for process injection suppression rules.

Suppress an alert

You can create a suppression rule directly from an alert. From the Main menu, go to **Modules > Threat Response > Alerts**. Select an alert and click **Actions > Suppress**. The suppression rule page appears and features all of the values that are required to suppress the alert. Provide a name and description for the suppression rule and select **Retroactive** if you want to apply the suppression rule against all existing alerts that have not been resolved. Click **Save**.

© 2025 Tanium Inc. All Rights Reserved

Edit and delete suppression rules

You can edit or delete existing suppression rules. From the Main menu, go to **Modules > Threat Response > Intel > Suppression Rules**. Select a suppression rule that you want to edit. Click **Actions > Edit**.

To delete a suppression rule, select the suppression rules that you want to delete. Click **Actions > Delete**.

View the status of a retroactive task

If you edit a suppression rule and select **Retroactive** to run the suppression rule against all existing alerts that have not been resolved, you can view the status of how that rule is retroactively applied. From the Main menu, go to **Modules > Threat Response > Intel > Suppression Rules**. Click **Retroactive Tasks**. View the status column to see if the retroactive task is Not Started, Incomplete, Completed, or has resulted in an error.

Import and export suppression rules

Import and export suppression rules to move them from one platform to another. For example, you can export All Signals suppression rules from a test system and import them to a production system. All Signals type suppression rules are imported and exported as CSV or JSON files.

Export specific suppression rules

1. From the Main menu, go to **Modules > Threat Response > Intel > Suppression Rules**.
2. Select the suppression rules that you want to export. Click **Actions > Export**.
3. Provide a name for the exported suppression rules.
4. Select to export the suppression rules in CSV or JSON format. If you select JSON, intel-specific suppression rules are omitted from the export.
5. Click **Export**.

Export all suppression rules

1. From the Main menu, go to **Modules > Threat Response > Intel > Suppression Rules**. Click **Export All**.
2. Select to export the suppression rules in CSV or JSON format.
3. Click **Export**.

Import suppression rules

1. From the Main menu, go to **Modules > Threat Response > Intel > Suppression Rules**. Click **Import** and browse to a JSON file that you want to import. Click **OK**. Suppression rules are imported as JSON files and have a file size limit of 1 MB.

© 2025 Tanium Inc. All Rights Reserved

2. Review the suppression rules to be imported. Click **OK**. You can **Skip** a suppression that is conflicting with one that already has the same name or **Import and Rename** to apply a suffix of `Duplicate <time stamp>` to the suppression. For example, if a suppression is named `test` and you select **Import and Rename**, the resulting imported rule would be named `test Duplicate <time stamp>`.
3. From the summary window that displays the suppression rules that have been imported, click **Finish**.
4. Refresh the list of suppression rules to view the suppression rules that have been imported.

Manage the impact of lateral movement with Tanium Impact

If you installed Tanium Impact, and are assigned the `Impact Asset Items Read` and `Impact Asset Details Read` permissions, an **Outbound Impact** column appears in the alerts results grid. The value in the **Outbound Impact** column quantifies the number of user accounts and endpoints that can be reached from the corresponding Windows endpoint. Click the alert to view the alert details. In the **Impact Details** section of the alert details you can view data to better understand the lateral impact the endpoint has in an environment should it become compromised to help prioritize alert remediation.

Click **Explore in Impact** to view more detailed information about how the Windows endpoint fits into a larger topology. For more information, see Contact Tanium Support on page 377.

Set up Tanium Connect forwarding

Threat Response sends event information to Tanium Connect by default. To save this event information, you must configure Connect for the events to be passed to a destination. If you do not configure a destination, the events are dropped.

You can configure a Connect forwarding connection at any time. If you configure the connection during the installation process, all history is captured.

1. From Connect, create a new connection with **Event** as the source and **Tanium Threat Response Alerts** as the event group.
2. Select the Threat Response events that you want preserved.
    - **Match Alerts Raw** sends alert details in JSON format. Match alerts are generated when intel deployed in a profile matches an event on an endpoint.
    - **Match Alerts** sends alert details as strings. Strings can be encoded in Base64 if the **Base64 encode events sent to Connect** setting is enabled. Match alerts are generated when intel deployed in a profile matches an event on an endpoint.
    - **All Events** includes scan matches. When you select **All Events**, audit events and deleted alerts are not sent to the destination as part of the **All Events** information. Audit events and deleted alerts are included in the Tanium **Audit Report**. For more information, see Export audit data.

© 2025 Tanium Inc. All Rights Reserved

> **NOTE** In Threat Response 4.0, **All Events** is effectively the same as **Match Events**; it does not send messages and notifications. Messages and notifications have been converted to audit messages in Threat Response 4.0 and are sent with the Audit source. If you have configured **All Events** enable the **Audit Report** type in Connect to continue receiving the same messages you expect.

When forwarding events to Tanium Connect using **Match Alerts** or **Match Alerts Raw**, an intel source field has been added that corresponds to the intel document that the generated alert is associated with.

If you want to Base64 encode event details that are sent to Connect, from the Threat Response overview page, click Settings , click **Service > Misc**, and enable **Base64 encode events sent to Connect**. For **Match Alerts** and **All Events**, enabling this setting encodes the details field of the sent data. The following table details the type of data for the details field of event details when this setting is enabled or disabled.

Base64 encode events sent to Connect implications

Setting state on Threat Response version	Match Alerts Raw	Match Alerts	All Events
Enabled on Threat Response version 3.10	JSON	B64	B64
Disabled on Threat Response version 3.10	JSON	STRING	STRING
Enabled on Threat Response version 4.0 and later	JSON	B64	B64
Disabled on Threat Response version 4.0 and later	JSON	STRING	STRING

3. Configure the destination; such as a SIEM service or Write to File. All data that is sent features a link to all alerts in the Threat Response workbench, which enables quick access to the alert in Threat Response for context.

When configuring reputation intel for Threat Response, you do not need to configure Tanium Connect as Threat Response inserts data into the reputation database.

For more information see the Tanium Connect User Guide.

© 2025 Tanium Inc. All Rights Reserved

Managing response activity

From the Main menu, go to **Modules > Threat Response > Response Activity** to view the status, create or stop a response action. A response action, unlike a scheduled action, runs once during a provided time range and ensures that if an endpoint is not online when you deploy the action, it runs when the endpoint comes online. Initiate a response action to a single affected endpoint. You can initiate Live Response, Quarantine, download a file, or gather a snapshot from a targeted endpoint.

The response actions that you can view are restricted to the actions that the user created. Users that have the have the bypass privilege can view additional response actions. A user that has multiple personas can view their response actions across personas, providing the personas have the ability to view response actions.

You can initiate response actions from an alert. For more information, see Initiate response actions from an alert.

Create a response action for an endpoint

1. From the Main menu, go to **Modules > Threat Response > Response Activity**.
2. Click **Create > Download File**, **Create > Gather Snapshot**, **Create > Live Response**, **Create > Quarantine**, or **Create > Unquarantine**.
3. Select an endpoint that is the target of the response action.

   When you download a file as a response action, the file is saved as saved evidence. From the Main menu, go to **Modules > Threat Response > Saved Evidence > Files** to access the files that you download.

4. Provide parameters for the response action. For example, if you select the response action for Live Response, you can specify the package you want to use for Live Response file collection.
5. Click **Run**. Confirm that you want to deploy the response action.

Response Action: Download File

1. From the Main menu, go to **Modules > Threat Response > Response Activity**.
2. Click **Create > Download File**.
3. Select an endpoint that is the target of the response action. When you download a file as a response action, the file is saved as saved evidence. From the Main menu, go to **Modules > Threat Response > Saved Evidence > Files** to access the files that you download.
4. Provide the full path of the file you want to download to saved evidence.
5. Provide an expiration time and date that corresponds to the expiration of the response action. The response action runs

© 2025 Tanium Inc. All Rights Reserved

every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.

6. Click **Run Response Action**. Confirm that you want to deploy the response action.

Response Action: Gather Snapshot

1. From the Main menu, go to **Modules > Threat Response > Response Activity**.
2. Click**Create > Gather Snapshot**.
3. Select an endpoint that is the target of the response action. When you gather a snapshot as a response action, the snapshot is saved as saved evidence. From the Main menu, go to **Modules > Threat Response > Saved Evidence > Snapshots** to access the snapshot that you gathered.
4. Provide an expiration time and date that corresponds to the expiration of the response action. The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.
5. Click **Run**. Confirm that you want to deploy the response action.

Response Action: Live Response

1. From the Main menu, go to **Modules > Threat Response > Response Activity**.
2. Click **Create > Live Response**.
3. Select an endpoint that is the target of the response action.
4. Select the **Live Response Package** to use. You can select **Threat Response - Live Response [Linux]**, **Threat Response - Live Response [Mac]**, or **Threat Response - Live Response [Windows]** depending on the operating system of the endpoint from which you want to collect data.
5. Select one or more **Collections** to use. A collection defines the data to collect from an endpoint. Default collections are provided, or you can create custom collections. For more information on collections and a procedure for creating a collection, see Collections.
6. Select a **Destination**. A destination is a location to save forensic data. The server that receives information from Live Response can be Azure, an Amazon S3 Bucket, or a server that communicates over SFTP, SCP, or SMB (Windows only - SMB destinations are not included in Live Response packages for macOS and Linux.) protocols. For more information on destinations and a procedure for creating a destination, see Destinations. You can select either **Defined Destination** or **Dynamic AWS S3 Configuration**. A defined destination is a preconfigured definition - including authentication data - that you can use to receive data from the targeted endpoint. A dynamic AWS S3 configuration enables you to enter dynamic credentials that are used to authenticate with a specific destination you can use in the context of the response action.

   If you select **Defined Destination**, provide the following information:

   a. Select one or more preconfigured destinations.

© 2025 Tanium Inc. All Rights Reserved

b. Provide a **Base Directory** that corresponds to a directory name where files are placed as they are collected. This directory is created under the **Remote Path** value that you provide in the destination you are using for the Live Response package. For example, if you provide a **Base Directory** of `MyCollection` where the **Remote Path** is `FileCollection`, the result would be `FileCollection/MyCollection`. Review the **Remote Path** setting that is specified in the preconfigured destination to understand where collected files are located.

c. (Optional) Select **Flatten Output Files** if you want all collected files placed in one directory where the filename includes the original path, but does not retain the folder structure.

If you select **Dynamic AWS S3 Configuration**, provide the following information:

a. Provide a **Bucket** that corresponds to the name of the S3 Bucket. When using an S3 bucket as a destination make sure that clients are synchronized with a time server. Transfers fail if the client time differs from the server time by more than 15 minutes.

b. Provide an **Access Key** that corresponds with a secret access key. For example, `AKIAIOSFODNN7EXAMPLE`.

c. Provide a **Secret Access Key** that corresponds with an access key ID. For example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`. Manage your access keys as securely as you do your user name and password.When you create access keys, you create the access key ID and secret access key as a set. During access key creation, AWS gives you one opportunity to view and download the secret access key part of the access key. If you do not download the key or if you lose the key, you can delete the access key and then create a new one.

d. Provide a **Session Token** that is a valid STS token if you are not using permanent keys.

e. Provide a **Region** that corresponds to an explicitly defined S3 region.

f. Provide a **Host** that corresponds to the fully qualified domain name of the host.

g. Provide a **Port** that corresponds to the port to use for the connection for the destination. The default is 443.

h. (Optional) Select **Use SSL** to enable SSL encryption.

i. Select **Force Path Style Types** to force API calls to use path-style URLs where the bucket name is part of the URL path for accessing buckets.

j. Select **Connection Timeout** to specify the amount of time to attempt to establish a connection.

k. Provide a **Remote Path** that corresponds to a path on the destination where data is collected.

l. Provide a **Base Directory** that corresponds to a directory name where files are placed as they are collected. This directory is created under the **Remote Path** value that you provide in the destination you are using for the Live Response package. For example, if you provide a **Base Directory** of `MyCollection` where the **Remote Path** is `FileCollection`, the result would be `FileCollection/MyCollection`.

m. (Optional) Select **Flatten Output Files** if you want all collected files placed in one directory where the filename includes the original path, but does not retain the folder structure.

7. Provide an expiration time and date that corresponds to the expiration of the response action. The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.

8. Click **Run**. Confirm that you want to deploy the response action.

© 2025 Tanium Inc. All Rights Reserved

Response Action: Quarantine

1. From the Main menu, go to **Modules > Threat Response > Response Activity**.
2. Click **Create > Quarantine**.
3. Select an endpoint that is the target of the response action.
4. Select the Quarantine Package to use. You can select **Threat Response - Quarantine Endpoint [Linux]**, **Threat Response - Quarantine Endpoint [Mac]**, or **Threat Response - Quarantine Endpoint [Windows]** depending on the operating system of the endpoint you want to quarantine.
5. Select the Quarantine Profile to use. A profile enables you to make a package that contains configuration information and rules that you can deploy to targeted endpoints. For more information on the Tanium Default Quarantine Profile, see Quarantining endpoints.
6. Provide an expiration time and date that corresponds to the expiration of the response action. The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.
7. Click **Run**. Confirm that you want to deploy the response action.

Response Action: Unquarantine

1. From the Main menu, go to **Modules > Threat Response > Response Activity**.
2. Click **Create > Unquarantine**.
3. Select an endpoint that is the target of the response action.
4. Provide an expiration time and date that corresponds to the expiration of the response action. The response action runs every four hours until a status is reported from the endpoint, or until the expiration time on the response action occurs.
5. Click **Run**. Confirm that you want to deploy the response action.

Stop a response action

1. From the Main menu, go to **Modules > Threat Response > Response Activity**.
2. Select the response action that you want to stop from the list of response actions.
3. Click **Actions > Stop**.

© 2025 Tanium Inc. All Rights Reserved

Collecting data from endpoints with Live Response



The workflows that consist of manually editing Live Response and Quarantine packages, generating the packages, and deploying the packages to endpoints manually will be deprecated in an upcoming version of Threat Response. These workflows have been replaced by Response Actions, where you can define a Live Response or Quarantine action that runs once during a provided time range and ensures that if an endpoint is not online when you deploy the action, it runs when the endpoint comes online. Initiating response actions enble you to provide configuation information that defines which Live Response and Quarantine parameters to use when collecting data or quarantining endpoints.

A critical step in the incident response process is the collection of data from compromised endpoints for further forensic analysis. Threat Response provides a feature called Live Response that you can use to collect specific information from endpoints to use for forensic analysis, data correlation, and to investigate potentially compromised systems with a customizable and extensible framework.

Live Response collects forensic information from endpoints, and transfers the results to a network location that you specify in a package. The Live Response package contains configuration files that identify the data to collect, and where to copy the data. Specify the data that you want to collect from endpoints, and the network destination to save the collected files.

Destinations

A destination is a location to save forensic data. The server that receives information from Live Response can be Azure, an Amazon S3 Bucket, or a server that communicates over SFTP, SCP, or SMB (Windows only - SMB destinations are not included in Live Response packages for macOS and Linux.) protocols.

For SSH (SFTP/SCP) destinations, a user with write access to the share on the destination is required. Consider modifying the `/etc/ssh/sshd_config` file on the server to allow only SFTP or SCP access. A best practice is to use Linux SFTP/SCP destinations for SCP/SFTP transfers.



SSH server destinations are only supported on Linux and macOS.

The key exchange algorithms supported by Live Response for SSH destinations include:

- curve25510-sha256@libssh.org
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

© 2025 Tanium Inc. All Rights Reserved

- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha256

NOTE

At least one of these algorithms must be supported by the server for SSH (SFTP/SCP) destinations.

For an SMB copy location, the system account is used. SMB shares work with domain joined endpoints. Either the specific endpoint must have write access, or the domain computers group must have write access. Required advanced permissions:

- Create files / write data
- Create folders / append data
- Write attributes

For Amazon S3 Bucket copy locations, ensure that clients are synchronized with a time server. Transfers fail if the client time differs from the server time by more than 15 minutes.

To access SMB destinations when a system has been quarantined, you must also allow access via Kerberos to the Domain Controller. For more information, see the example in Reference: Custom rules examples.

1. From the Main menu, go to **Modules > Threat Response > Management > Live Response**. Click **Create > Destination**.
2. In the General Information section, provide a name and description for the destination.
3. Select a destination type. Available destination types are Azure, S3, SSH, and SMB. The destination type that you select determines the types of required setting information. Refer to destination types for more information.
4. Click **Save**.

BEST PRACTICE

Be aware that keys you use to authenticate destinations should be considered public. Do not use keys that provide access to sensitive information, and ensure the keys are limited in scope. Do not allow keys to read, overwrite, or delete data.

Destination types

Different types of destinations require different settings.

NOTE

There is no option for disabling hostkey verification for SSH destinations in Live Response for Threat Response.

AZURE DESTINATIONS

For Azure destinations, the following settings are required:

© 2025 Tanium Inc. All Rights Reserved

Setting	Description
Storage Account	Provide the name of the storage account that contains Azure Storage data objects. The storage account provides a unique namespace for Azure Storage data that you can access from HTTP or HTTPS.
Container	Provide the name of the Azure Container Instance where Live Response data is saved.
Key File	Provide the storage account access key to construct a connection string to access Azure Storage. The values in the connection string are used to construct the Authorization header that is passed to Azure Storage.
SAS Token	A shared access signature (SAS) is a token that permits delegated access to resources in your storage account. The SAS token encapsulates all of the information needed to authorize a request to Azure Storage on the URL.
Maximum Attempts	Specifies the maximum number of attempts an operation will be tried before producing an error.
Simultaneous Uploads	Specifies the number of concurrent uploads that can occur.
Connection Timeout	The amount of time to attempt to establish a connection.

S3 DESTINATIONS

For S3 destinations, the following settings are required:

Setting	Description
Bucket	The name of the S3 Bucket. When using an S3 bucket as a destination make sure that clients are synchronized with a time server. Transfers fail if the client time differs from the server time by more than 15 minutes.
Access Key ID	An ID that corresponds with a secret access key. For example, `AKIAIOSFODNN7EXAMPLE`
Secret Access Key	A secret key that corresponds with an access key ID. For example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`. Manage your access keys as securely as you do your user name and password. When you create access keys, you create the access key ID and secret access key as a set. During access key creation, AWS gives you one opportunity to view and download the secret access key part of the access key. If you do not download the key or if you lose the key, you can delete the access key and then create a new one.
Region	An explicitly defined S3 region.
Host	The fully qualified domain name of the host.
Port	The port to use for the connection for the destination. The default is 443.
Use SSL	SSL encryption is enabled.

© 2025 Tanium Inc. All Rights Reserved

Setting	Description
Force Path Style Types	Forces API calls to use path-style URLs where the bucket name is part of the URL path for accessing buckets.
Connection Timeout	The amount of time to attempt to establish a connection.
Remote Path	A path on the destination where data is collected.

SSH DESTINATIONS

For SSH destinations, the following settings are required:

Setting	Description
Protocol	Select SFTP or SCP as the protocol to transfer collected files to the destination.
Authentication Type	Private Key or Password. The type of protocol that you select determines whether you are prompted to provide a private key or a password to authenticate with the destination.
Host	The fully qualified domain name of the host.
Port	The port to use for the SSH connection for the destination. The default is 22.
Username	The user name for the connection to the destination.

© 2025 Tanium Inc. All Rights Reserved

Setting	Description

Password or Private Key	The password for the user name, or a private key to authenticate the connection to the destination. An RSA key must be base64 encoded before you enter it into the private key field.
	
