ThreatQuotient

The Hive Action User Guide

Version 1.1.1

December 18, 2023

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.

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	1.1.0
Compatible with ThreatQ Versions	>= 5.20.0
Compatible with Hive Versions	4.x, 5.1.x, >=5.2.x
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Hive Action enables a user to create cases in The Hive with ThreatQ indicators attached as case observables.

The integration provides the following action:

- **The Hive Create Case** - Creates cases and observables in The Hive based on ThreatQ objects. For each object an observable will be attached to the created case.

The action is compatible with the following object types:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Course of Actions
- Exploit of Targets
- Identities
- Indicators
    - ASN
    - IP Address
    - IPv6 Address
    - CIDR Block
    - MD5
    - SHA-1
    - SHA-256
    - SHA-384
    - SHA-512
    - URL
    - FQDN
    - Filename
    - Email Address
    - Email Subject
- Intrusion Sets
- Malware
- Reports
- Tools
- TTPs
- Vulnerabilities

The action returns the following enriched system objects:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Course of Actions
- Exploit of Targets

- Identities
- Indicators
- Intrusion Sets
- Malware
- Reports
- Tools
- TTPs
- 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:
  - Adversaries
  - Assets
  - Attack Patterns
  - Campaigns
  - Course of Actions
  - Exploit of Targets
  - Identities
  - Indicators
    - ASN
    - IP Address
    - IPv6 Address
    - CIDR Block
    - MD5
    - SHA-1
    - SHA-256
    - SHA-384
    - SHA-512
    - URL
    - FQDN
    - Filename
    - Email Address
    - Email Subject
  - Intrusion Sets
  - Malware
  - Reports
  - Tools
  - TTPs
  - Vulnerabilities
- The Hive API Key with the following permissions:
  - ManageCase/create
  - ManageObservable
  - ManageTag
- The following observable types must exist in The Hive: autonomous-system, ip, hash, url, fqdn, filename, mail, mail-subject.
  - To add or update observable types login as an administrator and go to {{THE_HIVE_URL}}/administration/entities/observables)
  - The ThreatQ indicators are uploaded to The Hive according to the mapping table presented in the Actions section of this guide.

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

> 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.

You will still need to configure the action.

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:

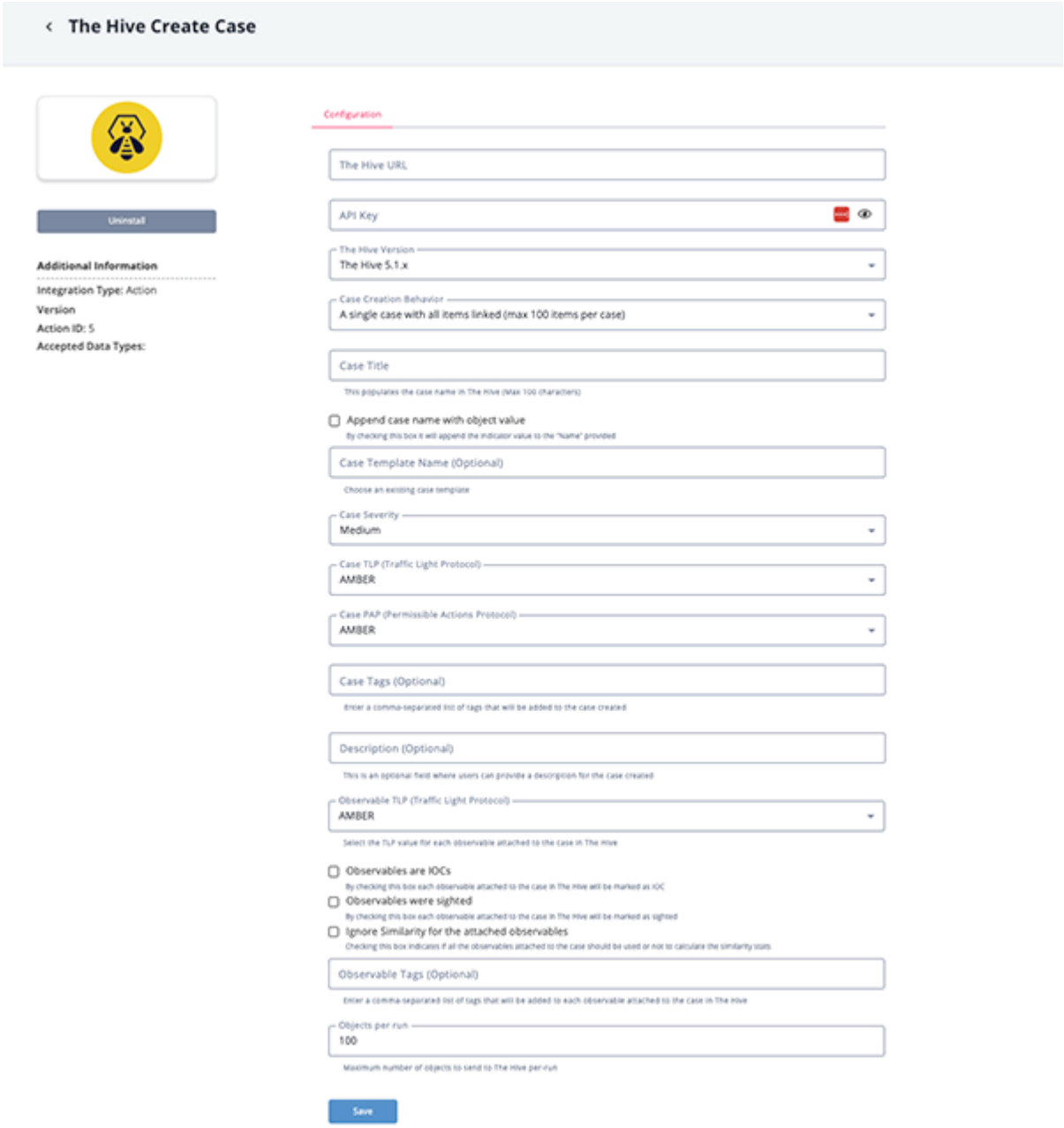
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

