ThreatQuotient

Tanium Action Bundle

Version 1.0.0

March 04, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email:	support@threatq.com
Web:	support.threatq.com
Phone:	703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2025 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Tanium Action Bundle enables teams to perform automated actions against Tanium to better secure their environment. The actions included in the bundle can perform automated exports of intelligence to Tanium so that it can be used to improve an organization's security posture and find critical vulnerabilities.

Tanium helps IT teams manage and secure all their devices. It gives a real-time view of everything on the network, allowing teams to identify risks/vulnerabilities, distribute software, and fix problems quickly. Tanium makes it easy for teams to investigate potential issues by allowing them to ask questions about their devices using natural language and take automated actions to address any issues.

The integration provides the following actions:

- **Tanium - Export Hash Reputations -** exports a dynamic list of hashes from ThreatQ to Tanium.
- **Tanium - Delete All Hash Reputations -** deletes hash reputations from your Tanium reputation database.
- **Tanium - Export YARA Rules -** exports a dynamic list of YARA Signatures from ThreatQ to Tanium.
- **Tanium - Get Assets Vulnerable to CVEs -** queries Tanium for vulnerable assets associated with threat intel included in a ThreatQ data collection.

The action is compatible with the following system object types:

- Indicators
    - MD5
    - SHA-1
    - SHA-256
- Signatures
    - YARA
- Vulnerabilities

The action returns the following enriched system objects:

- Assets
- Indicators (CVEs)
- Vulnerabilities

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following object types:
  - MD5, SHA-1, or SHA-256 type Indicator
  - YARA type Signature
  - Vulnerabilities

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine
6. Select the actions to install, when prompted, and click on **Install**.

    > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

7. The action(s) will now be installed on you ThreatQ instance. You will still need to configure the action(s).

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

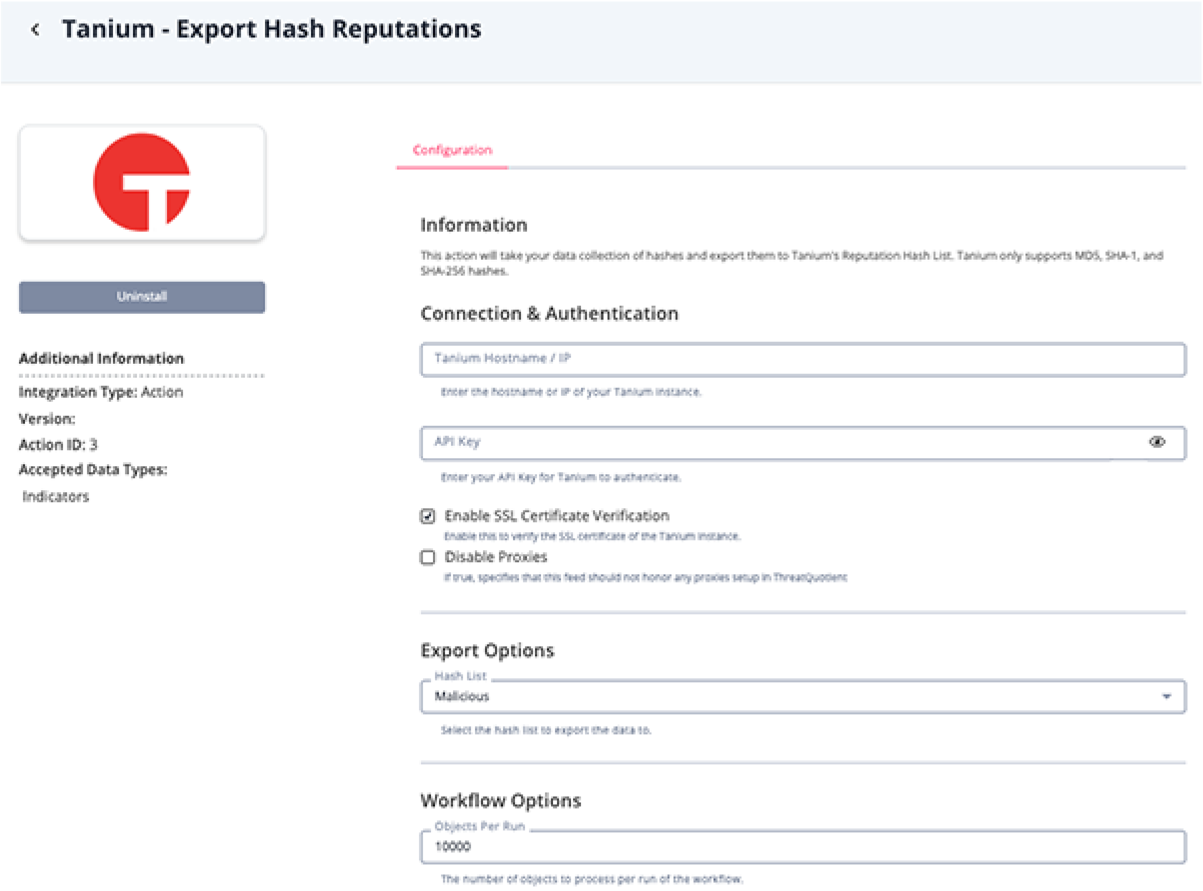
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