	NOTE You cannot password protect private keys used for live response destinations.
	
	In PowerShell you can convert to base64 encoding using the following command:
	
	`[Convert]::Tobase64String([System.IO.File]::ReadAllBytes('<filepath>')) | clip`
	
	Adding `| clip` to the end of the command sends the base64 output directly to the clipboard for pasting. If you try to copy and paste from the command line output, it is possible to introduce carriage returns which break the input and produce the error "`invalid character`" in the Tanium data entry console.
	
	On Linux you can convert to base64 encoding using the following command:
	
	`cat <filepath> | base64 -w 0`
	
	On macOS you can convert to base64 encoding using the following command:
	
	`cat <filepath> | base64 -b 0`
	
	NOTE Although the normal openSSH format is assumed to be base64, encode the entire key again before uploading.

Known Hosts	The content of an SSH known hosts file. See Generate known_hosts and test connections
Connection Timeout	The amount of time to attempt to establish a connection.
Remote Path	A path on the destination where data is collected. This path is relative to the home directory of the present user. Absolute paths are not supported.

SMB DESTINATIONS

NOTE The SMB transfer protocol is only supported on Windows operating systems. SMB destinations are not included in Live Response packages for macOS and Linux.

For SMB destinations, the following settings are required:

Setting	Description
Universal Naming Convention	The UNC path of the destination. For example, `\\server\folder`

© 2025 Tanium Inc. All Rights Reserved

Generate known_hosts and test connections

The **Threat Response - Live Response [Windows]** package contains `taniumfiletransfer_32.exe` and `taniumfiletransfer_64.exe`. When the package is deployed, the file that is appropriate for endpoint is copied to the endpoint and renamed to `taniumfiletransfer.exe`. Download `taniumfiletransfer_32.exe` or `taniumfiletransfer_64.exe` from the **Threat Response - Live Response [Windows]** package.

To see a list of supported protocols, run one of the following commands depending on the architecture you are using:

`taniumfiletransfer_64 protocol`
`taniumfiletransfer_32 protocol`

To see details about a specific protocol, including options for the protocol connection string, run: `taniumfiletransfer_64 protocol <protocol>`

To generate a known_hosts file for use with SFTP or SCP:

1. Connect to the host you want to get a capture from.
2. Get the target IP you want to transfer the file to.
3. Run the following command: `C:\> taniumfiletransfer_64.exe ssh-keyscan <host> > known_hosts` on Windows endpoints or `ssh-keyscan <host> > known_hosts` on Linux and macOS endpoints.

To update the known_hosts file in the live response package paste the contents of the file that you generated to the known_hosts field in the destination. The ssh-keyscan command produces a file with all SSH fingerprints commented with a # character. Edit the file that is created by using this command and remove the # before the fingerprints that should be accepted. A description of the fingerprints is provided with two ## characters and these should be left as comments. If you use a non-standard port, the output in the known_hosts file needs to be edited to reference that port. Lines starting with a double-hash ## need to be edited. For example, if you are using port 222, update the line:

```
## Host: 192.168.0.113:22 (192.168.0.113:22)...
```

to:

```
## Host: 192.168.0.113:222 (192.168.0.113:222)...
```

If the `known_hosts` file is not edited to reference the correct port, Live Response encounters a failure. The `known_hosts` file must be ASCII encoded.

Alternatively you can perform the following steps:

1. Generate the destination package. See Collect data from endpoints.
2. Delete the `known_hosts` file in the **Threat Response - Live Response [OS]** package.
3. Add the file you generated with no changes. Note that a Linux package cannot be updated from a Windows endpoint due to the changes Windows makes to the file format.
4. Save the package.

To test sending a file via an SFTP string enter the following command:

`C:\> taniumfiletransfer_64.exe send test_file -d sftp://<user>:<password>@<host>:/<dir>#knownHostsFile=known_hosts`

© 2025 Tanium Inc. All Rights Reserved

Collections

A collection defines the data to collect from an endpoint. The following configurations are provided with Live Response:

- **Standard Collection**: Use for default data. The standard collection contains file collectors to collect specific files from endpoints. See File Collector Sets for a reference of the file collectors that are contained in each type of collection. The following data is captured by default, and is configurable in the standard collection:
    - Enumerate Running Processes
    - Enumerate Process Modules
    - Enumerate System Drivers
    - Analyze Windows Prefetch
    - Analyze Windows Amcache
    - Analyze Windows Shimcache
    - Analyze Windows Filesystem .LNK Files
    - Analyze Windows Scheduled Jobs
    - Analyze Windows Recent Files Cache
    - Analyze Windows User Assist Recent Applications
    - Analyze Network Connection Details
    - Analyze Process and File Handle Details
    - Analyze System Startup
- **Extended Collection**: Use to collect the same data as the standard collection, plus more file based artifacts, such as the kernel, the Master File Table, USN Journal, event logs, registry hive files, and so on. The extended collection contains file collectors to collect specific files from endpoints. See File Collector Sets for a reference of the file collectors that are contained in each type of collection. The following data is configurable in the extended collection:
    - Enumerate Running Processes
    - Enumerate Process Modules
    - Enumerate System Drivers
    - Analyze Windows Prefetch
    - Analyze Windows Amcache
    - Analyze Windows Shimcache
    - Analyze Windows Filesystem .LNK Files
    - Analyze Windows Scheduled Jobs
    - Analyze Windows Scheduled Tasks Via Schtasks
    - Analyze Windows Recent Files Cache

© 2025 Tanium Inc. All Rights Reserved

- Analyze Windows User Assist Recent Applications
- Collect Parsed UsnJrnl Entries
- Analyze Network Connection Details
- Analyze Process and File Handle Details
- Analyze System Startup Applications
- Collect Recorder Database Snapshot

The option to **Collect Recorder Database Snapshot** enables you to collect a snapshot of either `recorder.db` or `monitor.db` from endpoints. **Collect Recorder Database Snapshot** creates a snapshot of a recorder database - whether or not it is encrypted - and adds the snapshot to the collection. The snapshot that this module creates is removed from the endpoint when the collection has completed. By default, recorder database snapshots are saved in a folder named `RecorderSnapshot` on a path that corresponds with the name of the endpoint. For example, `<base_directory>\<endpoint_name>\collector\RecorderSnapshot\<database_name>.db`.

- **Memory Collection**: Use for memory acquisition. The memory collection contains file collectors to collect specific files from endpoints. See File Collector sets for a reference of the file collectors that are contained in each type of collection. Memory data is configurable in the memory collection.

You can create a custom configuration to collect specific data from endpoints.

1. From the Main menu, go to **Modules > Threat Response > Management > Live Response**. Click **Create > Collection**.
2. In the General Information section, provide a name and description for the collection.
3. Select the modules that you want to include in the data collection. A module is a functional area of forensic investigation. For example, the Network Connections module collects data that is helpful to understanding network connections that the endpoint has been involved in. The operating system icons next to each module show the operating systems to which the modules apply.
4. Select the File Collector sets that you want to include in the collection. See File Collectors for more information.
5. Under Script Sets, select the script sets that you want to include in the collection. See Script Sets for more information.
6. Click **Save**.

File Collector sets

File collector sets to define the types of files that you want to collect from endpoints. For example, you can select all files of a specific type, or files that reside on a specific path. Live Response on Windows collects alternate data streams. The name of the alternate data stream is appended to the regular data stream preceded by an underscore. For example, if an alternate data stream named `hidden_datastream` exists for a file named `hosts`, this alternate data stream would be collected as `<path>\hosts_hidden_datastream`.



When setting a maximum recursive depth, enter `-1` to represent unlimited.

© 2025 Tanium Inc. All Rights Reserved

File collector set details

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Hosts File	Windows Hosts File	Standard, Extended	Windows	`%systemdrive%\windows\system32\drivers\etc`	`(^hosts$)`	1	1
	Non-Windows Hosts File	Standard, Extended	Linux, Mac	`/etc`	`(^hosts$)`	1	1
Etc Folder Tree	Etc	Standard, Extended	Linux, Mac	`/etc`	`.*`	15	Unlimited
Shell History Files	PowerShell History	Standard, Extended	Windows	`%userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\`	`^ConsoleHost_history.txt$`	0	1
	Bourne Again (bash) Shell History	Standard, Extended	Linux, Mac	`$HOME`	`^\.bash_history$`	0	1
	Bourne (sh) Shell History	Standard, Extended	Linux, Mac	`$HOME`	`^\.sh_history$`	0	1
	Bourne Again (bash) Sessions	Standard, Extended	Mac	`$HOME/.bash_sessions`	`.*history.*`	15	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Secure Shell (SSH) Files	User's Known Hosts	Standard, Extended	Linux, Mac	`$HOME/.ssh`	`^known_hosts$`	0	1
	User's Authorized Keys	Standard, Extended	Linux, Mac	`$HOME/.ssh`	`^authorized_keys$`	0	1
	Current SSH Users	Standard, Extended	Linux, Mac	`/var/run`	`^utmp.*`	0	1
	SSH Logon Logoff	Standard, Extended	Linux	`/var/log`	`^wtmp.*`	0	Unlimited
	Failed SSH Logon	Standard, Extended	Linux	`/var/log`	`^btmp.*`	0	Unlimited
	SSH Last Logged On Users	Standard, Extended	Linux	`/var/log`	`^lastlog$`	0	Unlimited
	SSH Daemon Configuration	Standard, Extended	Linux, Mac	`/etc/ssh`	`^sshd_config$`	0	Unlimited
	SSH Client Configuration	Standard, Extended	Linux, Mac	`/etc/ssh`	`^ssh_config$`	0	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Systemd Folder Tree	Systemd	Standard, Exended	Linux	`/etc/systemd/system`	`.*`	15	Unlimited
Kext Details	Kext Details	Standard, Extended	Mac	`/var/db/SystemConfiguration`	`^KextPolicy$`	15	Unlimited
	Kext Details (v11+)	Standard, Extended	Mac	`/var/db/SystemPolicyConfiguration`	`^KextPolicy$`	15	Unlimited
Master File Table	Windows Master File Table	Extended	Windows	`%systemdrive%`	`(\$MFT$)`	1	1
UsnJrnl	UsnJrnl	Extended	Windows	`%systemdrive%\$Extend`	`(%.UsnJrnl$)`	1	1
Kernel	Windows Kernel	Exended, Memory	Windows	`%systemdrive%\windows\system32\`	`ntoskrnl\.exe`	1	1
System Registry Hives	Windows System Registry Hives	Extended	Windows	`%systemdrive%\windows\system32\config\`	`((^system$)\|(^security$)|(^software$)\|(^sam$))`	1	4
User Registry Hives	Windows User Registry Hives	Extended	Windows	`%userprofile%\`	`(^ntuser\.dat$)`	2	Unlimited
Windows Event Logs	Windows Event Logs	Extended	Windows	`%systemdrive%\windows\system32\winevt\logs\`	`.*\.evtx`	1	2000

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Windows Prefetch Files	Windows Prefetch Files	Extended	Windows	`%systemroot%\prefetch\`	`(.*\.pf)|(layout\.ini)|(.*\.db)|(pfsvperfstats\.bin)`	1	Unlimited
Chrome User Data	Windows Chrome User Data - Cache	Extended	Windows	`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cache\`	`.*`	0	Unlimited
	Windows Chrome User Data - Local Storage	Extended	Windows	`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Storage\`	`.*`	0	Unlimited
	Windows Chrome User Data - Profile	Extended	Windows	`%LOCALAPPDATA%\Google\Chrome\User Data\Default\`	`.*`	0	Unlimited
	MacOS Chrome Data	Extended	Mac	`$HOME/Library/Application Support/Google/Chrome`	`.*`	9	Unlimited
	Linux Chrome Data	Extended	Linux	`$HOME/.config/google-chrome`	`.*`	9	Unlimited
Tanium Trace Database	Windows Tanium Trace Database	Extended	Windows	`%TANIUMDIR%\`	`^monitor\.db(\-)*(wal|shm|journal)*$`	0	Unlimited
Tanium Index Database	Windows Tanium Index Database	Extended	Windows	`%TANIUMDIR%\Tools\EPI\`	`^EndpointIndex\.db(\-)*(wal|shm|journal)*$`	0	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Shell Configuration Files	Bourne Again (bash) Settings	Extended	Linux, Mac	`$HOME`	`^\.bash(rc|_profile|_aliases)$`	0	1
	C Shell (csh and tcsh) Settings	Extended	Linux, Mac	`$HOME`	`^\.(tcshrc|cshrc)$`	0	1
Available Shells	Available Shells	Extended	Linux, Mac	`/etc`	`^shells$`	0	1
Passwd and Group Files	Passwd and Group Files	Extended	Linux,Mac	`/etc`	`^(passwd|group)$`	0	Unlimited
Shadow Files	Shadow Files	Extended	Linux, Mac	`/etc`	`^(shadow|gshadow|master\.shadow)$`	0	Unlimited
Sudoers Configuration	Sudoers File	Extended	Linux, Mac	`/etc`	`^sudoers$`	0	Unlimited
	Sudoers.d Folder Contents	Extended	Linux, Mac	`/etc/sudoers.d`	`.*`	15	Unlimited
Mount Points	Mount Points	Extended	Linux	`/etc`	^fstab$	0	1
	NFS Mount Points	Extended	Linux	`/etc`	^exports.*	0	1

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Preload Shared Libraries	LD Preload Shared Libraries	Extended	Linux	`/etc`	`ld\.so.*`	15	Unlimited
	LD Preload Shared Libraries Configuration Directory	Extended	Linux	`/etc/ld.so.conf.d`	`.*`	0	Unlimited
Auditd Configuration and Rules	LD Preload Shared Libraries	Extended	Linux	`/etc/audit`	`.*`	15	Unlimited
RPM GPG Keys	RPM GPG Keys	Extended	Linux	`/etc/pki/rpm-gpg`	`.*`	15	Unlimited
SSL/TLS Certificates and PKI	SSL/TLS Certificates Directory	Extended	Linux	`/etc/pki/tls`	`.*`	15	Unlimited
	SSL/TLS Certificate Authority Directory	Extended	Linux	`/etc/pki/CA`	`.*`	15	Unlimited
User Recently Used/Deleted Files	Recently Used GTK Files	Extended	Linux	`$HOME/.local/share`	`recently-used\.xbel`	15	Unlimited
	Recently Deleted Info	Extended	Linux	`$HOME/.local/share/Trash/info`	`.*`	15	Unlimited
	Recently Deleted Files	Extended	Linux	`$HOME/.local/share/Trash/files`	`.*`	15	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
User Vim Configuration	Vim Info	Extended	Linux, Mac	`$HOME`	`^\.viminfo$`	0	Unlimited
	Non-Windows Vim Configuration	Extended	Linux, Mac	`$HOME`	`^\.vimrc$`	0	Unlimited
	Windows Vim Configuration	Extended	Windows	`%homepath%\`	`^_vimrc$`	0	Unlimited
User Less History	Less History	Extended	Linux, Mac	`$HOME`	`^\.lesshst$`	0	Unlimited
User Database History	Database History	Extended	Linux, Mac	`$HOME`	`^\.(psql|mysql|sqlite)_history$`	0	Unlimited
Cron Settings	Cron Files	Extended	Linux, Mac	`/etc/`	`cron.*`	15	Unlimited
	Cron Logs	Extended	Linux, Mac	`/var/log`	`cron.*`	15	Unlimited
Spotlight Information	Spotlight Disk Database	Extended	Mac	`/.Spotlight-V100/Store-V2`	`.*store\\.db`	15	Unlimited
	User Spotlight Shortcuts	Extended	Mac	`$HOME/Library/Preferences/`	`^com\\.apple\\.spotlight\\.plist$`	15	Unlimited
	User Spotlight Shortcuts	Extended	Mac	`$HOME/Library/Application Support/`	`^com\\.apple\\.spotlight\\.Shortcuts$`	15	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
User and Application Analytics	MacOS User and Analytics Information	Extended	Mac	`/var/db/CoreDuet/Knowledge`	`^knowledgeC\\.db$`	15	Unlimited
	MacOS Per-User and Analytics Information	Extended	Mac	`$HOME/Library/Application Support/Knowledge/`	`^knowledgeC\\.db$`	15	Unlimited
Program Execution Reports	Program Execution Reports	Extended	Mac	`/Library/Logs/DiagnosticReports`	`.*\\.core_analytics`	15	Unlimited
	Program Execution Aggregate Analytics	Extended	Mac	`/private/var/db/analyticsd/aggregates`	`.*`	15	Unlimited
Domain User Information	Domain User Information	Extended	Mac	`/private/var/db/ConfigurationProfiles/Store/`	`ConfigProfiles\\.binary`	15	Unlimited
User Mail Data	User Mail Data	Extended	Mac	`$HOME/Library/Mail/`	`.*`	15	Unlimited
Microsoft Office	MacOS Microsoft Office Artifacts	Extended	Mac	`$HOME/Library/Group Containers/`	`^MicrosoftRegistrationDB\\.reg$`	15	Unlimited
Deleted Users	MacOS Deleted Users	Extended	Mac	`/Library/Preferences/`	`^com\\.apple\\.preferences\\.accounts\\.plist$`	15	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Notifications	MacOS Notifications Database Files	Extended	Mac	`/var/folders/`	`^db(-wal|-shm)*$`	15	Unlimited
Event Monitor	MacOS Event Monitor	Extended	Mac	`/System/Library/LaunchDaemons/`	`^com\\.apple\\.emond\\.plist$`	15	Unlimited
DHCP Leases	MacOS DHCP Leases	Extended	Mac	`/private/var/db/dhcpclient/leases/`	`.*`	15	Unlimited
MacOS Finder Information	MacOS Finder MRU	Extended	Mac	`$HOME/Library/Preferences/`	`^com\\.apple\\.finder\\.plist$`	15	Unlimited
	MacOS Recently Opened Items	Extended	Mac	`$HOME/Library/Preferences`	`^com\\.apple\\.recentitems\\.plist$`	15	Unlimited
	MacOS Recently Opened Items 11+	Extended	Mac	`$HOME/Library/Application Support/com.apple.sharedfilelist`	`.*`	15	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Network Services, Settings, and Logs	MacOS Network Services and Settings	Extended	Mac	`/Library/Preferences/SystemConfiguration/`	`^preferences\\.plist$`	15	Unlimited
	VPN Log	Extended	Mac	`/var/log`	`^ppp\\.out$`	15	Unlimited
	Daily Network Log	Extended	Mac	`/var/log`	`^daily\\.out$`	15	Unlimited
	Network Usage	Extended	Mac	`/var/networkd`	`^netusage\\.sqlite$`	15	Unlimited
	MacOS Remembered Networks	Extended	Mac	`/Library/Preferences/SystemConfigurations/`	`^com\\.apple\\.airport\\.preferences\\.plist$`	15	Unlimited
Update and Backup Information	MacOS Last Update	Extended	Mac	`/Library/Preferences/`	`^com\\.apple\\.SoftwareUpdate\\.plist$`	15	Unlimited
	MacOS Last Time Machine Backup	Extended	Mac	`/Library/Preferences/`	`^com\\.apple\\.TimeMachine\\.plist$`	15	Unlimited
Scripting Additions	MacOS Scripting Additions	Extended	Mac	`/System/Library/ScriptingAdditions/`	`.*`	15	Unlimited
System Administrators	MacOS System Administrators	Extended	Mac	`/var/db/dslocal/nodes/Default/groups/`	`^admin\\.plist$`	15	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Authorization Database	MacOS Authorization Database	Extended	Mac	`/var/db`	`^auth\\.db$`	1	Unlimited
Safari User Data	MacOS Safari User Data	Extended	Mac	`$HOME/Library/Safari/`	`^(History\\.db|Downloads\\.plist|TopSites\\.plist|RecentlyClosedTabs\\.plist|Bookmarks\\.plist|CloudTabs\\.db)$`	15	Unlimited
Firefox User Data	MacOS Firefox User Data	Extended	Mac	`$HOME/Library/Application Support/Firefox/Profiles/`	`^(places\\.sqlite|addons\\.json|extensions\\.sqlite|extensions\\.json|search\\.sqlite)$`	15	Unlimited
System Resource Utilization Management (SRUM) Database	System Resource Utilization Management (SRUM) Database	Extended	Windows	`%systemdrive%\windows\system32\sru`	`^srudb.dat$`	0	1
Edge (Chromium) Internet Explorer Data Collection (Mac)	MacOS Edge Data	Extended	Mac	`$HOME/Library/Application Support/Microsoft Edge/Default`	`.*`	9	Unlimited
	MacOS Edge Data - Cache	Extended	Mac	`$HOME/Library/Caches/Microsoft Edge/Default/Cache`	`.*`	9	Unlimited

© 2025 Tanium Inc. All Rights Reserved

File collector set details (continued)

File Collector set	File Collector	Featured in Collection	Operating System	Path	File Pattern	Maximum recursive depth	Maximum files to collect
Edge (Chromium) Internet Explorer Data Collection (Windows)	Windows Edge User Data - Cache	Extended	Windows	`%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Cache`	`.*`	0	Unlimited
	Windows Edge User Data - Local Storage	Extended	Windows	`%LOCALAPPDATA%\Microsoft\Edge\User Data\Default`	`.*`	0	Unlimited
	Windows IE v10-11	Extended	Windows	`%LOCALAPPDATA%\Microsoft\Windows\WebCache`	`.*`	0	Unlimited
	Windows IE v8-9	Extended	Windows	`%LOCALAPPDATA%\Microsoft\WindowsHistory`	`.*`	0	Unlimited
	Microsoft IE v6-7	Extended	Windows	`%LOCALAPPDATA%\LocalSettings\History\History`	`.*`	0	Unlimited
	Microsoft IE v8-9 Index.dat	Extended	Windows	`%APPDATA%\Microsoft\Windows\IEDownloadHistory\`	`index\.dat`	1	1
	Microsoft IE 8-9 Downloads	Extended	Windows	`%APPDATA%\Microsoft\Windows\IEDownloadHistory\`	`.*`	1	Unlimited

You can create custom file collector sets.

1. From the Main menu, go to **Modules > Threat Response > Management > Live Response**. Click **Create > File Collector Set**.
2. In the General Information section, provide a name and description for the file collection set.
3. Click **Create File Collector**.
4. Provide a name for the file collector.
5. Provide a path for files to collect. Paths support environment variables and regular expressions. For more information, see Regular expressions and environment variables.

© 2025 Tanium Inc. All Rights Reserved

6. Provide a file pattern for the files to collect. File patterns support regular expressions. For more information, see Regular expressions and environment variables.
7. Specify the maximum depth of directories to recurse from the path you provided.
8. Specify the maximum number of files to collect.
9. (Optional) Select **Raw** to preserve the format of the files that are collected. When using **Raw**, the following file systems are supported: NTFS, ExFat, Ext, Fat, and HFS Plus.
10. Select the operating systems from which you want the file collector to collect files.
11. Click the check mark in the top right to save the file collector.
12. Click **Save**.

Script sets

You can configure scripts to run on endpoints when you deploy the collection. Supported scripting languages include PowerShell and Python.

1. From the Main menu, go to **Modules > Threat Response > Management > Live Response**. Click **Create > Script Set**.
2. In the General Information section, provide a name and description for the script set.
3. Under **Scripts** click **Add a Script**.
4. Provide a filename for the script.
5. Select Python or PowerShell as the type of script.
6. Provide any script arguments to use as part of running the script.
7. Add the script source.
8. Click **Save**.

Script output is saved in a file that has the same as the script, and has `-results` appended to the file extension. For example, a script named `test.ps1` creates output in `test.ps1-results`. All standard output is directed to the collector directory.

Collect data from endpoints

To collect data from endpoints, deploy a Live Response package.



To prevent resource overload on endpoints, only issue this action manually. Do not create a scheduled action.

1. From the Main menu, go to **Modules > Threat Response > Response Activity > Create > Live Response**.
2. Target endpoints for data collection. Use an operating system-based question, for example: `Get Computer Name from machines with Is Windows containing "True"`.
3. Select the endpoints from which you want to collect data and click **Deploy Action**.

© 2025 Tanium Inc. All Rights Reserved

4. In the **Deployment Package** field, type `Live Response`.
5. Select the package that matches the collection and destination settings that you want to deploy.
6. In the **Base Directory** field, provide a directory name where files are placed as they are collected. This directory is created under the **Remote Path** value that you provide in the destination you are using for the Live Response package. For example, if you provide a Base Directory of `MyCollection` for an SSH destination where the **Remote Path** is `FileCollection`, the result would be `/home/username/FileCollection/MyCollection` since the remote path provided in SSH destinations is relative to the home directory of the present user. Depending on the type of destination, the location of the **Remote Path** can vary. For example, in SMB destinations it is explicit; whereas in SSH destinations it is relative to the home directory of the present user.
7. Optionally select **Flatten Output Files** if you want all collected files placed in one directory where the filename includes the original path, but does not retain the folder structure.
8. Click **Show Preview to Continue**.
9. After you preview the list of endpoints to which the action is being deployed, click **Deploy Action**.

Threat Response tests the connection by writing a LRConnectionTestfile to the destination. If the write fails, the action tries the other destinations in the transfer configuration in the order they are listed in the configuration file. If all the connection tests fail, the action does not proceed.

Tanium shows the package as complete almost immediately after the package is downloaded on the endpoints. This completion is not accurate because Live Response runs in detached mode. File transfers continue after the action completes.

The actual time to complete the transfer depends on the endpoint activity and connection speed between the endpoint and the destination system.

For macOS and Linux endpoints, memory data that is transferred to a destination is packaged in a ZIP file. For example, if you selected memory details as an included module, Live Response creates a ZIP file that contains a raw memory dump and additional system files. You can analyze this data with a tool such as Winpmem or Volexity Surge. For Windows endpoints, memory data is collected as one or more raw files.

Collect logs

In addition to the standard action logs on the endpoint (`Tanium_Client_Location\Tools\IR\data\Action_xxxxx\Action_####.log`), a log file of activities resides in the same directory. This file follows the naming convention: `YYYYMMDDhhmm_LR.log`.

When collection completes, the `YYYYMMDDhhmm_LR.log` is copied to the destination. The action log is not copied to the destination.

Use both the action log and the Live Response log to troubleshoot problems. The action log captures messages written to standard error (stderr).

Regular expressions and environment variables

File patterns support regular expression syntax.

© 2025 Tanium Inc. All Rights Reserved

The following table provides some example patterns to show how Live Response uses both regular expressions and environment variables on Windows, Linux, and macOS endpoints.

File patterns regular expression syntax

Example Live Response task	Operating system	Path	File pattern	Explanation
Collect host file	Windows	`%systemdrive%\windows\system32\drivers\etc`	`^hosts$`	Collects a single file called 'hosts' from an appropriate directory using the `%systemdrive%` environment variable to avoid assuming the system drive is `C:`.
	Linux/macOS	`/etc`	`^hosts$`	In this example, `hosts` matches.
Collect Bash History of every user	Windows	Not Applicable	Not Applicable	Not Applicable
	Linux/macOS	`$HOME`	`/.bash_history$`	A file name that matches `.bash_history`. The forward slash in the file pattern `/.bash_history$` is necessary since an environment variable ($HOME) is used for a path and the environment variable does not include a trailing forward slash.
Collect a file named findme.txt from platform root	Windows	`C:\`	`^findme.txt$`	The filename starts with `findme.txt`
	Linux/macOS	`/`	`^findme.txt$`	The filename starts with `findme.txt`

Any environment variables that you use resolve as described in the following table. Paths containing environment variables apply to all user profiles on the endpoint.

Environment variable support

Environment variable	Supported operating system	Corresponding value
`%appdata%`	Windows	*`C:`*`\Users\`*`username`*`\appdata\roaming`

© 2025 Tanium Inc. All Rights Reserved

Environment variable support (continued)

Environment variable	Supported operating system	Corresponding value
`%homepath%`	Windows	`\Users\`*`username`*
`%localappdata%`	Windows	*`C:`*`\Users\`*`username`*`\appdata\local`
`%psmodulepath%`	Windows	*`C:`*`\Users\`*`username`*`\documents\windowspowershell\modules`
`%temp%`	Windows	*`C:`*`\Users\`*`username`*`\appdata\local\temp`
`%tmp%`	Windows	*`C:`*`\Users\`*`username`*`\appdata\local\temp`
`%userprofile%`	Windows	*`C:`*`\Users\`*`username`*
`%taniumdir%`	Windows	The Tanium Client directory. Defaults are: `\Program Files\Tanium\Tanium Client\` (32-bit OS) `\Program Files (x86)\Tanium\Tanium Client\` (64-bit OS)
`$TANIUMDIR`	Linux, Mac	The Tanium Client directory. Defaults are: `/Library/Tanium/TaniumClient/` (macOS) `/opt/Tanium/TaniumClient/` (Linux)
`$HOME`	Linux, Mac	All user home directories that do not have a home directory set to blocklisted shells, and match shells that are listed in `/etc/shells` file. If there is no `/etc/shells` file, all shells are allowed.
Environment variables that are local to the endpoint are supported. For example, if `%SYSTEMROOT%` is set on an endpoint to expand to `C:\WINDOWS`, you can use such a variable on a path.		

© 2025 Tanium Inc. All Rights Reserved

Quarantining endpoints

NOTE

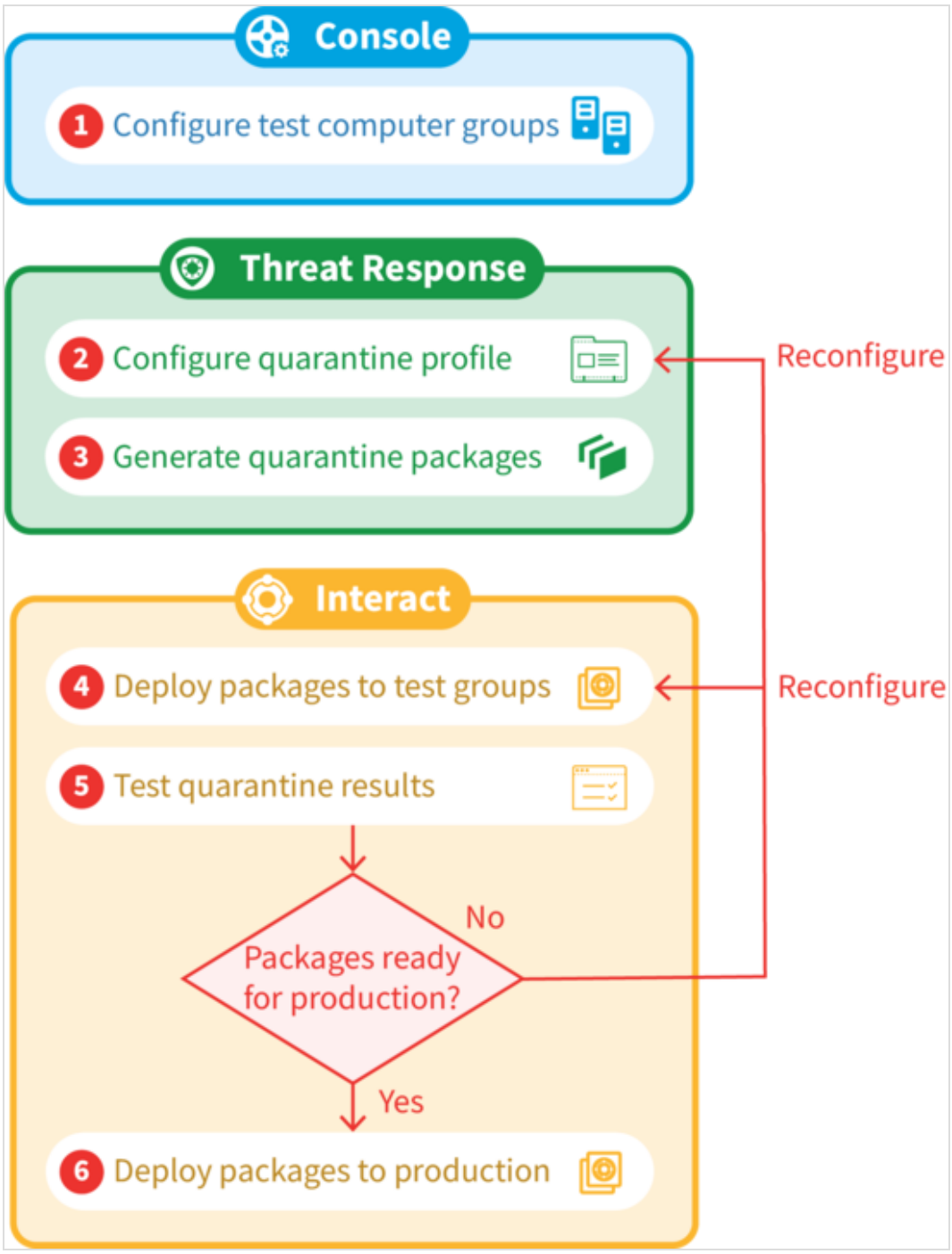
The workflows that consist of manually editing Live Response and Quarantine packages, generating the packages, and deploying the packages to endpoints manually will be deprecated in an upcoming version of Threat Response. These workflows have been replaced by Response Actions, where you can define a Live Response or Quarantine action that runs once during a provided time range and ensures that if an endpoint is not online when you deploy the action, it runs when the endpoint comes online. Initiating response actions enble you to provide configuation information that defines which Live Response and Quarantine parameters to use when collecting data or quarantining endpoints.

Quarantine a Windows, Linux, or macOS endpoint that shows evidence of compromise or other suspicious activity. Use Threat Response to apply, remove, and test for quarantine.

Quarantine enables you to create custom profiles that contain rules that define the parameters to use for quarantining endpoints. After you create a profile, you can generate packages that you can deploy to targeted endpoints to quarantine them. The following diagram illustrates the basic workflow for deploying quarantine profiles:

Example quarantine workflow

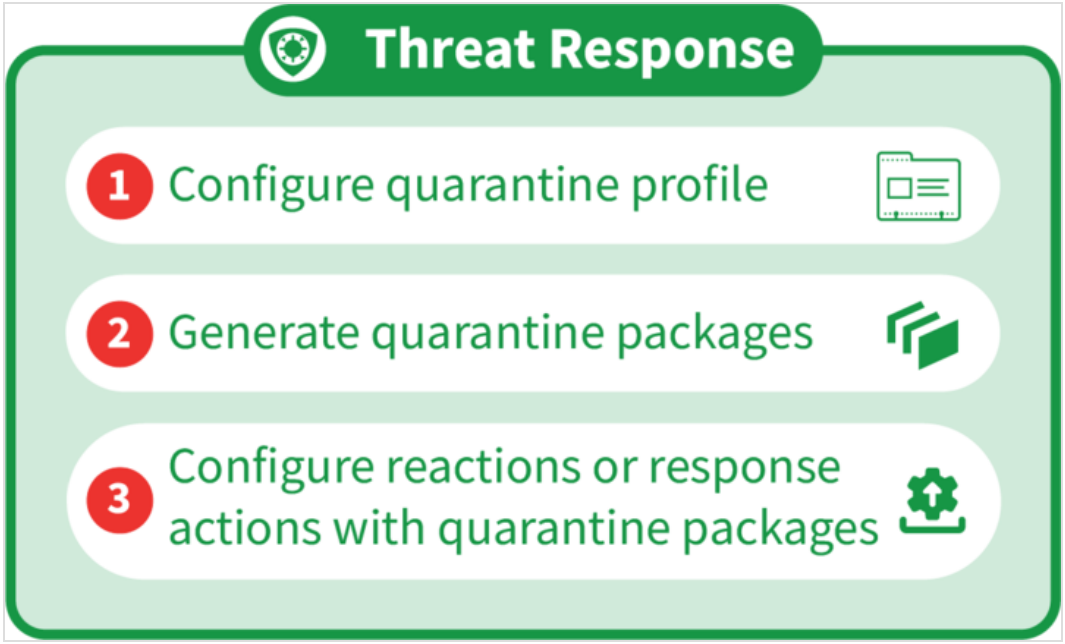
© 2025 Tanium Inc. All Rights Reserved



You can also use quarantine profiles to use as part of a response action or reaction. In this case, you can generate quarantine packages that are used when reactions match on an endpoint or as a response action that you initiate as a response to an alert.

Example quarantine workflow

© 2025 Tanium Inc. All Rights Reserved



When an endpoint is quarantined, by default the only approved traffic allowed on the quarantined endpoint includes:

- Between the Tanium Client on the quarantined endpoint and Tanium Server over port 17472.
- Between the quarantined endpoint and DHCP or DNS servers to obtain and resolve IP addresses.
- Direct Connect connections to the endpoint.
- Live Response destinations.

Threat Response includes a safety feature that automatically reverses a quarantine policy. After a quarantine policy is applied, the effect of the policy is logged. If the endpoint is able to communicate with Tanium Server, Threat Response logs the successful application of the policy. If a policy prevents the endpoint from communicating with Tanium Server, Threat Response backs out the policy and saves logs in the action folder.

BEST PRACTICE

Tanium Automate implements in playbook steps. You can configure reusable playbooks with various steps and run a playbook multiple times to streamline and simplify your business processes. For more information on building a playbook, see Tanium Automate User Guide: Building playbooks. For more information on the available playbook steps, see Tanium Automate User Guide: Reference: Steps.

Before you begin

IMPORTANT

Test quarantine policies before deploying the profile. Do not apply a profile until its behavior is known and predictable. Incorrectly configured profiles can block access to Tanium Server.

© 2025 Tanium Inc. All Rights Reserved

- You must have a Content Administrator account for Tanium Console. For more information, see Tanium Core Platform User Guide: Managing Roles.
- Identify the traffic that is required when an endpoint is under quarantine.
- You must have a lab endpoint on the target operating system (Windows, Linux, or Mac) you can use to test the quarantine policies. You must be able to physically access the machine or to access it using RDP (Windows) or SSH (Linux, Mac).
- You must have access to the endpoint that you want to quarantine through a sensor or saved question in the Tanium Console.
- Beginning with Threat Response 4.6, the Quarantine packages are included with Threat Response. Do not install the IRQuarantine solution on environments where releases of Threat Response 4.6 or later is installed.
- By default an attempt to quarantine an endpoint with a response action times out after seven days. If you are using quarantine as a response action, you can set the **Action Expiration Time** to a custom value when the response action is created. If you deploy quarantine packages to endpoints using Tanium Interact or the Tanium Console, the action uses the value of the package timeout.



Quarantine operates as a layer 3 network firewall and functions at the IP and port level without awareness of higher-layer protocols or application-specific traffic. Quarantine does not recognize any proxies or solutions that operate above layer 3 such as those at layer 4 (Transport) or layer 7 (Application). For these proxies or higher-layer solutions to interact with or be permitted by the quarantine solution, their details must be explicitly defined as `IP:Port` pairs in the quarantine configuration. If the Tanium Client is connected through a proxy during the quarantine action and **All Tanium Servers** is selected, a rule for `CurrentProxy` is added to allow for Tanium Client communications.