Export Hash Reputations Parameters

PARAMETER	DESCRIPTION
Tanium Hostname / IP	The hostname or IP of your Tanium instance.
API Key	Your Tanium API Key.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Hast List	Select the hash list to export. Options include: ◦ Malicious ◦ Non-Malicious
Objects per Run	The number of objects to process per run of the workflow. The default value is 10000.



Tanium - Export Hash Reputations

Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 3

Accepted Data Types:

Indicators

Configuration

Information

This action will take your data collection of hashes and export them to Tanium's Reputation Hash List. Tanium only supports MD5, SHA-1, and SHA-256 hashes.

Connection & Authentication

Tanium Hostname / IP

Enter the hostname or IP of your Tanium instance.

API Key

Enter your API Key for Tanium to authenticate.

☑ Enable SSL Certificate Verification

Enable this to verify the SSL certificate of the Tanium instance.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Export Options

Hash List: Malicious

Select the hash list to export the data to.

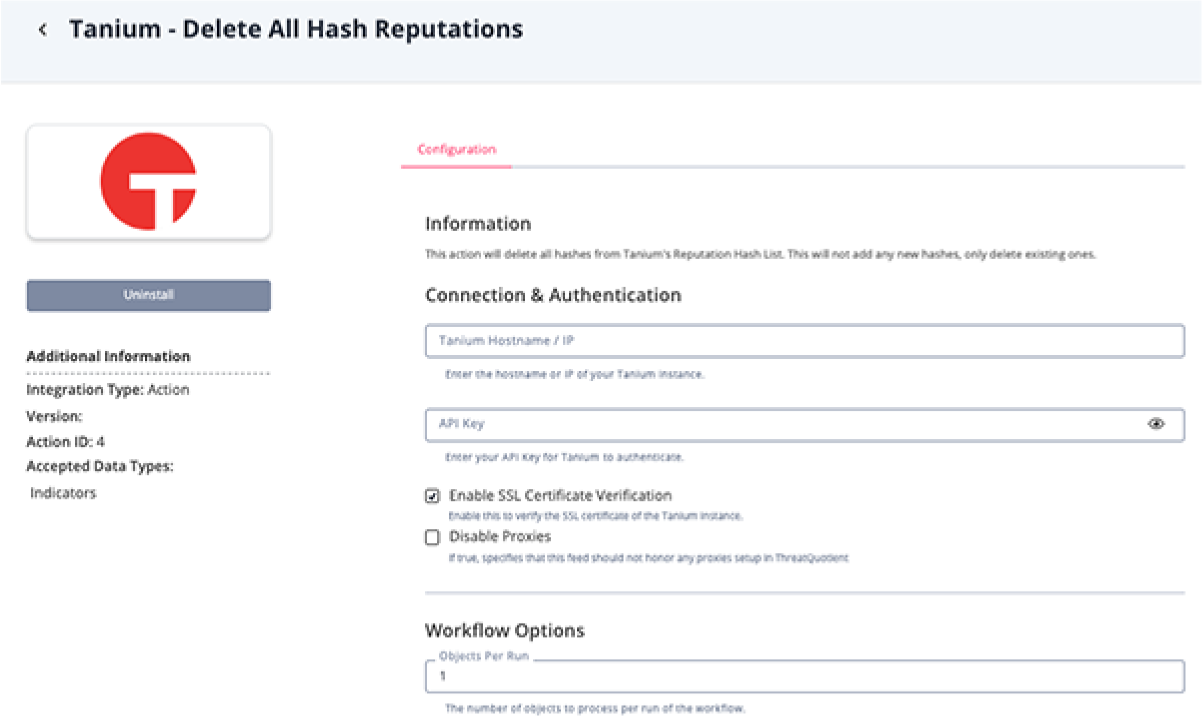
Workflow Options

Objects Per Run: 10000

The number of objects to process per run of the workflow.

Delete All Hash Reputations Parameters

PARAMETER	DESCRIPTION
Tanium Hostname / IP	The hostname or IP of your Tanium instance.
API Key	Your Tanium API Key.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects per Run	The number of objects to process per run of the workflow. The default value is 1.



Tanium - Delete All Hash Reputations

Additional Information

Integration Type: Action
Version:
Action ID: 4
Accepted Data Types:
Indicators

Information

This action will delete all hashes from Tanium's Reputation Hash List. This will not add any new hashes, only delete existing ones.

Connection & Authentication

Tanium Hostname / IP
Enter the hostname or IP of your Tanium instance.

API Key
Enter your API Key for Tanium to authenticate.

☑ Enable SSL Certificate Verification
Enable this to verify the SSL certificate of the Tanium instance.

☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

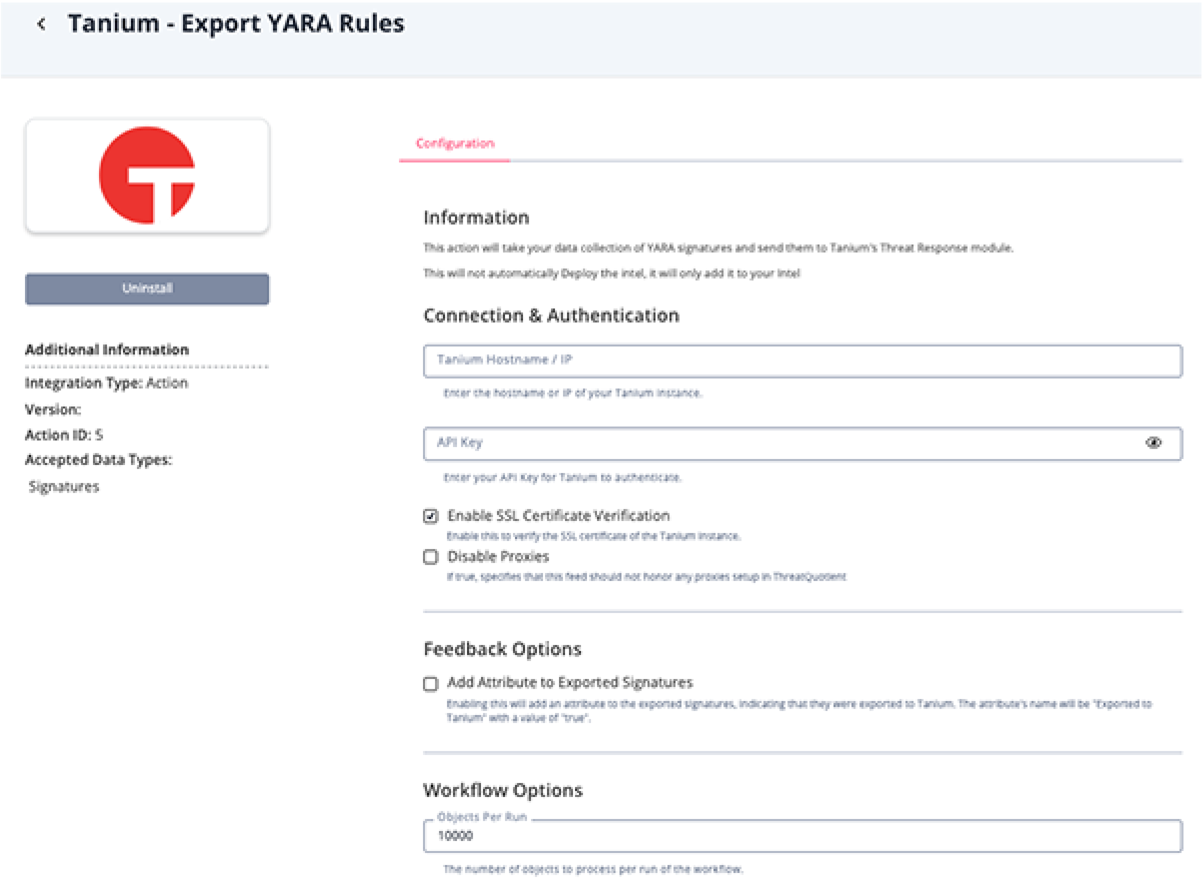
Workflow Options

Objects Per Run: 1
The number of objects to process per run of the workflow.

Export YARA Rules Parameters

PARAMETER	DESCRIPTION
Tanium Hostname / IP	The hostname or IP of your Tanium instance.
API Key	Your Tanium API Key.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Add Attribute To Exported Signatures	Enable this parameter to add an attribute to the exported signatures to indicate that they were exported to Tanium. The attribute's name will be `Exported to Tanium` with a value of `true`. This parameter is disabled by default.

PARAMETER	DESCRIPTION
Objects per Run	The number of objects to process per run of the workflow. The default value is 10000.



‹ **Tanium - Export YARA Rules**

Additional Information

Integration Type: Action
Version:
Action ID: 5
Accepted Data Types:
Signatures

Information

This action will take your data collection of YARA signatures and send them to Tanium's Threat Response module.

This will not automatically Deploy the intel, it will only add it to your Intel

Connection & Authentication

Tanium Hostname / IP

Enter the hostname or IP of your Tanium instance.

API Key

Enter your API Key for Tanium to authenticate.

☑ Enable SSL Certificate Verification

Enable this to verify the SSL certificate of the Tanium instance.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Feedback Options

☐ Add Attribute to Exported Signatures

Enabling this will add an attribute to the exported signatures, indicating that they were exported to Tanium. The attribute's name will be "Exported to Tanium" with a value of "true".