Endpoint operating system requirements

Supported Windows versions

- Windows 7 (SP1)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

© 2025 Tanium Inc. All Rights Reserved

- Windows Server 2019
- Windows Server 2022
- Windows Server 2025
- Windows Server 2012R2 or later
- Windows Server 2008R2 (SP1)

Supported Linux OS versions

- AlmaLinux 8.x
- AlmaLinux 9.x
- RedHat/CentOS 5 IPTables on SYSV
- RedHat/CentOS 6 IPTables on SYSV
- RedHat/CentOS 7 Firewalld on Systemd (Note: A reboot is required on RedHat/CentOS 7.1 endpoints after removing quarantine.)
- RedHat/CentOS 8
- RedHat/CentOS 9
- Rocky Linux 8.x
- Rocky Linux 9.x
- Ubuntu 12, 14 UFW on Upstart
- Ubuntu 15, 16, 18, 20, 22, and 24 UFW on Upstart/Systemd

CentOS Stream 8 and 9 variants of CentOS are not currently supported.

Supported macOS versions

- OS X 10.9 Mavericks
- OS X 10.10 Yosemite
- OS X 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11.0 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura

© 2025 Tanium Inc. All Rights Reserved

- macOS 14 Sonoma
- macOS 15 Sequoia
- macOS 26 Tahoe

OSX 10.8 - Mountain Lion and earlier releases are based on ipfirewall (IPFW) and are not supported.

Create quarantine rules

Quarantine rules are the building blocks of profiles. Each profile that you create contains one or more rules. Quarantine rules define allowed traffic direction, allowed IP addresses, ports, and protocols. All other traffic is blocked. These rules are in the same format for Windows, Linux and macOS. If you do not define any quarantine rules, the default values are used, which gives the quarantined endpoint access only to the Tanium Server and permits DNS/DHCP traffic. If you previously provided a Windows IPsec policy file, the IPsec policy overrides the custom quarantine rules.

1. From the Main menu, go to **Modules > Threat Response > Management > Quarantine**. Click the **Rules** tab.
2. Click **Create**. Provide a name and description for the rule.
3. Select the **Direction** for the rule. You can select either **In** or **Out**. The value you select specifies whether incoming or outgoing traffic is allowed.
4. Select the **Protocol** for the traffic. You can select **ICMP**, **TCP**, or **UDP**. If you specify ICMP, the ICMP protocol is allowed to communicate to and from the specified addresses. This limitation is because IPSec does not filter ICMP Type/Codes. The filtering is done by advfirewall. When using quarantine rules to block the ICMP protocol, the MTU negotiation packages can become blocked when the size of the MTU package on the endpoint is larger than the router allowed MTU size. Normally the router will see a packet that is too large and send an ICMP packet to the endpoint to identify that the packet is too large and advises lowering the permissible MTU size. If the negotiation packet is not able to reach the destination due to quarantine, the endpoint can become unresponsive. The endpoint is still is quarantined but loses communication with the Tanium Server. Disabling ICMP traffic while quarantined should only be done after proper testing.
5. Enter an **IP Address** for the rule. Enter any IPv4 address or you can use `ANY` for all.
6. Enter a **CIDR**. Valid values are 0-32 or, if `ANY` is used in IP Address, undefined. This is the subnet mask that represents the number of bits available to the IP address. Undefined is the same as 32 and uses the IP address.
7. (TCP or UDP protocols only) Enter a **Port**. Valid values are 0-65535. Ranges are not currently supported, only individual ports or all ports can be defined. Setting the number as 0 allows all ports.

Create a quarantine profile

A profile enables you to make a package that contains configuration information and rules that you can deploy to targeted endpoints. When you create a profile you can define the criteria for the scope of a quarantine within the Threat Response workbench. You can import existing `taniumquarantine.dat` files into a profile. If you import an existing `taniumquarantine.dat` file into a profile, ensure that all configurations are specified in the correct syntax.

Quarantine uses the legacy `taniumquarantine.dat` file if the quarantine package is called directly. This file is ignored by quarantine actions that are issued by the Threat Response workbench and Threat Response API (for example in a reaction or response action). All quarantine actions issued from the Threat Response workbench or THR API (for example in a reaction or

© 2025 Tanium Inc. All Rights Reserved

response action) ignore the taniumquarantine.dat file and use the appropriate `quarantineprofileconfig_#.dat file`. If no profile is specified in these cases, quarantine uses the default profile that is specified in the Threat Response Quarantine Workbench.

A syntax example is provided for each setting in the following steps.



With the introduction of profiles and rules for quarantine, you can change the details contained in profiles and rules after an endpoint has been quarantined. Changes to the profiles or rules after a quarantine has been applied on an endpoint has no effect on that endpoint unless it is unquarantined and requarantined.

1. From the Main menu, go to **Modules > Threat Response > Management > Quarantine**. Click **Create**. Provide a name and description for the profile.
2. In the **Rules** section, add or remove rules to the profile. Quarantine rules and options define allowed traffic direction, allowed IP addresses, ports, and protocols. All other traffic is blocked. These rules are in the same format for Windows, Linux and macOS. If you do not define any quarantine rules, the default values are used, which gives the quarantined endpoint access only to the Tanium Server and permits DNS/DHCP traffic. If you previously provided a Windows IPsec policy file, the IPsec policy overrides the custom quarantine rules. Test the quarantine profile before deploying the profile. Do not apply a profile until its behavior is known and predictable. Incorrectly configured profiles can block access to the

© 2025 Tanium Inc. All Rights Reserved

Tanium Server. For more information about rules, see Create quarantine rules.

© 2025 Tanium Inc. All Rights Reserved

3. In the **Servers** section, configure server details for the profile. You can configure server settings, alternate Tanium servers, VPN servers, and configure a message to notify the user that the system is being quarantined.

© 2025 Tanium Inc. All Rights Reserved

a. In the **Configuration** section, configure server settings to use with the profile. You can select the following allowances:

Server settings

Allowance Name	Option Name (configuration file)	Description
All DHCP	*AllDHCP*	Allows DHCP traffic to any destination. When updating `taniumquarantine.dat` files manually*, use the following format: Set to `true` to allow traffic Default: `true`
DNS	*AllDNS*	Allows DNS traffic to any destination. When updating `taniumquarantine.dat` files manually*, use the following format: Set to `true` to allow traffic Default: `true`
	CurrentDNS	Allows DNS traffic only to the DNS servers currently configured on the endpoint being quarantined. When updating `taniumquarantine.dat` files manually*, use the following format: Set to `true` to allow traffic Default: `false`
All Tanium Servers	*TaniumServers*	Allows Tanium traffic to the Tanium Servers that are defined in the ServerList or Servers configuration on the Tanium Client. When updating `taniumquarantine.dat` files manually*, use the following format: Set to `true` to allow traffic Default: `true` NOTE: This option only applies to Tanium Servers and Zone Servers on TCP/17472. It does not include the module server, and it does not include TCP/17475 and TCP/17486 required for Direct Connect/Live Endpoint connections. Additional rules are required.
Direct Connect	See Reference: Custom rules examples	Allows Direct Connect to access quarantined endpoints.

© 2025 Tanium Inc. All Rights Reserved

Server settings (continued)

Allowance Name	Option Name (configuration file)	Description
Live Response	See Reference: Custom rules examples	Allows Live Response to collect data from quarantined endpoints.

*= To specify configuration settings in `taniumquarantine.dat`, use the following format:
`OPTION:OptionName:OptionValue`

b. In the **Advanced Settings** section, select whether or not to **Validate Availability** of the Tanium Server.

Advanced settings

Setting Name	Option Name (configuration file)	Description
Validate Tanium Server Availability	*CheckTS*	Validate that the Tanium Server can be reached on the Tanium port. If this validation fails, the quarantined status of the endpoint is revoked. When updating `taniumquarantine.dat` files manually*, use the following format: Set to `true` to validate that the Tanium Server can be reached on the Tanium port Default: `true`

*= To specify configuration settings in `taniumquarantine.dat`, use the following format:
`OPTION:OptionName:OptionValue`

c. In the **Alternate Tanium Servers** section, specify alternate Tanium Servers to use with this profile.

Alternate Tanium servers

Setting Name	Option Name (configuration file)	Description
Alternate Tanium Servers	*ALTTS*	Specify IP addresses. For example, use this option when you want to avoid using DNS during Quarantine. When removed from quarantine, the original Tanium Server is restored. Separate with a comma or leave empty for no alternates.

*= To specify configuration settings in `taniumquarantine.dat`, use the following format:
`OPTION:OptionName:OptionValue`

© 2025 Tanium Inc. All Rights Reserved

d. In the **VPN Servers** section, specify any VPN servers to use with the profile. Paste one or more IP addresses in a line-delimited list.

VPN servers

Setting Name	Option Name (configuration file)	Description
VPN Servers	*VPNSERVERS*	Specify the VPN servers to automatically create rules for with a comma-delimited list. When updating `taniumquarantine.dat` files manually*, use the following format: IP:50/51,UDP:500,4500,TCP/UDP:443 Default: `NO VPNServers`
*= To specify configuration settings in `taniumquarantine.dat`, use the following format: `OPTION:OptionName:OptionValue`		

4. (Windows and macOS only) In the **Notification** section, specify a message that displays to the user upon quarantine of the endpoint.

Notification settings

Setting Name	Option Name (configuration file)	Description
Notification Message	*Notify*	Specify a string message to notify the user that the system is being quarantined. The message limit is 255 characters. Certain characters are not allowed, such as ($), (!), (`), (‘),(*) and some characters require escapes, such as (\"). Test any special characters before using in production. NOTE: The Notification Message option is not supported on Windows 10 and 11 Home edition or Linux endpoints. Notification messages in languages other than English might require a different character code. For example, in the case of Japanese messages, apply the following character codes: For Windows: Shift-JIS, and for macOS: UTF-8. Character codes are applied when the notification message is defined in the taniumquarantine.dat file. Default: `No notification`
*= To specify configuration settings in `taniumquarantine.dat`, use the following format: `OPTION:OptionName:OptionValue`		

© 2025 Tanium Inc. All Rights Reserved

5. Click **Save**.

Delete a profile

To delete a profile, from the Main menu, go to **Modules > Threat Response > Management > Quarantine** and select a profile. Click  Delete. When a quarantine profile is deleted, the reactions that use that profile revert to using the default quarantine profile on the next intel deployment, regardless of whether the quarantine packages are generated after the deletion or not. If the quarantine packages are generated, but intel is not deployed, the reactions or response actions will fail. For this reason, deploy intel before generating the packages.

Duplicate a profile

You can duplicate a profile to create a version of the profile that is tailored to a specific scenario. The name of the duplicated profile has the time stamp that the original profile was duplicated to the profile name. To duplicate a profile, from the Main menu, go to **Modules > Threat Response > Management > Quarantine** and select a profile. Click  Duplicate.

Edit a profile

To edit a profile ,from the Main menu, go to **Modules > Threat Response > Management > Quarantine** and select a profile. Click  Edit.

Export a profile

To export a profile, from the Main menu, go to **Modules > Threat Response > Management > Quarantine** and select a profile. Click  Export. The profile is exported to the downloads directory of the web browser in JSON format.

Export all profiles

To export all profiles, from the Main menu, go to **Modules > Threat Response > Management > Quarantine**. Select the profiles that you want to export and click **Export All**. The profiles are exported to the downloads directory of the web browser in JSON format.

Import a profile

To import a profile, from the Main menu, go to **Modules > Threat Response > Management > Quarantine**. Click **Import**. Drag and drop the profile that you want to import in either JSON or DAT format. Alternatively, you can browse to the profile. Click **Import**.

© 2025 Tanium Inc. All Rights Reserved

Generate Quarantine Packages

When you have created a profile and assigned rules to the profile, you can **Generate Packages** to create quarantine packages that you deploy to targeted endpoints.

BEST PRACTICE

Deploy intel before generating quarantine packages.

Quarantine package descriptions

Package Name	Description
Threat Response - Quarantine Endpoint [Windows]	The Threat Response - Quarantine Endpoint [Windows] package uses Windows IPsec policies to quarantine the endpoint. You can also add custom rules and options. See Reference: Create custom quarantine rules on page 347 for more information. NOTE: You cannot use Windows IPsec Quarantine on networks where a domain IPsec policy is already enforced. **Check that the IPsec Policy Agent service is running on the endpoints** Optionally, you can verify that the IPsec Policy Agent is listed as a running service in Windows. 1. In Interact, ask the question: Get Service Details containing "PolicyAgent" from all machines with Service Details containing "PolicyAgent" 2. In the table that gets returned, check the results in the following columns. • **Service Status**: Running or Stopped • **Service Startup Mode**: Manual or Automatic 3. If necessary, drill down into the results to determine which endpoints do not have the IPsec Policy Agent running.

© 2025 Tanium Inc. All Rights Reserved

Quarantine package descriptions (continued)

Package Name	Description
Threat Response - Quarantine Endpoint [Linux]	The Threat Response - Quarantine Endpoint [Linux] package quarantines endpoints that are running Linux-based operating systems that support the use of the **iptables** module. IMPORTANT You cannot use Threat Response - Quarantine Endpoint [Linux] on endpoints where SELinux is enforcing without first adding a policy for Tanium Quarantine. Deploy the **Apply Linux Quarantine SELinux Policy** package to endpoints that are enforcing SELinux policies to add a policy for Tanium Quarantine. When the policy for Tanium Quarantine is added to an endpoint that is enforcing SELinux, you can quarantine the endpoint using the **Apply Linux IPTables Quarantine** package. Verify that endpoints are not using Network Manager Threat Response - Quarantine Endpoint [Linux] checks to ensure that the **iptables** module is installed and disables the use of the **Network Manager** module on endpoints that are targeted for quarantine. You can check for Linux-based endpoints that are running Network Manager by using the **Linux Network Manager** sensor to determine if Network Manager is enabled. In Interact, type network manager to find the sensor. This sensor has no parameters.
Threat Response - Quarantine Endpoint [Mac]	The Threat Response - Quarantine Endpoint [Mac] package quarantines endpoints that are running Mac OS X operating systems that support the use of Packet Filter (PF) rules. This package creates packet filter rules that isolate endpoints by eliminating communication with network resources. PF software must be installed on endpoints that are targeted for quarantine.

1. From the Main menu, go to **Modules > Threat Response > Management > Quarantine**. Click **Generate Packages**.
2. You can view the status of the package creation from **Management > Audit > Tasks.** Each time you generate quarantine packages a task is listed that is named **Generate Quarantine Packages**.
3. When you have generated packages that contain the quarantine parameters that you have defined in the profile that you used to generate the package, you can deploy the packages to endpoints. Follow the steps in test quarantine on endpoints to deploy the packages to endpoints.

Test quarantine on endpoints

By default, the quarantine on the endpoint blocks all communication except with the Tanium Server.

IMPORTANT
Do not deploy quarantine packages to production endpoints without testing first.

© 2025 Tanium Inc. All Rights Reserved

1. Target computers for quarantine. The questions provided assume that the endpoints have been assigned a name that matches a convention for identifying them as test endpoints.
   a. Click **Create a Question**, and ask one of the following questions to target an appropriate group of endpoints.
      i. `computer name contains testendpointname and is windows equals true`
      ii. `computer name contains testendpointname and is linux equals true`
      iii. `computer name contains testendpointname and is mac contains true`
   b. Select the row from the drill-down question results, and click **Deploy Action**.
2. In the **Deployment Package** field, type the name of the quarantine package that you want to deploy:
   - `Threat Response - Quarantine Endpoint [Windows]`
   - `Threat Response - Quarantine Endpoint [Linux]`
   - `Threat Response - Quarantine Endpoint [Mac]`
3. (Optional) Define quarantine rules and options.
   For more information about quarantine rules, see Reference: Create custom quarantine rules on page 347.
   - If you already attached a `taniumquarantine.dat` file to the package you are deploying, you do not need to make any other configurations.
   - Otherwise, select **Override Config** to apply custom rules to the action.
   - If you are using the options and rules in this package deployment, select any options that you want to enable and enter your custom quarantine rules into the **Custom Quarantine Rules** field.
4. Click **Show Preview to Continue** to preview the targeting criteria for the action. Click **Deploy Action**.
5. Verify quarantine of the targeted endpoint.
   Confirm that the computer has no available means of communication to resources other than Tanium Server and any endpoints that you configured in custom quarantine rules.
   You can use RDP (Windows), SSH (Linux/macOS), the Ping network utility, or a similar means to confirm that communication is blocked. By default, the only traffic that the quarantine allows is between Tanium Client on the quarantined computer and Tanium Server over port 17472. If the computer is a server that must allow connections to name servers, verify that those connections are allowed to pass through.
6. Verify the visibility of the quarantined computer to Tanium Server.
   a. Target the endpoint with a question or sensor.
   b. Check the sensor results for the visibility of the quarantined endpoint.
   c. On the Quarantine dashboard, click **Isolated Machines**. A single computer is listed with a `Yes` on the **Quarantine: Isolated Machines** page.

Action folders are located under the Tanium Client installation folder on the endpoint, usually `Downloads\Action_XXXX.log`.

© 2025 Tanium Inc. All Rights Reserved

View quarantined endpoints

You can easily and immediately see what endpoints are quarantined from the **Overview** page of the Threat Response workbench. You can remove endpoints from quarantine from the **Overview** page of the Threat Response workbench. For more information on removing endpoints from quarantine, see Remove quarantine.

Remove endpoints from quarantine

You can remove endpoints from quarantine from the **Overview** page of the Threat Response workbench. In the Quarantined Endpoints section of the **Overview** page of the Threat Response workbench, view the endpoints that are currently quarantined. Select one or more endpoints to remove from quarantine and click **Remove from Quarantine**.

Alternatively, you can deploy the `Threat Response - Unquarantine Endpoint [Windows]`, `Threat Response - Unquarantine Endpoint [Linux]`, or `Threat Response - Unquarantine Endpoint [Mac]` package to the endpoint to remove the quarantine from the computer. Use RDP (Windows), SSH (Mac/Linux), the Ping utility, or another method to confirm the removal of the quarantine and the normal communication of the test computer.



Removing endpoints from quarantine from the workbench uses a response action, which enables targeting of offline endpoints. The packages only target online endpoints.

Reference: Create custom quarantine rules

You can define quarantine rules and options by either attaching a configuration file to the package, or by selecting options in Tanium Console when you deploy a quarantine action. Using this technique only impacts standard platform actions. For most quarantine operations, use the Threat Response workbench or response actions.

Attach configuration file to package

You can attach a `taniumquarantine.dat` configuration file that defines quarantine rules and options to either a new package or the existing Quarantine packages. Then push that package out to the endpoints. For an example `taniumquarantine.dat` file, see Reference: Custom rules examples on page 349.

1. From the Main menu, go to **Administration > Content > Packages**.
2. You can either create a new package, or edit one of the existing Quarantine packages:
   - `Threat Response - Quarantine Endpoint [Windows]`
   - `Threat Response - Quarantine Endpoint [Linux]`
   - `Threat Response - Quarantine Endpoint [Mac]`

© 2025 Tanium Inc. All Rights Reserved

3. Update the `taniumquarantine.dat` file.
    a. To download the current file, click **Download**.
    b. Remove the file that is currently in the package.
    c. Click **Add** to upload the updated `taniumquarantine.dat` file.
4. Click **Save** to save the updates to the package.

Add custom quarantine rules that allow connectivity for Direct Connect and Live Response to the quarantine package to avoid issues collecting artifacts during an investigation.

Select options in user interface when you deploy Quarantine actions

When you deploy the `Threat Response - Quarantine Endpoint [Windows]`, `Threat Response - Quarantine Endpoint [Linux]`, or `Threat Response - Quarantine Endpoint [Mac]` actions, you can define the quarantine rules and options as a part of that action. For more information, see Test quarantine on endpoints on page 345.

Reference: Custom rules and options

Custom rules format

The format for custom rules is not case sensitive. Put each rule on a new line. Trailing white spaces are not supported. This format is used for both the configuration file and in the user interface.

```
Direction:Protocol:IPAddress:CIDR:Port
#Comment
```

Direction

Valid values: `IN` or `OUT`
Specifies whether incoming or outgoing traffic is allowed.

Protocol

Valid values: `ICMP`, `TCP`, `UDP`
If you specify ICMP, the ICMP protocol is allowed to communicate to and from the specified addresses. This limitation is because IPSec does not filter ICMP Type/Codes. The filtering is done by advfirewall.

When using quarantine rules to block the ICMP protocol, the MTU negotiation packages can become blocked when the size of the MTU package on the endpoint is larger than the router allowed MTU size. Normally the router will see a packet that is too large and send an ICMP packet to the endpoint to identify that the packet is too large and advises lowering the permissible MTU size. If the negotiation packet is not able to reach the destination due to quarantine, the endpoint can become unresponsive. The endpoint is still is quarantined but loses communication with the Tanium Server. Disabling ICMP traffic while quarantined should only be done after proper testing.

© 2025 Tanium Inc. All Rights Reserved

IPAddress

Specifies any IPv4 address or you can use `ANY` for all.

CIDR

Valid values: `0-32` or, if `ANY` is used in IPAddress, undefined.
Subnet masks in dotted decimal format are not permitted in the input file. Undefined (blank) is same as /32 and uses the IPAddress only.

Port

Valid values: `0-65535` or undefined
Leave undefined (blank) to permit all ports. Ranges are not currently supported, only individual ports or all ports can be defined.



When using the Custom Quarantine Rules parameter in the package, the total characters should be 1100 or less. If you need more characters, you can use a custom DAT file.

Reference: Custom rules examples

Example for **Custom Quarantine Rules** field

```
IN:UDP:10.0.0.21:32:161
OUT:UDP:10.0.0.21:32:162
```

This example defines two rules:

- Allow SNMP queries (UDP Port 161) from another device at 10.0.0.21.
- Allow SNMP traps (UDP Port 162) to be sent to a device at 10.0.0.21.



This example demonstrates the use of parameter options in the package and not a `taniumquarantine.dat` file.

`taniumquarantine.dat` sample file

For DAT files, each entry must be on one line; you cannot use pipe (|) characters to combine lines. Trailing white spaces are not supported.

© 2025 Tanium Inc. All Rights Reserved

```
#Allow ICMP out to a specific IP Address
OUT:ICMP:192.168.10.15:32:0
#Allow ICMP in from a specific IP Address
IN:ICMP:192.168.20.10:32:0
#Allow ICMP out to any IP Address
OUT:ICMP:ANY::0
#Allow ICMP in from any IP Address
IN:ICMP:ANY::0
#Allow Kerberos to DC (10.10.1.10) - to allow SMB access
OUT:TCP:10.10.1.10::88
#Allow TCP port 80 in from a specific /24 subnet
IN:TCP:192.168.1.0:24:80
#Allow UDP port 161 in from a specific IP Address
IN:UDP:10.0.0.21:32:161
#Allow HTTPS (tcp 443) out to a specific /16 subnet
OUT:TCP:192.168.0.0:16:443
OPTION:ALLDNS:TRUE
OPTION:CURRENTDNS:FALSE
OPTION:ALLDHCP:TRUE
OPTION:TANIUMSERVERS:TRUE
OPTION:CHECKTS:TRUE
OPTION:NOTIFY:This Device has been Quarantined
#Allow Live Endpoint/Direct Connect from LAN to Tanium Module Server
(192.168.10.9)
OUT:TCP:192.168.10.9:32:17475
#Allow Live Endpoint/Direct Connect from remote endpoint to Zone Server
(172.16.31.31)
OUT:TCP:172.16.31.31:32:17486
#Allow Live Response from LAN to NAS (\\192.168.10.135\Tanium\THR-Live-Response)
OUT:TCP:192.168.10.135:32:22
#Allow Live Response from LAN to NAS (\\192.168.10.135\Tanium\THR-Live-Response)
OUT:TCP:192.168.10.135:32:443
#Allow Live Response from LAN to NAS (\\192.168.10.135\Tanium\THR-Live-Response)
OUT:TCP:192.168.10.135:32:445
```

© 2025 Tanium Inc. All Rights Reserved

Exporting audit data

You can review actions taken from the Threat Response workbench to audit for malicious internal actions or to validate remediation steps. For more information about viewing notifications and task status, and viewing and exporting action log data, see Troubleshooting.

Events and alerts generated by Threat Response are sent to Connect. By configuring a Connect destination, this information is actionable outside of Tanium. Export data from Threat Response to Tanium Connect destinations, such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server, to gain visibility into Threat Response actions that users have performed during a specific time range.



Audit log and system notification pruning runs every 24 hours and the default retention for audit logs and system notifications is 90 days. You can use the Threat Response API to change the number of days to a maximum of 365. If you need to retain audit logs or system notifications for longer periods, send the data to Tanium Connect. Tasks are not pruned.

You can send the following events to Connect:

Events to send to Tanium Connect

Detection events	Action type
Group configurations	• Creating • Deleting • Modifying
On-demand scans	• Initiating • Deleting
Service settings	• Resetting • Modifying
System user	• Modifying
Labels	• Modifying • Deleting

© 2025 Tanium Inc. All Rights Reserved

Events to send to Tanium Connect (continued)

Detection events	Action type
Intel	• Creating • Deleting • Modifying • Modifying labels of intel
Alerts	• Deleting • Modifying • Deleted batches of alerts • Modifying batches of alerts
Profiles	• Creating • Editing • Importing • Deleting • Reordering profiles • Deploying a profile • Duplicating
Configurations	• Creating • Editing • Importing • Deleting • Duplicating
Filters	• Creating • Editing • Importing • Deleting • Duplicating
Intel Deployment	• Migrating

© 2025 Tanium Inc. All Rights Reserved

Events to send to Tanium Connect (continued)

Detection events	Action type
Service Account	• Setting • Deleting
Threat Response Settings (With the exception of detection or recorder specific settings)	• Creating • Editing • Deleting
Recorder Settings	• Uploading Zone Server certifications • Adding, deleting, or deploying Zone server settings to endpoints • Saving values for default module server address, service URL for snapshot uploads, and the maximum number of rows to export from live connections
Live Endpoint Connections	• Creating and deleting live endpoint connections • Viewing directories from live endpoint connections • Downloading and deleting files from live endpoint connections • Creating and deleting exports from live endpoint connections • Creating, uploading, and deleting snapshots from live endpoint connections • Creating and deleting events from live endpoint connections
Live Response Collections	• Creating • Editing • Duplicating • Deleting

© 2025 Tanium Inc. All Rights Reserved

Events to send to Tanium Connect (continued)

Detection events	Action type
Live Response Destinations	• Creating • Editing • Duplicating • Deleting
Live Response File Collectors	• Creating • Editing • Duplicating • Deleting
Live Response Script Sets	• Creating • Editing • Duplicating • Deleting
Live Response Packages	• Generating
Notifications	• Creating (Including notifications for intel safeguards) • Deleting

Tanium Connect

To export data from Threat Response to Connect destinations such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server, create a connection.

Before you begin

- You must have access to Connect with Connect User role.
- You must have Connect 4.10.5 or later.

Create a connection

1. From the Connect menu, click **Connections** and then click **Create Connection** .
2. Under General Information, provide a name and description for the connection. Select a Log Level.
3. Under Source, Select **Tanium Threat Response Audit Source**.

© 2025 Tanium Inc. All Rights Reserved

4. In the type field, select **Audit Report**.
5. In the **Batch Size** field, enter the number of rows of Threat Response data to return at a time. The default is 1000.
6. In the **Minutes to Collect** field, enter the number of minutes prior to the start time to collect data. For an exhaustive log, leave this field blank.
7. Select **Send the Audit State Column to Tanium Connect as JSON** to send the data in JSON format. If selected, data is sent as a string object.
8. Under Destination, select where you want Connect to send the audit data. Provide any additional configuration for the type of destination you select.
9. Provide any filters you want to apply to the data. You can use filters to modify the data that you are getting from your connection source before it is sent to the destination.
10. Expand **Columns** to review the format of the output data. Make changes as appropriate and add any custom columns that are relevant.
11. Click **Save Changes**.

Test a connection and review audit data

1. From the Connect **Overview** page, click **Connections**.
2. Click the connection that you created for Threat Response audit data.
3. Click **Run Now**. Confirm that you want to run the connection.
4. View the summary of the run.
5. View the audit report in the destination that you configured for the connection.

Schedule the connection

For information on how to run connections on a schedule, see Tanium Connect User Guide: Schedule connections.

© 2025 Tanium Inc. All Rights Reserved

Maintaining Threat Response

Perform monthly maintenance tasks to ensure that Threat Response successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Threat Response is not performing as expected, you might need to troubleshoot issues or change settings. See Troubleshooting Threat Response on page 361 for related procedures.

Review and remediate Tanium Threat Response issues

1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the Client Management menu, select **Client Health** and click the **Deployment** tab.
3. Review the **Health Failures** panel for issues that relate to Threat Response domains:
    - `dec` (Direct Connect)
    - `index` (Tanium Index)
    - `recorder` (Tanium Recorder)
    - `stream` (Tanium™ Stream)
    - `threatresponse` (Tanium™ Threat Response Client Extension)
4. Investigate health failures and review the status and configurations of endpoint tools for Threat Response, including:
    - Non-default configuration settings on clients
    - Tools versions
    - Client extension versions
    - (Windows only) Tanium™ Driver status and version
    - Berkeley Packet Filter (BPF) support

    For the specific steps, see .
5. From the Main menu, go to **Modules > Threat Response > Overview**.
6. Go to the **Metrics** panel and check the Threat Response **Coverage**.
7. If the **Coverage** is lower than expected, investigate and remediate coverage as described under . If coverage issues might result from missing or misconfigured Threat Response profiles, click the **Coverage** value to open the **Profiles** page and review profile configurations. For details about profile issues, see .
8. To investigate and remediate other Threat Response issues, see:

Get Threat Response endpoint tools status and configurations

Ask the question: `Get Client Extensions - Status from all machines`.

© 2025 Tanium Inc. All Rights Reserved

This retrieves the status of Client Extensions (such as Threat Response, Index, Recorder), Threat Response profile status, and any client extensions health issues.

The following domains are Threat Response related:

- dec
- index
- recorder
- stream
- threatresponse

Threat Response related domains

Domain	Key	Value	Explanation
[Any]	health_check	[Any value]	For more information, see Tanium Client Management User Guide: Monitor the client health overview in Client Management and take corrective actions to ensure Threat Response is healthy in your environment.
recorder	has_event_source	[Multiple]	This displays which event sources the Tanium Recorder is using.
recorder	has_subscription	[Multiple]	This displays which Tanium components are consuming events from the Tanium Recorder process.
recorder	is_using_tanium_driver	True | False	(Windows Only) This displays if the Tanium Recorder Process is consuming events from the Tanium Driver.
recorder	min_requirements_met	True | False	This displays if the system meets the minimum CPU requirements for the Tanium Recorder to run. Two or more CPU cores are required.
threatresponse	applied_intel_revision	[Any]	This value identifies the version of Threat Response intel currently installed on the endpoint.
threatresponse	applied_profile applied_profile_id applied_profile_revision	[Multiple]	These keys return information about which Threat Response profile name, profile unique ID, and profile revision is currently in use on the endpoint.

Ask the question: `Get Client Health - Client Settings from all machines`.

© 2025 Tanium Inc. All Rights Reserved

This question returns any non-default configuration settings that are set explicitly on the clients. If settings are not explicitly set, no results are displayed for that setting. It is useful to review these settings for any non-default settings which you can set on Threat Response or Tanium Client components and causing unexpected behavior.

The following domains are Threat Response related:

- dec
- index
- recorder
- stream
- threatresponse

Ask the question: `Get Endpoint Configuration - Tools Status from all machines`.

This returns the Threat Response tools versions targeted and installed to verify the correct endpoint tools are installed. Current tools versions can be referenced in the Threat Response release notes: https://kb.tanium.com/Category:Tanium_Threat_Response

The following Tool Names are Threat Response related:

- Threat Response
- Threat-response-cx
- Threat Response Stream
- cx-stream
- Incident Response
- index-cx
- Direct Connect
- dec-cx
- Driver
- Recorder
- Recorder BPF Support

Ask the question: `Get Client Extensions - Installed Extensions from all machines`.

This returns the installed Threat Response client extension binary versions. Current client extension binary versions can be referenced in the Threat Response release notes: https://kb.tanium.com/Category:Tanium_Threat_Response

The following Domains are Threat Response related:

- index
- recorder
- stream

© 2025 Tanium Inc. All Rights Reserved

- threatresponse

Ask the question: `Get Tanium Driver Status from all machines with Is Windows matches true`.

This returns the installed Tanium Driver Status from all Windows machines (Tanium Driver is supported on Windows only). The following tables include some common Tanium Driver Status results:

Tanium Driver successful installation results

Successful installation	
Tanium Driver Status Results that indicate it is properly installed and running	Service Status: `SERVICE_RUNNING` Driver install path: `\SystemRoot\System32\drivers\TaniumRecorderDrv.sys`

Tanium Driver installation errors

Errors to look for	
Tanium Driver	Install Recommended
Tanium Driver Service is not installed	Service Installation: Not installed
Tanium Driver Service is present but not running	Service Status: Not started Service Status: SERVICE_STOPPED
Tanium Driver is not installed	Driver Location: Not installed Driver Version N/A Driver Controller Version N/A

Ask the question: `Get Tanium Driver Version from all machines with Is Windows matches true`.

This returns the installed Tanium Driver Version of the binary on disk from all Windows endpoints (Tanium Driver is supported on Windows only). This can be useful to verify that the correct version of the Tanium Driver is installed.

Tanium Driver Versions by Threat Response release: https://kb.tanium.com/Category:Tanium_Threat_Response

Use the following sensors to help troubleshoot and determine if eBPF is supported and available for use by Tanium Recorder on Linux systems.

Sensors to evaluate eBPF support

Sensor	Results
Recorder - Is BPF BCC Supported	Returns True if BPF BCC is supported on the endpoint.
Recorder - Is BPF CO-RE Supported	Returns True if BPF CO-RE (Compile Once Run Everywhere) is supported on the endpoint.
Recorder - Is BPF Supported Details	Returns details about whether or not BPF is supported on the endpoint.

For more information, see Tanium Interact User Guide: Asking questions.

© 2025 Tanium Inc. All Rights Reserved

Monitor and troubleshoot Threat Response coverage

The following table lists contributing factors into why the Threat Response coverage metric might be lower than expected, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Threat Response

Contributing factor	Corrective action
Tools not deployed	Ensure the Threat Response Action Group is set to `All Computers`. Ensure the Trends Action Group is set to `All Computers`. Ensure that all endpoints belong to a computer group that is defined in a Threat Response profile.
Tools in an unhealthy state	Refer to the client health features in Client Management. For more information, see Tanium Client Management User Guide: Monitor the client health overview in Client Management and take corrective actions to ensure Threat Response is healthy in your environment.

Monitor and troubleshoot mean time to investigate threats

The following table lists contributing factors into why the mean time to investigate threats metric might be higher than expected, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Threat Response

Contributing factor	Corrective action
Alert status not being properly updated in the Threat Response workbench	Ensure analysts are accurately updating alerts from `New` to `In Progress` and then from `In Progress` to `Resolved`. If alerts are sent to a SIEM or another location, ensure that your workflow uses the Tanium Threat Response API to appropriately set alert state in Tanium to be able to track this metric correctly.

Monitor and troubleshoot mean time to remediate threats

The following table lists contributing factors into why the mean time to investigate threats metric might be higher than expected, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Threat Response

Contributing factor	Corrective action
Alert status not being properly updated in the Threat Response workbench	Ensure analysts are accurately updating alerts from `New` to `In Progress` and then from `In Progress` to `Resolved`. If alerts are sent to a SIEM or another location, ensure that your workflow uses the Tanium Threat Response API to appropriately set alert state in Tanium to be able to track this metric correctly.

© 2025 Tanium Inc. All Rights Reserved

Troubleshooting Threat Response

If Threat Response is not performing as expected, you might need to troubleshoot issues or change settings. For more information, see Contact Tanium Support on page 377.

General troubleshooting

- Collect logs
  - Collect troubleshooting information from the Threat Response service
  - Collect troubleshooting information from endpoints

Managing the Threat Response workbench

- View notifications
- View task status
- View and export log data

Endpoint troubleshooting

- Remove Threat Response tools from endpoints

Threat Response component troubleshooting

- Profiles and configurations
  - My device has no profile or the wrong profile
- Detection and Intel
  - No alerts are generated
  - Too many alerts are generated
- Index
  - Configure client disk space use
  - Files are not being hashed or indexed
- Recorder
  - The lifetime of recorder events is too short
  - File, network, or security events are not displayed on Oracle Linux server
  - Identify Linux endpoints that are missing auditd
  - Start or stop the recorder
- Live connections
  - Cannot establish a live connection

© 2025 Tanium Inc. All Rights Reserved

- Live Response
  - Test Live Response connections manually
- Stream
  - Stream is not sending data
  - Stream is sending too much data
- Live Response
  - Configuration not available or not updated to the latest settings when deploying package
  - Action not running on endpoint
  - Artifacts not being copied to destination
- Quarantine
  - Custom configurations are missing
  - Live Connections are not working while quarantined
  - Live Response is not working to copy files to the destination while quarantined
- Verify endpoint tools
- Contact Tanium Support
- Uninstall Threat Response

Collect logs

Collect troubleshooting information from the Threat Response service

Use Threat Response to compile a collection of logs relevant for troubleshooting. You can collect logs and other artifacts from the Threat Response service located on the server to help troubleshoot service side issues. The ZIP file is also known as a support bundle.

1. From the Threat Response overview page, click Help, then click the **Troubleshooting** tab.
2. Click **Create Package**. Normally creating the troubleshooting package takes a few minutes, but can take longer for large packages.
3. When the status of the package creation is complete, click **Download Package**.

The log zip file might take a few moments to appear in the download folder.

Collect troubleshooting information from endpoints

You can collect logs and other artifacts from individual endpoints to help resolve issues. Collecting logs from endpoints requires a live connection to the endpoint from which you want to gather troubleshooting information.

© 2025 Tanium Inc. All Rights Reserved

1. From the Main menu, click **Administration > Client Management** to open the **Client Management Overview** page.
2. From the Client Management menu, click **Client Health**.
3. In the Direct Connect section, create a live connection to the endpoint from which you want to collect troubleshooting information.
4. Click the Gather tab. In the domain section select Threat Response.
5. Click **Gather from Endpoint**.
6. A package is gathered from the endpoint. The name of the link is the time stamp of the troubleshooting package. Select the Must Gather that you want to download and click **Download** to download a ZIP file that contains troubleshooting information.