Workflow Options

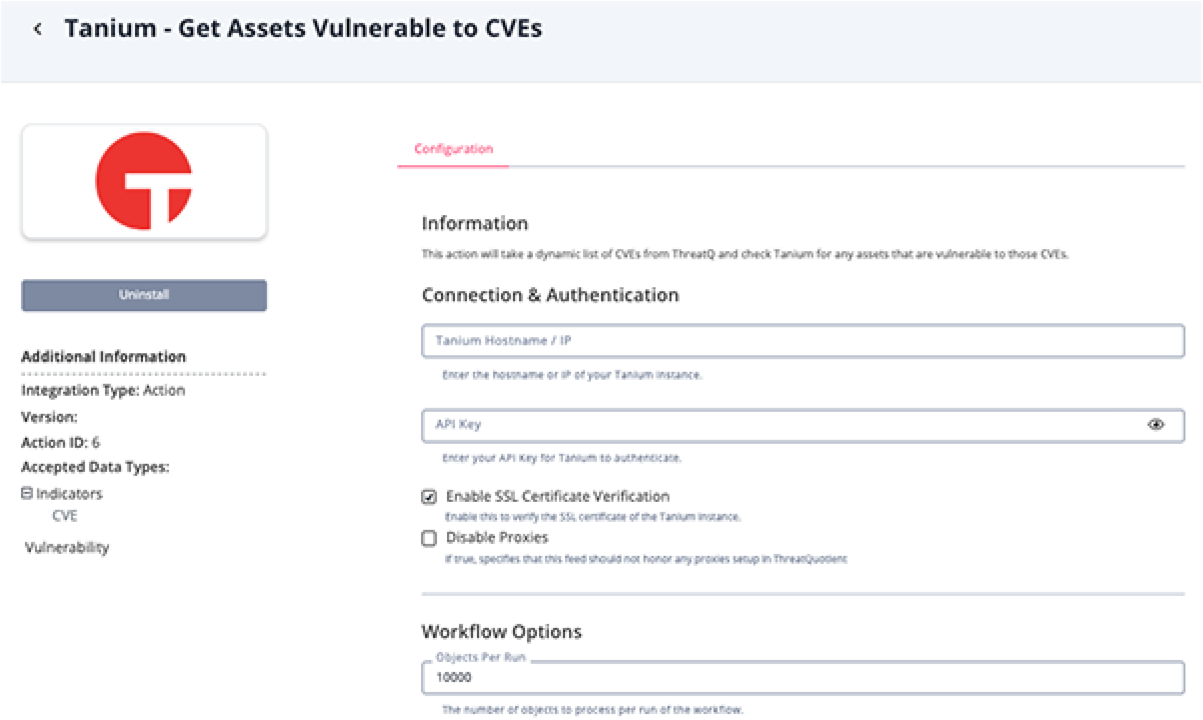
Objects Per Run: 10000

The number of objects to process per run of the workflow.

Get Assets Vulnerable to CVEs Parameters

PARAMETER	DESCRIPTION
Tanium Hostname / IP	The hostname or IP of your Tanium instance.
API Key	Your Tanium API Key.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.

PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects per Run	The number of objects to process per run of the workflow. The default value is 10000.


‹ Tanium - Get Assets Vulnerable to CVEs

Additional Information
Integration Type: Action
Version:
Action ID: 6
Accepted Data Types:
⊟ Indicators
CVE
Vulnerability

Information

This action will take a dynamic list of CVEs from ThreatQ and check Tanium for any assets that are vulnerable to those CVEs.

Connection & Authentication

Tanium Hostname / IP
Enter the hostname or IP of your Tanium instance.

API Key
Enter your API Key for Tanium to authenticate.

☑ Enable SSL Certificate Verification
Enable this to verify the SSL certificate of the Tanium instance.

☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Workflow Options

Objects Per Run: 10000
The number of objects to process per run of the workflow.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Tanium - Export Hash Reputations	The Export Hash Reputation action will export hashes to your Tanium Reputation database	Indicators	MD5, SHA-1, SHA-256
Tanium - Delete All Hash Reputations	The Delete All Hashes action will clear all hashes from Tanium's Reputation database	Indicators	All
Tanium - Export YARA Rules	The Export YARA Rules action will export YARA rules to your Tanium Intel database	Signatures	YARA
Tanium - Get Assets Vulnerable to CVEs	The Get Assets Vulnerable to CVEs action will query Tanium for assets being affected by selected vulnerabilities	Vulnerabilities, Indicators	Indicators - CVE

Export Hash Reputations

The Export Hash Reputations action will export a dynamic list of hashes to Tanium's Reputation database. This will allow Tanium to use this intelligence to detect suspicious or malicious files on the registered devices. Each hash will include a note containing the indicator's score, tags, description, and other relevant information.

> There is no mapping for this action as no enriched data is returned.

Delete All Hash Reputations

The Delete Hash Reputations action will delete all hash reputations from your Tanium reputation database regardless of the data collection it uses or number of objects per run. This is useful if you want to clear out all the hashes that have been exported to Tanium, before re-building the database with new hashes.

> There is no mapping for this action as no enriched data is returned.