For more information about using client health features in Client Management, see Tanium Client Management User Guide: Monitor the client health overview in Client Management and Tanium Client Management User Guide: Access detailed client health and troubleshooting information on an endpoint.



The legacy **Troubleshooting** button has been removed from direct connections to endpoints and the **Must Gather** column from the grid for connected endpoints has been removed. Any previous Threat Response troubleshooting bundles are removed on upgrade to a newer version of Threat Response.

View notifications



Viewing notifications requires the **Threat Response Audit** permission.

From the Main menu, go to **Modules > Threat Response > Management > Audit > System Notifications**.These notifications show various Threat Response service related events and notifications. You can expand these notifications to view additional information.

- Alert Pruning: Notifies when alerts have been pruned from the Threat Response alerts database.
- Automatic Intel Deployment Error: Threat Response has failed to deploy the Intel database.
- Intel Deployment Excluded Intel: Possible corrupted Intel database.
- Endpoint Throttle: Alerts were throttled at the endpoint level for an Intel document. An endpoint throttles alerts that match five times in five minutes for the same intel document. When this occurs, alerts are not sent to the service until the cool off time of one hour occurs. After one hour, alerts are sent to the service again.
- Service Throttle Start: Alerts were throttled at the service level for an Intel document. You can customize the values for service level throttling from the Alert Throttling section of the Service Settings in the Threat Response workbench. Intel documents that initiate alerts at a rate that exceeds the settings you provide are disabled. If additional alerts match during the cool off period, the extension factor calculated time is added to the cool off time.

© 2025 Tanium Inc. All Rights Reserved

- Service Throttle Update: Alerts were throttled again after the original throttle start at the service level for an Intel document.
- Tanium Signal Stream Update: Threat Response updated to a new version of Tanium Signals.

To delete a notification, select the row and click **Delete**.

View task status



Viewing task status requires the **Threat Response Audit** permission.

You can view the status of and review other historic data for Threat Response tasks.

From the Main menu, go to **Modules > Threat Response > Management > Audit > Tasks**.

When troubleshooting, it is useful to identify tasks which have not been completed successfully. You can filter by task status:

- Error
- Incomplete
- Not Started
- Started

Some examples of Threat Response tasks include (but are not limited to):

- Deploy Profile
- Deploy Intel
- Deploy Tools
- Generate Live Response packages
- Response Action
- Start Index
- Suppress Alerts

In the event of an error, you can locate a specific task and expand the cell to view results and metadata from log files. The data that appears in the advanced details view provides information that is useful for troubleshooting and saves the time of trying to locate debugging information in lengthy log files or in formats that are not intended to be human readable.

View and export log data



Viewing and exporting log data requires the **Threat Response Audit** permission.

You can view and export data for actions in tables of the Threat Response database for Threat Response tasks. You can view and export audit data from the following tables of the Threat Response database:

© 2025 Tanium Inc. All Rights Reserved

- Alert
- Audit
- Collection Config
- Config
- Cron Task
- Endpoint Must Gather
- Event Evidence
- Export
- File Collector Set
- File Evidence
- File Management
- Filter
- Intel DB
- Intel Document
- Intel Document Label
- Label
- Live Connection
- Live Response Package
- Migration
- On Demand Scan
- Plugin Schedule Subscription
- Profile
- Response Action
- Script Set
- Service Account
- Settings
- Snapshot
- Source
- Suppression Rule
- Task

© 2025 Tanium Inc. All Rights Reserved

- Transfer Destination
- Yara Scope

1. From the Main menu, go to **Modules > Threat Response > Management > Audit > Logs**.
2. Expand any row to view JSON to show the details of the action.
3. (Optional) Select one or more actions and click **Export Selected Logs** to export data for the actions to the local downloads folder as a JSON file. Click **Export All** to export all the logs to the local downloads folder as a JSON file.
4. (Optional) Filter the table of actions to display a more focused list of actions. You can filter by specific tables in the Threat Response database, specific action types, specific personas, users, or a time range.

Remove Threat Response tools from endpoints

You can deploy an action to remove Threat Response tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:
   `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for , drill down as necessary, and select the targets from which you want to remove Threat Response tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select .
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   NOTE

   If reinstallation is blocked, you must unblock it manually:

   - To allow Threat Response to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

© 2025 Tanium Inc. All Rights Reserved

7. (Optional) To remove all Threat Response databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   CAUTION

   When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   BEST PRACTICE

   If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

9. Click **Show preview to continue**.
10. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

NOTE

If you have enabled Endpoint Configuration approval, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

My device has no profile or the wrong profile

The profile deployment process is the process of generating, saving, and deploying a profile from the server to the endpoint. If an endpoint, or client, does not have a profile or the incorrect profile, then the profile deployment action could have failed on the server.

Common reasons for failure include the following:

- The profile is disabled.
  - From the Main menu, go to **Modules > Threat Response > Management > Profiles**. Ensure that the intended profile is **Enabled**. Any endpoints that are targets of a disabled profile receive the next applicable enabled profile based on priority. Any configurations deployed by the profile before it was disabled are removed if no profile is currently applicable.
- The profile was not deployed.
  - From the Main menu, go to **Modules > Threat Response > Management > Profiles** and make sure a profile has successfully deployed. A profile has successfully deployed if it has a green check under the status column.
  - Verify the last deployment time.
  - Verify the Profile Targeting (Computer Groups).

© 2025 Tanium Inc. All Rights Reserved

    - Verify the Profile Priority.
    - Verify the Profile ID on the Profiles page and compare to the output of **Client Extensions - Status**.
    - Verify the Profile Revision on the Profiles page and compare to the output of **Client Extensions - Status**.
    - From the **Threat Response > Tasks** page, verify that the profile was deployed successfully.
- The profile was deployed, but it did not reach the client.
    - Verify in Endpoint Configuration that the Threat Response Profile configuration was updated.
    - Verify the Endpoint Configuration - Manifest was updated on the endpoints.
    - Verify there are no pending Endpoint Configuration Approvals.
    - Verify there are no pending Action Approvals for Endpoint Configuration.
- The profile was deployed and received, but the client was unable to apply the correct configuration.
    - Verify the currently installed Threat Response Profile ID and revision matches the Threat Response deployed profile using the **Client Extensions - Status** sensor.
    - Review the `<Tanium Client>\Logs\threat-response.txt` log to identify issues applying the profile.
    - If endpoints are not applying configurations as expected, try creating a simple change to the profile (for example, change the description) and save the profile to increment the revision number. Then deploy the profile again. The updated revision forces the client to re-apply the entire profile.
    - Review the output of the `Client Extensions - Status` sensor for any health_check results.

Should none of these actions resolve the issue then a server-side troubleshooting bundle is required. For more information, see Collect Troubleshooting Bundle. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium for analysis.

No alerts are generated

Outside specific testing of intel should be assumed that alert generation is a scarce occurrence. Under normal circumstances it is to be hoped that a given system does not generate alerts based on deployed intel, as such no alerts or very low numbers of alerts should be considered normal operation. The alert generation and collection process involve interaction between the client and the service of Threat Response and so validation of both of these is required to validate that the process is working as expected.

The following steps are targeted at troubleshooting a testing scenario where alert generation is expected because of user interaction on an endpoint to validate the detection and alerting process.

To validate that the service side parts of the process have been applied correctly:

- Ensure that profile and intel have been deployed as expected and that the system shows the correct profile ID and revision and intel revision from the **Client Extensions - Status** sensor. If this output shows issues then the following steps would be recommended as initial remedial actions:

© 2025 Tanium Inc. All Rights Reserved

    - Redeploy all relevant profiles and intel from the Threat Response profiles page validate any actions do not require approval and are waiting in the queue.
    - Ensure that the Threat Response System Notifications page does not show throttle messages for the intel document in question.

Should none of these actions resolve the issue and either the profiles have not deployed, or the questions have not been issued then a server-side troubleshooting bundle is required. For more information, see Collect Troubleshooting Bundle. Return the collected information and a detailed description of the issue seen as well as the steps taken to Tanium for analysis.

If the above checks show the expected results then endpoint investigation is required. To validate that the endpoint is working as expected (these actions assume access to the endpoint is available) the following steps should be attempted:

- Validate that the **Endpoint Configuration - Tools** Status sensor shows all relevant tools installed.
- Ensure that any actions being taken to trigger alerts are starting from a new process each time they are attempted (such as, if a user is trying to trigger a signal from a command prompt then open a new command prompt for each attempt).
- Ensure that the Threat Response **System Notifications** page does not show throttle messages for the intel document in question.

If one of the above actions show unexpected output, then take the following steps to try and resolve the issue:

- Redeploy any tools that have not deployed as expected by using the **Endpoint Configuration - Reinstall Tool** action targeting the tool in question.
- Wait for throttles to clear for a given intel document or attempt firing a different intel document from the endpoint.
- Ensure commands to trigger alerts are executed in a new instance for each attempt.

If none of the above steps show an issue or provide a resolution then a client-side troubleshooting bundle is required. For more information, see Collect Troubleshooting Bundle. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Too many alerts are generated

The following steps are directed at validating the source of the high number of alerts and should be performed to ensure that any remedial actions are targeted correctly:

- Validate the intel document names and ID's associated with the number of alerts using the Trends Boards, Threat Response home page graphics or the **Alerts** page.
- Investigate if the alerts matches are intended or unintended based on the syntax of the indicator and the alert details provided.

Depending on the findings from the above actions there can be several courses of action that you can perform to reduce the alert load:

© 2025 Tanium Inc. All Rights Reserved

- Remove the intel document from the profile associated with affected endpoints and then redeploy the profile and intel database.
- Modify the intel document to ensure it is matching the correct artifacts or endpoint behavior and redeploy the intel document.
- For Tanium Signal-based alerts it is possible to create a suppression rule associated with the intel document to prevent specific circumstances from creating alerts. Once configured, a suppression rule must be deployed to the endpoints using the Intel deployment action to ensure alerts are suppressed on the endpoints and on the service.
- Configure or tune endpoint or service throttling to prevent higher than expected numbers alerts from being sent for a given intel document.



An alert backlog can grow on the endpoints and in the service, which could mean that the above remedial actions prevents new alerts on the endpoints, and might not resolve the situation with a very large backlog.

Should alerts continue to arrive in the user interface and cause performance issues, it is advised to create a support case with Tanium with a detailed description of the issue seen and the steps taken.

The lifetime of recorder events is too short

The lifetime of the recorder is controlled by the settings for the database from the Threat Response recorder configuration. The default values are 1 gigabyte (GB) for size and 90 days for length.

The volume of data sent to the recorder is regulated by the filters associated with its configuration. These filters are used to include or exclude specific elements of telemetry in the recorder database.

There are two possible reasons why the database does not hold events for a sufficient retention period:

- The size of the DB is not sufficient to store all of the required data.
- The length of time the DB holds events is too short.

There are multiple options available to ensure the required data is recorded in the database:

- Modify the maximum size of the recorder database.
- Modify the maximum retention period for the recorder database.
- Modify the filters for the configuration to reduce the recorded events in the DB.



The settings for maximum size and retention period take effect in the order that they are received by the endpoint. If the maximum database size is reached before the maximum lifetime of the database then the recorder will start pruning events from the database to ensure that it remains at the maximum size. Alternatively, if the maximum retention period is reached before the maximum size is reached then the recorder starts pruning events.

© 2025 Tanium Inc. All Rights Reserved

You might need to change both configurations at the same time to achieve the required outcome. Because of the uncertainty of the impact of changing the database size or the retention period these options are less optimal when trying to regulate the retention period.

If it is impossible to change the maximum size (this is the most common situation), or more control of the content of the database is required, then the alternative, and preferred, option is to use filters to remove unnecessary recorded telemetry from the database. This exercise requires some investigation of the database content and validate the unnecessary content and create filters for it.



When deploying filters, any process filters that are applied filters all activity from that process (there is no file, registry, etc data recorded) as such these are the broadest filters and can reduce the amount recorded telemetry quickly. Deploying other filters for the other event types (file, network, registry, security, and image events) are more specific and can be used to remove very specific events from the recorded telemetry. For additional information about filters, see Create filters.

On Linux endpoints, a System filter enables you to specify a path that is excluded from audit configuration. When providing this type of filter, be sure to provide the full path to the file.

Should there continue to be issues with the volume of data recorded then a client-side troubleshooting bundle and an export of the Recorder configuration are required. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

File, network, or security events are not displayed on Oracle Linux server

If you are not seeing file, network, or security events in the recorder results, you can disable SELinux. When SELinux is enabled and the auditd fallback is disabled on Oracle Linux, only process information is returned. Alternatively, ensure that the Client Recorder Extension configuration parameters are set as follows:

- **CX.recorder.AuditdStopAuditdService** is set to 0.
- **CX.recorder.AuditdEnableAudispdFallback** is set to 1.

For more information, see Client Recorder Extension User Guide: Configuring recorded events .

Identify Linux endpoints that are missing auditd

If Linux endpoint events are not being recorded, they might be missing the audit daemon and audispd services. Ideally, the audit daemon is installed and configured before installing the Threat Response module, but it is possible for endpoints to come online at a later time.

1. (Optional) Create the auditd package.
   You can either create a general installation package and put the logic in the scripts or you can have a simple script and put the logic in the Tanium query. See Tanium Core Platform User Guide: Creating and managing packages.
2. Ask the question: `Get Installed Application Exists[audit] from all machines with Is Linux containing "true"`.

© 2025 Tanium Inc. All Rights Reserved

3. Deploy the appropriate auditd package to the identified endpoints.



If you need to distribute the package to a large number of endpoints, spread the changes out over time to avoid a negative impact on the network.

Start or stop the recorder

You might need to manually start or stop the recorder.

Resolve the underlying issue and restart the recorder. Or, if you find that the recorder is using more system resources than expected, you can stop the recorder and troubleshoot the issue.

1. Identify the computer groups that contain endpoints on which you want to stop the recorder.
2. Deploy a profile that does not contain a recorder configuration to the computer groups you want to target.
3. You can optionally create a live endpoint connection to specific endpoints to troubleshoot any issues.

To start the recorder, deploy a profile that has a recorder configuration to the targeted computer groups.

Configure client disk space use

You can use two configurable client settings for disk space use:

CX.core.DiskSpaceWarningPercent

CX.core.DiskSpaceCriticalPercent

Use these client settings to surface warnings about the amount of disk space left on the disk that the Tanium Client is installed on. By default, these settings are 5% and 1% respectively. CX-core checks the available disk space on the endpoint once every five minutes.

When the DiskSpaceCriticalPercent threshold is reached, IndexCX pauses indexing until the free disk space is increased above the critical threshold. Endpoints that have reached either the Warning or Critical thresholds will display a health check in the Client Extensions - Status sensor. Use the following question to list all endpoints with a disk space health check:

`Get Computer Name and Client Extensions - Status contains disk space from all machines with Client Extensions - Status contains disk space`

Modifying client disk space thresholds

The free disk space thresholds can be set via the command line or using a Tanium Action. For more information, see Tanium Client Management User Guide: Managing client settings and Index configurations.

Command line example:

Set the warning threshold to 10 percent and the critical threshold to 5 percent:

```
./TaniumClient config set CX.core.DiskSpaceWarningPercent 10
```

```
./TaniumClient config set CX.core.DiskSpaceCriticalPercent 5
```

© 2025 Tanium Inc. All Rights Reserved

Tanium action example

Windows	Non-Windows
Package: Modify Tanium Client Setting	Package: Modify Tanium Client Setting [Non-Windows]
RegType: REG_DWORD	Type: Numeric
ValueName: CX.core.DiskSpaceWarningPercent	ValueName: CX.core.DiskSpaceWarningPercent
ValueData: 10	ValueData: 10

You can check non-default disk space settings with the question:

`Get Tanium Client Explicit Setting[CX.core.DiskSpaceWarningPercent] and Tanium Client Explicit Setting [CX.core.DiskSpaceCriticalPercent] from all machines`

A result of “Key/Value not found” indicates that the setting is the default value (5% for Disk Space Warning and 1% for Disk Space Critical).

Files are not being hashed or indexed

Index is optimized to minimize endpoint resource utilization. The solution indexes local file systems, computes file hashes, and gathers file attributes and magic numbers. This information is recorded in an SQLite database for detection and reporting of threat indicators for files at rest.

Index creates and maintains an inventory of the file system on an individual endpoint with the following operations:

- Detect file changes
- Compute file hashes
- Calculate magic number

For more information about indexing in Threat Response, see Client Index Extension User Guide.

If the configuration does not exclude the file or location then it is possible that Index is not running on the system for some reason.

To validate that this is the case, perform the following steps:

- Use the **Client Extensions - Status** sensor to validate that Index is running and configured.
- Validate that the scheduled action for the starting index, **Threat Response - Start Index** has reached the endpoint by reviewing the scheduled action and its targeting.

If the index process is not showing as running then it might be possible to restart the process by manually targeting the relevant action for the operating system in the **Threat Response - Start Index** (Linux/Mac/Windows) question.

© 2025 Tanium Inc. All Rights Reserved

Cannot establish a live connection

Live connections are established using the shared service component Direct Connect. Elements of the Direct Connect services are included in the Threat Response user interface to enable users to search for devices and make connections and the capabilities for downloading files or navigating the Recorder database are provided on top of this connection via Threat Response.

To ensure that Direct Connect is working as expected, perform the following steps:

- Review the outputs of the **Get Client Extensions - Status** sensor to validate that the endpoints in question have the required endpoint tools deployed and are working as expected.
- Review the outputs of the **Direct Connect - Connection Configuration** sensor to validate that the endpoints in question have the correct configuration.
- Review the outputs of the saved question **Direct Connect - Endpoint Info** and ensure the endpoint in question is showing in the results (this can also serve to refresh the data that shows in the live response search bar).

Should the outputs of these commands show an issue then it might be required to force the distribution of the Direct Connect tools to the endpoint in question to ensure that it is ready to accept connections, issuing the action **Endpoint Configuration - Reinstall Tool** for the relevant operating system, and selecting the option for Direct Connect in the Tool Name dropdown list to reinstall the tools on the endpoint.

Should there continue to be issues connecting to the endpoint then a client-side troubleshooting bundle should be collected for Direct Connect. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Test Live Response connections manually

To test Live Response connections manually, see Generate known_hosts and test connections.

Stream is not sending data

Stream provides the capability to send telemetry from the recorder directly to destinations outside of the Tanium infrastructure such as SIEM. The stream capability relies on the correct configuration from the service as well as access to the configured destination to be able to perform its function. It is important to first validate that the receiving side for the telemetry is configured and running as expected testing this from target endpoints is the only way to ensure that connectivity is working as expected. As with most components, there is a service and an endpoint component to troubleshooting problems.

To validate the service side components of Stream:

- Validate that Stream and Recorder tools are deployed and reporting as expected using the **Get Client Extensions - Status** sensor.
- Ensure the Stream configuration is pointing to the correct destination or URL and that any credentials are included to ensure that the endpoints have access to the destination.
- Validate that **Dry Run** is not enabled in the configuration. By default, **Dry Run** is enabled when you create a stream configuration.

© 2025 Tanium Inc. All Rights Reserved

- Ensure that any filters applied to the Stream configuration send the required telemetry from the endpoint to the destination system.
- When deploying a custom configuration, validate that the JSON syntax is correct and that the client is able to parse and deploy the given configuration.
- If investigating Linux systems then validate that there are no system file filters that may be preventing the Recorder from gathering the telemetry required to send.

Should all of the above appear to be configured and working as expected then this might indicate an endpoint issue. To validate that the endpoint is working as expected it can require access to the endpoint.

- Ensure enough time has passed for Stream to reach the threshold of sending data, this can take some time depending on the configuration and the amount of telemetry being generated by the endpoint.
- Ensure that the endpoint can resolve and contact the destination server for receipt of telemetry (there are many options for this but commands such as ping, host, nslookup, telnet, etc.).
- Validate that the endpoint has recorded the events expected to be sent to the destination utilizing the live connection capability.

If after verifying the availability of the receiving side, service, and endpoint configurations and connectivity there is still no telemetry being received then a client-side troubleshooting bundle and an export of the Stream configuration are required. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Stream is sending too much data

The volume of data sent from any given client to the Stream destination is determined by the activity on the endpoint and the configuration that has been applied to Stream. While the volume of data is not in essence an error it is something that may cause issues on specific endpoints or on the receiving side.

There are two mechanisms available to reduce the volume of data being sent by Stream depends on the configuration and the requirements for the data being sent from each endpoint. The two options available are:

- Disable specific event types from being sent.
- Use filters to reduce the numbers of specific events sent.

Depending on the requirements for the use of the telemetry being sent from Stream, you can use one or both of these mechanisms to reduce the total amount of data being sent from the endpoints:

- Removing an entire event type from the configuration removes all of the events of this type from the data being sent from the endpoint to the receiving side. Unlike Recorder filters, when disabling process events the other event types for the given process are sent (although the references to process in these events are no longer resolvable).
- Utilizing filters to remove events from being sent represents a more specific reduction in data volumes. The filters available are the same as those available for the Recorder configuration and can be reused.

© 2025 Tanium Inc. All Rights Reserved



NOTE

It should be considered that although Stream utilizes data from the Recorder, Stream is a separate subscription to the recorder data, and options including the Stream configuration do not impact the data being sent to the Recorder database, or vice versa.

Should there continue to be issues with the volume of data being sent via Stream then a client-side troubleshooting bundle and an export of the Stream configuration are required. Return the collected information and a detailed description of the issue seen and the steps taken to Tanium via a support case for analysis.

Configuration not available or not updated to the latest settings when deploying package

If a configuration is not available or has not updated to the latest settings when you deploy a Live Response package to endpoints, from the Main menu, go to **Modules > Threat Response > Management > Live Response**, and click **Generate Packages**. You must update all Live Response packages that you deploy to endpoints to reflect updated configurations.

Action not running on endpoint

If an action is not running on an endpoint, ensure that the connection to the endpoint is working by testing the Live Response connections manually. For more information, see testing connections manually.

If the connections to remote endpoints work correctly, but actions are not running, confirm that action approval is not stopping the action from running. Action approval means that actions a user initiates cannot deploy until another user approves those actions. Approvers can be users with the Administrator reserved role or a role that grants Approve Action and Sensor read permissions. If your organization allows exceptions to approval requirements, you can configure a role that grants Bypass Action Approval permission. For more inforrmation, see Tanium Console User Guide: Managing Action Approval.

Artifacts not being copied to destination

If artifacts are not being copied to the destination, review the Live Response log in the folder that corresponds to the action ID.

In addition to the standard action logs on the endpoint (`Tanium_Client_Location\Downloads\Action_###\Action_####.log`), a log file of activities resides in the same directory. This file follows the naming convention: `YYYYMMDDhhmm_LR.log`.

When collection completes, the `YYYYMMDDhhmm_LR.log` is copied to the destination. The action log is not copied to the destination.

Use both the action log and the Live Response log to troubleshoot problems. The action log captures messages written to standard error (`stderr`).

© 2025 Tanium Inc. All Rights Reserved

Custom configurations are missing

The content of `taniumqarantine.dat` is restored to the default values every time quarantine content is updated. For example, if you upgrade Threat Response or install a newer version of the Tanium Quarantine solution, any custom configurations that you have added to the quarantine packages either by using the Live Response workbench or by editing the packages manually are overwritten with the default versions of the packages.

BEST PRACTICE

Keep a backup copy of any Live Response packages that contain custom configurations so that you can restore your customized packages after a tools upgrade.

Live Connections are not working while quarantined

If you are unable to make live connections to endpoints that you have quarantined, make sure that the ports that Tanium Direct Connect uses to communicate with remote endpoints are not blocked on the target endpoint, and that the IP addresses for the Tanium Module Server (or Zone Server, if applicable) are not blocked. For a list of the ports that must be enabled for remote endpoint communication, see Tanium Direct Connect User Guide: Requirements.

Live Response is not working to copy files to the destination while quarantined

If Live Response is not copying files to the destination while quarantined, make sure that all destination IP addresses and ports for the protocols you are using are defined in the quarantine configuration. For more information, see Isolating Endpoints: Reference: Custom rules and options.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version. For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions.

Uninstall Threat Response

You might need to remove Threat Response from the Tanium Module Server for troubleshooting purposes.

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. Under Threat Response, click **Uninstall**. Click **Proceed with Uninstall** to complete the process.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about how to submit a support case, see Case Submission Form.

© 2025 Tanium Inc. All Rights Reserved

Reference: Common health check issues

Review common Threat Response health check issues and possible solutions. For information about general issues in Threat Response, see Troubleshooting Threat Response on page 361.

Fatal error loading subscriptions: auditd raw logging is enabled. Not loading rules.

Cause

This health check appears when `auditd.conf` is configured to log messages.

Solution

Consider using RAW logging only in instances where disabling would cause a data point of interest to be dropped. For example, use RAW logging if an endpoint has excess resources to handle the CPU and IO load, and an application such as Splunk is analyzing data. To disable RAW logging, deploy the **Recorder - Disable Raw Logging [Linux]** package. The package edits the `auditd.conf` file with the appropriate setting to disable raw logging for the version of auditd on the endpoint. Deploy the **Recorder - Auditd [Linux]** package to restart auditd after disabled raw logging.

Scan completion took longer than configured scan interval. Maybe under spec or subscription misconfigured?

Cause

This health check appears when an Index scan exceeds the configured scan interval.

Solution

Ensure that all endpoints meet the system requirements for the Client Index Extension and that the subscription is configured properly. Change the scan interval in the Index configuration.

Subscription has dropped events: <subscription name>

Cause

This health check appears when the number of pending journal files has reached or exceeded the maximum number of pending files. A single dropped event causes this health check to display; however, no count of dropped events is provided.

© 2025 Tanium Inc. All Rights Reserved

Solution

No action is required with the recorder to address this error. Ensure that systems meet the minimum requirements. Action to mitigate this health check might be required on the consumer end if, for example, a Signal returns many matches that result in alerts.

System minimum requirements not met to enable features: Single CPU detected. Not loading rules.

Cause

This health check appears when an endpoint with a single CPU is detected.

Solution

The Client Recorder Extension does not start on endpoints with a single logical core without updating the `CX.recorder.EnableSingleCpuRequirement` configuration setting to 0. To update `CX.recorder.EnableSingleCpuRequirement` to 0, edit the **Recorder - Set Recorder Extension Setting [*OS*]** package to add a parameter with the configuration key `EnableSingleCpuRequirement` and a value of `0`, and deploy the package to appropriate endpoints. Alternatively, you can run the following command from the Tanium Client directory on endpoints to update this configuration setting:

(Windows) `TaniumClient.exe config set CX.recorder.EnableSingleCpuRequirement 0`

(Linux and macOS) `./TaniumClient config set CX.recorder.EnableSingleCpuRequirement 0`

All configured audit rules did not load. Check rules for correctness. Recorder may not be seeing all events.

Cause

This health check appears when there is a problem with the existing ruleset. Auditd is encountering an invalid rule and is aborting rule loading. Recorder determines this by returning a nonzero exit code for `auditctl -R /etc/audit/audit.rules`.

Solution

Ensure that no rules are invalid in `/etc/audit/rules.d/audit.rules`.

© 2025 Tanium Inc. All Rights Reserved

TaniumAuditPipe not running.

Cause

This health check appears when the TaniumAuditPipe is installed, but not currently running. This health check commonly occurs. when running SELinux with a policy that was incorrectly applied.

Solution

Ensure that the directories for Tanium client and above are not symlinks. Ensure that all policies for SELinux have been installed correctly. Review the var/log messages and ensure the pipe is starting.

Failed to configure Tanium Driver provider. Check extensions log. Recorder may not be seeing all events.

Cause

This health check appears when a connection to the Tanium Driver cannot be established.

Solution

Use the **Tanium Driver Status** and **Tanium Driver Version** sensors to ensure that the Tanium Driver is installed properly and running. Look for error messages in these sensors. You can use Tanium Endpoint Configuration to reinstall the Tanium Driver and/or Tanium Recorder.

Fatal error loading subscriptions: waiting for TaniumAuditPipe to be available. Not getting events.

Cause

This health check appears when audispd is not running, or if it is crashing. The audit pipe is a child process of audispd.

Solution

Ensure that the directories for the Tanium client and above are not symlinks. Ensure that all policies for SELinux have been installed correctly. Review the var/log messages and ensure the pipe is starting.

Profile and/or Intel not fully resolved.

Cause

This health check displays when profiles or intel are not up to date or are incomplete on endpoints.

© 2025 Tanium Inc. All Rights Reserved

Solution

Ensure that intel and profiles are deployed to endpoints and that all endpoints meet the minimum requirements. Use the **Client Extensions - Status** sensor to verify that the profile and intel versions are the expected versions.

© 2025 Tanium Inc. All Rights Reserved

Reference: Alert data

The Threat Response Client Extension (THR-CX) manages detections and all endpoint resource throttling related to detection and alerting. Alerts are actively acknowledged when they are received and are not duplicated for the same artifact on the same endpoint.

THR-CX returns a finding when intel matches occur. Findings are made available to the Threat Response service. If conditions are met, the Threat Response service uses the content in the finding to generate an alert. A finding consists of the objects it describes. Through the `whats` object in a finding, a list of `ArtifactActivity` types is provided. In the `ArtifactActivity`, an `acting_artifact` (an Artifact) and/or some `relevant_actions` can be returned. Those `relevant_actions` are `ArtifactAction`, which each can have an `Artifact` and a `verb` that describes relevant data points.

A finding from a Signal features an `acting_artifact` that holds a process. Depending on the Signal definition, it can contain zero or more `relevant_actions`. For example, if the Signal was checking to see if a file was deleted, there would be a `relevant_action` that has a `FileArtifact` as the target with a `verb` of "`delete`".

A sample alert


```
{
  "Alert Id": "00000000-0000-0000-21c5-3019f0ac0143",
  "Timestamp": "2022-06-10T23:19:38.000Z",
  "Computer Name": "mediatoo",
  "Computer IP": "172.16.8.70",
  "Intel Id": 365,
  "Intel Type": "tanium-signal",
  "Intel Name": "Unsigned Process Creating a Binary",
  "Intel Labels": "Beta,Execution,Windows",
  "Match Details": {
    "finding": {
      "whats": [
        {
          "intel_intra_ids": [
            {
              "id": 1204114022
            },
            {
              "id": 1670888670
            },
```


© 2025 Tanium Inc. All Rights Reserved

```
            {
              "id": 2753281896
            },
            {
              "id": 3854795733
            }
          ],
          "source_name": "recorder",
          "artifact_activity": {
            "relevant_actions": [
              {

              },
              {
                "verb": 6,
                "target": {
                  "file": {
                    "path": "C:\\Users\\Bob\\AppData\\Local\\Temp\\gfw-install-CZejgRlL.exe",
                    "hash": {
                      "md5": "d41d8cd98f00b204e9800998ecf8427e",
                      "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                      "sha256":
"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                    },
                    "size_bytes": {

                    },
                    "modification_time": "2022-06-10T23:19:37.000Z",
                    "instance_hash_salt": "132993767777627641"
                  },
                  "instance_hash": "8639093369865776459",
                  "artifact_hash": "15425104092171844481"
                },
                "timestamp": "2022-06-10T23:19:37.000Z",
                "tanium_recorder_event_table_id": "4611686018468280136"
```


© 2025 Tanium Inc. All Rights Reserved

```
              },
              {
                "verb": 6,
                "target": {
                  "file": {
                    "path": "C:\\Users\\Bob\\AppData\\Local\\Temp\\gfw-install-CZejgRlL.exe",
                    "hash": {
                      "md5": "d41d8cd98f00b204e9800998ecf8427e",
                      "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                      "sha256":
"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                    },
                    "size_bytes": {

                    },
                    "modification_time": "2022-06-10T23:19:37.000Z",
                    "instance_hash_salt": "132993767777627641"
                  },
                  "instance_hash": "86390933698657764 59",
                  "artifact_hash": "15425104092171844481"
                },
                "timestamp": "2022-06-10T23:19:37.000Z",
                "tanium_recorder_event_table_id": "4611686018468280136"
              }
            ],
            "acting_artifact": {
              "process": {
                "handles": [

                ],
                "pid": 8372,
                "arguments": "\"C:\\Program Files\\Git\\usr\\bin\\mktemp.exe\" -t gfw-install-
XXXXXXXX.exe",
                "file": {
                  "file": {
```


© 2025 Tanium Inc. All Rights Reserved

```
                    "path": "C:\\Program Files\\Git\\usr\\bin\\mktemp.exe",
                    "hash": {
                      "md5": "2204459dcbf34aed8906daac26db6f56"
                    }
                  },
                  "instance_hash": "7306911300040087486",
                  "artifact_hash": "7306911300040087486"
                },
                "user": {
                  "user": {
                    "name": "Bob",
                    "domain": "MEDIATOO"
                  }
                },
                "parent": {
                  "process": {
                    "handles": [

                    ],
                    "pid": 7528,
                    "arguments": "sh \"C:\\\\Program Files\\\\Git\\\\mingw64\\\\bin\\\\git-
update-git-for-windows\" --quiet --gui",
                    "file": {
                      "file": {
                        "path": "C:\\Program Files\\Git\\usr\\bin\\sh.exe",
                        "hash": {
                          "md5": "0d46559e826c8a7b5d432d0a91954ba2"
                        }
                      },
                      "instance_hash": "4573824187960625975",
                      "artifact_hash": "4573824187960625975"
                    },
                    "user": {
                      "user": {
                        "name": "Bob",
```


© 2025 Tanium Inc. All Rights Reserved

```
                    "domain": "MEDIATOO"
                  }
                }"start_time": "2022-06-10T23:19:37.000Z",
                "tanium_unique_id": "8426546338933681227"
              },
              "instance_hash": "2725601412602158353",
              "artifact_hash": "6063500060437154276"
            },
            "start_time": "2022-06-10T23:19:37.000Z",
            "tanium_unique_id": "3601155573093657773"
          },
          "instance_hash": "17370642301569032073",
          "artifact_hash": "16343609532904785305",
          "is_intel_target": true
        }
      }
    }
  ],
  "domain": "threatresponse",
  "intel_id": "365:2:761d796b-b362-455f-98ae-6d0472ecf640",
  "hunt_id": "1",
  "threat_id": "1204114022,1670888670,2753281896,3854795733",
  "source_name": "recorder",
  "system_info": {
    "os": "Microsoft Windows 11 Pro",
    "bits": 64,
    "platform": "Windows",
    "build_number": "22000",
    "patch_level": "10.0.22000.0.0"
  },
  "first_seen": "2022-06-10T23:19:38.000Z",
  "last_seen": "2022-06-10T23:19:38.000Z",
  "finding_id": "2433404061633741123",
  "reporting_id": "reporting-id-placeholder"
```


© 2025 Tanium Inc. All Rights Reserved

```
    },
    "match": {
      "version": 1,
      "type": "process",
      "source": "recorder",
      "hash": "16343609532904785305",
      "properties": {
        "pid": 8372,
        "args": "\"C:\\Program Files\\Git\\usr\\bin\\mktemp.exe\" -t gfw-install-XXXXXXXX.exe",
        "recorder_unique_id": "3601155573093657773",
        "start_time": "2022-06-10T23:19:37.000Z",
        "ppid": 7528,
        "user": "MEDIATOO\\Bob",
        "file": {
          "md5": "2204459dcbf34aed8906daac26db6f56",
          "fullpath": "C:\\Program Files\\Git\\usr\\bin\\mktemp.exe"
        },
        "parent": {
          "pid": 7528,
          "args": "sh \"C:\\\\Program Files\\\\Git\\\\mingw64\\\\bin\\\\git-update-git-for-
windows\" --quiet --gui",
          "recorder_unique_id": "8426546338933681227",
          "start_time": "2022-06-10T23:19:37.000Z",
          "ppid": 10396,
          "user": "MEDIATOO\\Bob",
          "file": {
            "md5": "0d46559e826c8a7b5d432d0a91954ba2",
            "fullpath": "C:\\Program Files\\Git\\usr\\bin\\sh.exe"
          }
        }
      }
    }
  },
  "MITRE Techniques": "[\"T1036\",\"T1036.001\"]",
  "Impact Score": ""
```


© 2025 Tanium Inc. All Rights Reserved

```
}
```

The following fields in the parent JSON provide information that is globally relevant to all alerts and provides information to identify the alert and details about where the alert originated. Not all fields are included in every alert, and sometimes values can be omitted. For example, if Tanium Impact is not present in the environment, you can expect an empty value for Impact score.

Parent JSON fields and descriptions

Field	Field type	Description
`Alert ID`	string	A unique ID that is assigned to an alert.
`Timestamp`	timestamp	The timestamp for when the alert was generated on the endpoint.
`Computer Name`	string	The name of the endpoint on which the alert was generated.
`Computer IP`	IP address	The IPv4 address of the endpoint on which the alert was generated.
`Intel ID`	number	The ID of the intel document that matched an event to generate the alert.
`Intel Type`	string	The type of intel that matched an event to generate the alert.
`Intel Name`	string	The name of the intel document that matched an event to generate the alert.
`Intel Labels`	string	Any labels that have been assigned to the intel document that matched an event to generate the alert.
`MITRE Techniques`	array	Any MITRE techniques that are relevant to the intel document that matched an event to generate the alert. For more information about MITRE, see MITRE Attack Framwork.
`Impact Score`	number	The score assigned to the endpoint by Tanium Impact. For more information about Tanium Impact, see Tanium Impact User Guide.

The following tables provide a reference to the objects in the alert, and descriptions of the fields each object supports.

- Artifact
- ArtifactAction (relevant_actions)
- ArtifactActivity
- ArtifactHash
- AutomationEngine
- DNSRequestArtifact
- DriverArtifact

© 2025 Tanium Inc. All Rights Reserved

- ExternalSecurityEvent
- FileArtifact
- Finding
- Finding.Whats
- IntraIdContext
- LocalSystemInfo
- MicrosoftDefenderEventArtifact
- NetworkPortArtifact
- ProcessArtifact
- ProcessArtifact.Handle
- ReactionStatusDetails
- ServiceArtifact
- SignatureData
- Step
- StepResult
- UserArtifact
- WindowsPEInfo
- WindowsPEInfo.Exports
- WindowsPEInfo.Section
- WindowsPEInfo.Import
- WindowsPEInfo.Symbol
- RegistryArtifact
- RegistryArtifact.MultiSZ
- RegistryArtifact.Value

Finding

Finding fields and descriptions

Field	Field type	Description
`intel_id`	string	An ID that represents the intel document.
`hunt_id`	string	An ID that represents a hunt. A hunt is a grouping of the currently active intel.