Export YARA Rules

The Export YARA Rules action will export a dynamic list of YARA signatures from ThreatQ to Tanium's Intel database. Once the YARA signatures are in Tanium, you'll be able to deploy them to facilitate the detection of malicious files on your devices.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Attribute	Exported to Tanium	N/A	`true`	If the user field `Add Attribute to Exported Signatures` is enabled.

Get Assets Vulnerable to CVEs

The Get Assets Vulnerable to CVEs action will query Tanium for assets that are vulnerable to the selected data collection of CVEs. This will allow you to identify assets that are at risk to prioritized CVEs and take action to remediate the vulnerabilities.

Sample Request:

```
{
   "query": "query vulnerableAssetsByCVE($cveId: String!, $first: Int!) {\r\n
endpoints(first: $first) {\r\n    edges {\r\n      node {\r\n        id\r\n
name\r\n        eidFirstSeen\r\n        eidLastSeen\r\n        ipAddress\r\n
macAddresses\r\n        compliance {\r\n          cveFindings(filter: { path:
\"cveId\", op: MATCHES, value: $cveId }) {\r\n
absoluteFirstFoundDate\r\n            affectedProducts\r\n
cisaNotes\r\n            cisaProduct\r\n            cisaRequiredAction\r\n
cisaShortDescription\r\n            cisaVendor\r\n
cisaVulnerabilityName\r\n            cpes\r\n            cveId\r\n
cvssScoreV3\r\n            isCisaKev\r\n            severityV3\r\n
summary\r\n          }\r\n        }\r\n      }\r\n    }\r\n    pageInfo {\r\n
startCursor\r\n      endCursor\r\n      hasPreviousPage\r\n
hasNextPage\r\n    }\r\n  }\r\n}\", \"variables\": { \"first\": 500, \"cveId\":
\"CVE-2020-8623\" }"
}
```

Sample Response:

```
{
    "data": {
        "endpoints": {
            "edges": [
                {
                    "node": {
                        "id": "1002",
                        "name": "falks-imac.gubisrath.local",
                        "eidFirstSeen": "2024-03-04T09:29:39Z",
                        "eidLastSeen": "2024-03-13T17:39:12Z",
                        "ipAddress": "192.168.42.72",
                        "macAddresses": [
                            "18:31:bf:30:0d:51"
                        ],
                        "compliance": {
                            "cveFindings": [
                                {
                                    "absoluteFirstFoundDate": "2024-03-12",
                                    "affectedProducts": [
                                        "libssh",
                                        "podman-tui",
                                        "proftpd"
                                    ],
                                    "cisaDateAdded": null,
                                    "cisaDueDate": null,
                                    "cisaNotes": "",
                                    "cisaProduct": "",
                                    "cisaRequiredAction": "",
                                    "cisaShortDescription": "",
                                    "cisaVendor": "",
                                    "cisaVulnerabilityName": "",
                                    "cpes": [
                                        "cpe:/a:openbsd:openssh",
                                        "cpe:/a:putty:putty"
                                    ],
                                    "cveId": "CVE-2023-48795",
                                    "cveYear": "2023",
                                    "cvssScoreV3": 5.9,
                                    "excepted": false,
                                    "firstFound": "2024-03-12",
                                    "isCisaKev": false,
                                    "lastFound": "2024-03-12",
                                    "lastScanDate": "2024-03-12",
                                    "scanType": "oval",
                                    "severityV3": "Medium",
                                    "summary": "The SSH transport protocol with
certain OpenSSH extensions, found in OpenSSH before 9.6 and other products,
allows remote attackers to bypass integrity checks such that some packets are
omitted (from the extension negotiation message), and a client and server may
consequently end up with a connection for which some security features have
been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH
Binary Packet Protocol (BPP), implemented by these extensions, mishandles the
handshake phase and mishandles use of sequence numbers. For example, there is
an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with
Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if
CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick
Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh
before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2,
golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through
1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko
before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus
through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,
ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4,
NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH
library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0,
TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig,
FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT
before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta,
WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before
9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2
module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust,
and the Russh crate before 0.40.2 for Rust."
                                }
```

```
                            ]
                        }
                    }
                }
            ],
            "pageInfo": {
                "startCursor": "MzM5NTU4OjA=",
                "endCursor": "MzM5NTU4OjI=",
                "hasPreviousPage": false,
                "hasNextPage": false
            }
        }
    }
}
```