© 2025 Tanium Inc. All Rights Reserved

Finding fields and descriptions (continued)

Field	Field type	Description
`threat_id`	string	An ID that provies a way to differentiate findings within a single intel document, this field offers a way to separate.
`source_name`	string	Informational name of where Threat Response found the finding. Valid values are live, tanium-index, tanium-recorder, netstat, and at-rest.
`system_info`	LocalSystemInfo	The information about the system on which the finding happened.
`artifact`	Artifact	Deprecated.
`first_seen`	timestamp	The timestamp of the first finding of the instance.
`last_seen`	timestamp	The timestamp of the last finding of the instance.
`whats[]`	Finding.Whats	A short description of the finding. This is specific to the intel type and the finding itself. Some examples might be the rule name for YARA, the hash for a bad hash, or the technique for process injection.
`description`	string	A text description of the finding.
`finding_id`		Internal use only.
`legacy_detect_alert_payload`		Deprecated.
`reporting_id`	string	Information that you can use to identify whether the alert was triggered by an On-Demand scan. This data includes the Scan ID when an alert is the result of an On-Demand Scan.
`domain`	string	For all findings, the domain is `threatresponse`.
`reason`	string	Information from a third-party source, for example, Deep Instinct. If available, this field can contain the cause for the finding.

Finding.Whats

Finding.Whats fields and descriptions

Field	Field type	Description
`source_name`	string	Informational name of where Threat Response found the finding. Valid values are live, tanium-index, tanium-recorder, netstat, and at-rest.
`artifact_activity`	ArtifactActivity	The state change that is responsible for the current state.

© 2025 Tanium Inc. All Rights Reserved

Finding.Whats fields and descriptions (continued)

Field	Field type	Description
`intel_intra_ids[]`	IntraIdContext	Internal use only. The intel id that generated this What instance. When that intel specifies intra_id's, those may be populated here to give indication of what conditions were met to yield to the match.
`security_event`	ExternalSecurityEvent	An external entity was used to locate a finding. It is possible to learn information from the external event and even enrich it. In as much, this is supplemental to the `what` but not part of it.
`additional_fields`	protobuf "Struct"	Free-form extra data for findings; populated for Defender, Deep Instinct, and Process Injection

ArtifactActivity

ArtifactActivity fields and descriptions

Field	Field type	Description
`acting_artifact`	ProcessArtifact	Corresponds to the ProcessArtifact object.
`relevant_actions[]`	ArtifactAction	Corresponds to the ArtifactAction object.
`bystander`	ProcessArtifact	Corresponds to the ProcessArtifact object. In some cases, when a detection is made, it is due to an inline inspector such as Microsoft defender or Deep Instinct inspecting an object because a handle to it has been opened. In many cases, this ends up being Tanium or the EPP solution.

IntraIdContext

IntraIdContext fields and descriptions

Field	Field type	Description
`id`	deprecated; internal use	Internal use only. Deprecated.
`token`	string	Internal use only.
`id_v2`	internal use	Internal use only.
Note: A data structure for internal use that helps identify the components within an intel document that matched.		

© 2025 Tanium Inc. All Rights Reserved

ExternalSecurityEvent

ExternalSecurityEvent fields and descriptions

Field	Field type	Description
`timestamp`	timestamp	The timestamp of the external security event.
`type_identifier`	string	A representation of the type or non-unique id of the event in string format.
`unique_identifier`	string	A unique identifier to the event source if one is available.
`external_action`	enum	a value that corresponds to the type of external action. Value values are (0)unspecified, (1)clean, (2)quarantine, (3)remove, and (4)block.

ArtifactAction (relevant_actions)

ArtifactAction fields and descriptions

Field	Field type	Description
`verb`	enum	The type of action. Valid values are (0)unknown, (1)connect (including reconnect), (2)accept, (3)disconnect, (4)delete, (5)open, (6)create, (7)move (including rename), (8)write, (9)query, (10)load, (11)inject, (12)execute, and (13)set permissions.
`target`	Artifact	The entity acted-upon. For file move or rename, this is the destination. In most cases this holds the entity, which can be various artifact objects.
`origin`	Artifact	Used for things like move/rename of file. Most times this is not used.
`timestamp`	timestamp	The timestamp of the action.
`tanium_recorder_event_table_id`	number	For cases where the target of this action can be found in the Tanium Recorder, this id allows for deeper inspection.
`tanium_recorder_context`	MatchItem	Deprecated.

Artifact

Artifact fields and descriptions

Field	Field type	Description
`instance_hash`	hash	Uniquely identifes an artifact instance across time on a single endpoint.
`artifact_hash`	hash	Correlates related items across time on a single endpoint or even across endpoints.
`is_intel_target`	bool	Indicates that this was the artifact originally scoped and found by the intel.

© 2025 Tanium Inc. All Rights Reserved

Artifact fields and descriptions (continued)

Field	Field type	Description
process	ProcessArtifact	Corresponds to the ProcessArtifact object.
user	UserArtifact	Corresponds to the UserArtifact object.
file	FileArtifact	Corresponds to the FileArtifact object.
windows_registry	RegistryArtifact	Corresponds to the RegistryArtifact object.
windows_event_log	WindowsEventLogArtifact	Corresponds to the WindowsEventLogArtifact object.
service	ServiceArtifact	Corresponds to the ServiceArtifact object.
dns	DNSRequestArtifact	Corresponds to the DNSRequestArtifact object.
port	NetworkPortArtifact	Corresponds to the NetworkPortArtifact object.
driver	DriverArtifact	Corresponds to the DriverArtifact object.
windows_defender_event	WindowsDefenderEventArtifact	Corresponds to the WindowsDefenderEventArtifact object.

LocalSystemInfo

LocalSystemInfo fields and descriptions

Field	Field type	Description
os	string	The operating system of the endpoint on which the finding occurs.
build_number	string	If available, the build level of the operating system of the endpoint.
patch_level	string	If available, the patch level of the operating system of the endpoint.
bits	number	Valid values are 32 or 64.
platform	enum	The platform of the endpoint. Valid values are: (0)Unknown, (1)Windows, (2)Mac, (3)Linux, (4)AIX, and (5)Solaris.

ProcessArtifact

ProcessArtifact fields and descriptions

Field	Field type	Description
pid	number	The process ID of the ProcessArtifact.
name	string	The name of the ProcessArtifact.

© 2025 Tanium Inc. All Rights Reserved

ProcessArtifact fields and descriptions (continued)

Field	Field type	Description
working_directory	string	The working directory of the ProcessArtifact.
arguments	string	The command line of the ProcessArtifact including any arguments.
start_time	timestamp	The start time of the ProcessArtifact.
end_time	timestamp	The end time of the ProcessArtifact.
file	FileArtifact	Corresponds to the FileArtifact object.
user	UserArtifact	Corresponds to the UserArtifact object.
parent	ProcessArtifact	Corresponds to the ProcessArtifact type that represents an ancestory of the ProcessArtifact.
tanium_unique_id		A unique ID assigned to the ProcessArtifact.
handles[]	ProcessArtifact.Handle	Corresponds to the ProcessArtifact.Handle object.
tanium_recorder_table_id		An ID that corresponds to a table in the Recorder database.

ProcessArtifact.Handle

ProcessArtifact.Handle fields and descriptions

Field	Field type	Description
name	string	A possible name of the ProcessArtifact.
type	string	A possible type of the ProcessArtifact.

UserArtifact

UserArtifact fields and descriptions

Field	Field type	Description
name	string	The user who initiated the artifact.
domain	string	The domain (or group on macOS/Linux) under which the artifact was initiated.
user_id	string	The user ID of the user who initiated the artifact.
group_id	string	The group ID of the user who initiated the artifact.

© 2025 Tanium Inc. All Rights Reserved

FileArtifact

FileArtifact fields and descriptions

Field	Field type	Description
`path`	string	The full path in the file system for the FileArtifact.
`hash`	ArtifactHash	Corresponds to the Artifact Hash type. The algorithm and hash of the file artifact.
`size_bytes`	number	The file size of the FileArtifact.
`modification_time`	timestamp	The timestamp of the most recent file modification for the FileArtifact.
`instance_hash_salt`	hash	Internal use only.
`magic_number`	number	Deprecated.
`magic_number_hex`	string	The hex value of the magic number for the FileArtifact.
`windows_pe_info`	WindowsPEInfo	Information about Windows PE endpoints.
`signature_data`	SignatureData	Corresponds to the SignatureData object.
`container`	Artifact	Corresponds to the FileArtifact object.

RegistryArtifact

RegistryArtifact fields and descriptions

Field	Field type	Description
`hive`	string	The hive (a logical group of keys, subkeys, and values) in the registry.
`key_path`	string	The path to the key in the registry.
`modification_time`	timestamp	The timestamp of the most recent modification for the RegistryArtifact.
`num_subkeys`	number	The number of subkeys of the RegistryArtifact.
`num_values`	number	The number of values of the RegistryArtifact.
`values[]`	RegistryArtifact.Value	Corresponds to the RegistryArtifact.Value object.

RegistryArtifact.Value

RegistryArtifact.Value fields and descriptions

Field	Field type	Description
`name`	string	The name of the registry value.

© 2025 Tanium Inc. All Rights Reserved

RegistryArtifact.Value fields and descriptions (continued)

Field	Field type	Description
reg_dword	number	The data type of the registry value. Only one of these fields are supported for each object instance.
reg_qword	number	
reg_sz	string	
reg_expand_sz	string	
reg_multi_sz	WindowsRegistryArtifact.MultiSZ	
reg_binary	bytes	

RegistryArtifact.MultiSZ

RegistryArtifact.MultiSZ fields and descriptions

Field	Field type	Description
reg_sz[]	string	A sequence of null-terminated strings, terminated by an empty string (\0). The following is an example: String1\0String2\0String3\0LastString\0\0. The first \0 terminates the first string, the second-from-last \0 terminates the last string, and the final \0 terminates the sequence.

WindowsEventLogArtifact

WindowsEventLogArtifact fields and descriptions

Field	Field type	Description
eid	number	A unique ID that corresponds to a specific endpoint.
log_name	string	Name of the event log to which events from different logging components are written. Events are commonly logged for system, security, and applications.
source_name	string	Name of the program or software causing the event log.
message	string	The content of the log that matched to generate the alert.
computer	string	Name of the computer logging the event.
category	string	Identifies the type of recorded event log. Application developers can also define task categories to serve as extra information about the event.
gen_time	timestamp	Includes the date and time when the event occurred.
write_time	timestamp	Includes the date and time when the event was logged.

© 2025 Tanium Inc. All Rights Reserved

WindowsEventLogArtifact fields and descriptions (continued)

Field	Field type	Description
`category_number`	number	A numeric representation of the category.

ServiceArtifact

ServiceArtifact fields and descriptions

Field	Field type	Description
`name`	string	A string that corresponds to the name of an artifact that comes from a Windows service value.
`descriptive_name`	string	A string that corresponds to the descriptive name of an artifact that comes from a Windows service value.
`description`	string	A string that corresponds to the description of an artifact that comes from a Windows service value.
`started_as`	string	A string that corresponds to the started at time of an artifact that comes from a Windows service value.
`mode`	string	A string that corresponds to a Windows service value.
`status`	string	A string that corresponds to a Windows service value.
`type`	string	A string that corresponds to a Windows service value.
`exe`	FileArtifact	Corresponds to the FileArtifact object.
`dll`	FileArtifact	Corresponds to the FileArtifact object.
`process`	ProcessArtifact	Corresponds to the ProcessArtifact object.
`arguments`	string	The command line of the ServiceArtifact including any arguments.

DNSRequestArtifact

DNSRequestArtifact fields and descriptions

Field	Field type	Description
`host`	string	The service that runs Domain Name System (DNS)
`record_name`	string	The name of the record that directs a hostname to an IP address.
`ttl`	number	The duration of time to cache a query before requesting a new one.

© 2025 Tanium Inc. All Rights Reserved

DNSRequestArtifact fields and descriptions (continued)

Field	Field type	Description
ipv4	string	The IPv4 address of the endpoint.
cname	string	A record that functions as an alias for domain names that share a single IP address.
observed_time	timestamp	Correlates to when the request was seen in a cache or in an actual request if that was available.
text_request	string	A text version of the record request.
text_response	string	A text version of the response to the record request.

NetworkPortArtifact

NetworkPortArtifact fields and descriptions

Field	Field type	Description
protocol	string	The protocol that was used in the network event. For example, HTTP.
local_ip	string	The IP address of the local endpoint.
remote_ip	string	The IP address of the remote endpoint.
local_port	number	The port used on the local endpoint.
remote_port	number	The port used on the remote endpoint.
state	string	The state of the remote network port. For example, forwarding.
process	ProcessArtifact	Corresponds to the ProcessArtifact object.
connection_time	timestamp	The timestamp of the network connection.

DriverArtifact

Driver artifact fields and descriptions

Field	Field type	Description
name	string	The name of the DriverArtifact.
file	Artifact	Corresponds to the FileArtifact object.

© 2025 Tanium Inc. All Rights Reserved

ArtifactHash

Artifact hash fields and descriptions

Field	Field type	Description
`md5`	string	The hash of the artifact using the MD5 hashing algorithm.
`sha1`	string	The hash of the artifact using the SHA1 hashing algorithm.
`sha256`	string	The hash of the artifact using the SHA256 hashing algorithm.

AutomationEngine

AutomationEngine fields and descriptions

Field	Field type	Description
`friendly_name`	string	The name given to a reaction by the user.
`dry_run`	boolean	Whether or not a reaction was run in audit mode.
`step`	Step	Repeated field of step results from an automation.

ReactionStatusDetails

ReactionStatusDetails fields and descriptions

Field	Field type	Description
`at`	timestamp	Timestamp at which the reaction was completed.
`automation_engine`	AutomationEngine	Collected details from an internal run of a reaction.

Step

Step fields and descriptions

Field	Field type	Description
`friendly_name`	string	The name of the reaction step given by the user.
`reaction_step_idx`	integer	An index of the step that was run. Zero based index.
`result`	StepResult	The result information for this step.
`artifact`	Artifact	A repeated artifact field of the artifacts that were acted on by the step.
`step_type`	string	A system specified string of a generalization of what the step was (Remove File, Kill Process, Quarantine, etc.)

© 2025 Tanium Inc. All Rights Reserved

StepResult

StepResult fields and descriptions

Field	Field type	Description
`step_name`	string	Name of the step. Matches friendly_name from Step.
`step_number`	integer	An index of the step that was run. Zero based index.
`step_description`	string	Description of what the step was doing.
`step_message`	string	Result message from the step. Empty if no errors.
`result_code`	enum	An enumeration of the result of a step. Valid values are (0)Step has not yet been run, (1)Step completed successfully with no errors, (2)Step completed with non-critical errors. Automation will continue, (3)Step failed with critical error. Automation will exit, (4)Step timed out
`start`	timestamp	Timestamp of when the step started.
`end`	timestamp	Timestamp of when the step completed.

SignatureData

SignatureData fields and descriptions

Field	Field type	Description
`status`	enum	The status of the signature data. Valid values are (0)Unverified, (1)Verified, (2)NoSignature, (3)Error, (4)Disallowed, (5)NotTrusted, (6)NotTrustedPolicy, (7)FileNotExists, (8)NotChecked, (9)Pending, (10)CheckingDisabled, and (11)TimedOut.
`issuer`	string	The entity who issued the signature.
`subject`	string	The subject of the signature.

MicrosoftDefenderEventArtifact

MicrosoftDefenderEventArtifact fields and descriptions

Field	Field type	Description
`timestamp_ms`	number	The timestamp of the Microsoft Defender event.
`event`	ETWDefenderEvent	The event ID of the Microsoft Defender event. For more information about Microsoft Defender events, see https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus.

© 2025 Tanium Inc. All Rights Reserved

WindowsPEInfo

WindowsPEInfo fields and descriptions

Field	Field type	Description
`type`	string	The type of object.
`timestamp`	timestamp	The timestamp of the object.
`sections[]`	WindowsPEInfo.Section	Corresponds to the WindowsPEInfo.Section object.
`exports`	WindowsPEInfo.Exports	Corresponds to the WindowsPEInfo.Exports object.
`imports[]`	WindowsPEInfo.Import	Corresponds to the WindowsPEInfo.Import object.

WindowsPEInfo.Section

WindowsPEInfo.Section fields and descriptions

Field	Field type	Description
`name`	string	The name of the section.
`size_bytes`	number	The size (in bytes) of the section.

WindowsPEInfo.Exports

WindowsPEInfo.Exports fields and descriptions

Field	Field type	Description
`name`	string	The name of the export.
`symbols[]`	WindowsPEInfo.Symbol	Corresponds to the WindowsPEInfo.Symbol object.

WindowsPEInfo.Import

WindowsPEInfo.Import fields and descriptions

Field	Field type	Description
`name`	string	The name of the import.
`symbols[]`	WindowsPEInfo.Symbol	Corresponds to the WindowsPEInfo.Symbol object.

© 2025 Tanium Inc. All Rights Reserved

WindowsPEInfo.Symbol

WindowsPEInfo.Symbol fields and descriptions

Field	Field type	Description
`name`	string	The name of the symbol.

© 2025 Tanium Inc. All Rights Reserved

Reference: Set up the zone proxy service

In Threat Response, the options for the Zone Proxy setup is contained in Tanium Direct Connect. To use Direct Connect to manage zone proxy connections, you must install and enable Direct Connect. For more information, see Tanium Direct Connect User Guide: Installing.

In earlier versions of Threat Response there was a requirement to make a configuration from Threat Response and import on the zone server. In the current version, the configurations for zone proxy are all contained in Direct Connect. When Direct Connect is configured and running there are no required actions for Threat Response. When the Direct Connect service is enabled when making a live connection the Threat Response service issues the **Deploy Direct Connect - Open Session** action.

To install Direct Connect and configure the Direct Connect Zone Proxy:

1. Install Direct Connect. See Tanium Direct Connect User Guide: Installing for more information.
2. Install and configure the Direct Connect Zone Proxy. See Tanium Direct Connect User Guide: Configure Zone Proxies for more information.

In an upgrade scenario, to get the zone proxy to run on the same ports are you have been using you need to stop and remove the current zone proxy infrastructure prior to installing the Direct Connect proxy and ensure that the ports are available for the new service. From Threat Response, click Settings and click the current zone server configuration. To move from this configuration to the Direct Connect configuration, use the same port in the Direct Connect configuration.

© 2025 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Threat Response

For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Threat Response example

The following mutation requires Threat Response and assigns the **Resolved** status to a Threat Response alert.

Assign Resolved status to an alert (`mutation.threatResponseAlertResolve`)

ASSIGN RESOLVED STATUS TO ALERT

The following request assigns the **Resolved** status to the Threat Response alert matching the GUID.

```
mutation exampleResolveTHRAlert($guid: ID) {
  threatResponseAlertResolve(ref: {guid: $guid}) {
    resolved
    guid
    error
  }
}
```

Include the GUID variable in the **Variables** panel or in your variables dictionary:

```
{
  "guid": "12345678-90ab-cdef-1234-567890abcdef"
}
```

Example response:

```
{
  "data": {
```

© 2025 Tanium Inc. All Rights Reserved

```
    "threatResponseAlertResolve": {
      "resolved": true,
      "guid": "12345678-90ab-cdef-1234-567890abcdef",
      "error": null
    }
  }
}
```

© 2025 Tanium Inc. All Rights Reserved