ThreatQuotient provides the following default mapping for this action based on each item with the `data.endpoints.edges[].node` array returned by the Tanium API:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.name`	Asset Value	N/A	`.eidLastSeen`	`falks-imac.gubisrath.local`	N/A
`.id`	Asset Attribute	Tanium Endpoint ID	`.eidLastSeen`	`1002`	N/A
`.eidLastSeen`	Asset Attribute	Last Seen	`.eidLastSeen`	`2024-03-13T17:39:12Z`	Updatable
`.macAddresses[]`	Asset Attribute	MAC Address	`.eidLastSeen`	`18:31:bf:30:0d:51`	Updatable
`.ipAddress`	Asset Attribute	IP Address	`.eidLastSeen`	`192.168.42.72`	Updatable
`.compliance.cveFindings[].affectedProducts`	Indicator/ Vulnerability Attribute	Affected Product	`.compliance.cveFindings[].absoluteFirstFoundDate`	`libssh`	N/A
`.compliance.cveFindings[].cisaProduct`	Indicator/ Vulnerability Attribute	Affected Product	`.compliance.cveFindings[].absoluteFirstFoundDate`	N/A	N/A
`.compliance.cveFindings[].cisaVendor`	Indicator/ Vulnerability Attribute	Affected Vendor	`.compliance.cveFindings[].absoluteFirstFoundDate`	N/A	N/A
`.compliance.cveFindings[].cisaVulnerabilityName`	Indicator/ Vulnerability Attribute	Vulnerability Name	`.compliance.cveFindings[].absoluteFirstFoundDate`	N/A	N/A
`.compliance.cveFindings[].isCisaKev`	Indicator/ Vulnerability Attribute	Is CISA KEV	`.compliance.cveFindings[].absoluteFirstFoundDate`	`false`	N/A
`.compliance.cveFindings[].isCisaKev`	Indicator/ Vulnerability Tag	N/A	N/A	N/A	If `.compliance.cveFindings[].isCisaKev` is True, `exploited` tag

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					will be ingested for this object
`.compliance.cveFindings[].cvssScoreV3`	Indicator/ Vulnerability Attribute	CVSSv3 Base Score	`.compliance.cveFindings[].absoluteFirstFoundDate`	`5.9`	Updatable
`.compliance.cveFindings[].severityV3`	Indicator/ Vulnerability Attribute	CVSSv3 Severity	`.compliance.cveFindings[].absoluteFirstFoundDate`	`MEDIUM`	Updatable
`.compliance.cveFindings[].summary`, `.compliance.cveFindings[].cisaShortDescription`, `.compliance.cveFindings[].cisaRequiredAction`, `.compliance.cveFindings[].cisaNotes`, `.compliance.cveFindings[].cpes[]`	Indicator/ Vulnerability Description	N/A	N/A	`The SSH transport protocol with certain OpenSSH extensions...`	Fields concatenated into HTML

Enriched Data

> Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

Export YARA Rules

METRIC	RESULT
Run Time	1 minute
Signatures	125
Signatures Attributes	125

Get Assets Vulnerable to CVEs

METRIC	RESULT
Run Time	1 minute
Assets	2
Asset Attributes	8
Vulnerabilities	10
Vulnerability Attributes	80

Known Issues / Limitations

- **Tanium - Export Hash Reputations -** the action will only update the notes of a hash if it already exists in Tanium's Reputation database, but it will not modify its existing type (Malicious or Non-Malicious).
- **Tanium - Export YARA Rules -** the action might log Bad Request errors if the exported YARA is not validated by Tanium.

Change Log

- **Version 1.0.0**
    - Initial release