PARAMETER	DESCRIPTION
The Hive URL	The URL for your The Hive instance.
API Key	Your The Hive API Key.
The Hive Version	Select your version of The Hive. Options include: ◦ The Hive 5.2.x (default) ◦ The Hive 5.1.x ◦ The Hive 4.x
Case Creation Behavior	Select the case creation behavior. Options include: ◦ A single case with all items linked (default). The maximum is 100 items per case. ◦ Individual Cases per item
Case Title	This populates the case name in The Hive. Maximum length is 100 characters.
Append case name with object value	Enabling this parameter it will append the indicator value to the case name provided.

PARAMETER	DESCRIPTION
	Total length must be less than 400 characters.
Case Template Name (Optional)	Enter an existing case template from The Hive.
Case Severity	Select the severity for the new case. Options include: ◦ Low ◦ Medium (default) ◦ High ◦ Critical
Case TLP (Traffic Light Protocol)	Select the TLP value for the new case. Options include: ◦ White ◦ Green ◦ Amber (default) ◦ Amber+Strict ◦ Red
Case PAP (Permissible Actions Protocol)	Select the PAP value for the new case. Options include: ◦ White ◦ Green ◦ Amber (default) ◦ Red
Case Tags (Optional)	Enter a comma-separated list of tags that will be added to the case created.
Description (Optional)	This is an optional field where users can provide a description for the case created.
Observable TLP (Traffic Light Protocol)	Select the TLP value for each observable attached to the case in The Hive. Options include: ◦ White ◦ Green ◦ Amber (default) ◦ Amber+Strict ◦ Red

PARAMETER	DESCRIPTION
Observables are IOCs	Enabling this parameter with result in each observable attached to the case in The Hive to be marked as IOC.
Observables were sighted	Enabling this parameter will result in each observable attached to the case in The Hive to be marked as Sighted.
Ignore Similarity for the attached observables	Enabling this parameter will result in all observables attached to the case being used to calculate the similarity stats.
Observable Tags	Optional - enter a comma-separated list of tags that will be added to each observable attached to the case in The Hive.
Objects per run	Maximum number of objects to send to The Hive per-run.



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

Actions

The integration provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
The Hive Create Case	Creates case and observables in The Hive based on TQ objects.	Adversaries, Assets, Attack Patterns, Campaigns, Course of Actions, Exploit of Targets, Identities, Indicators, Intrusion Sets, Malware, Reports, Tools, TTPs, Vulnerabilities	Indicator Types: ASN, IP Address, IPv6 Address, CIDR Block, MD5, SHA-1, SHA-256, SHA-384, SHA-512, URL, FQDN, Filename, Email Address, Email Subject

The Hive Create Case

The Hive Create Case action creates cases in The Hive based on TQ objects. For each object an observable will be created in The Hive and attached to the newly created case.

`POST {{THE_HIVE_URL}}/api/v1/case`

Sample Request:

```
{
  "title": "Block IPs: 1.2.3.4, 1.2.3.5",
  "description": "Case generated using ThreatQ Platform.",
  "tlp": 2,
  "pap": 2,
  "severity": 3,
  "tags": [
    "malicious_traffic"
  ]
}
```

Sample Response:

```
{
  "_id": "~23423",
  "_type": "Case",
  "_createdBy": "username@org",
  "_createdAt": 1695642985743,
  "title": "Block IP: 1.2.3.4",
  "description": "Case generated using ThreatQ Platform.",
  "severity": 3,
  "tlp": 2,
  "pap": 2,
  "number": 22,
  "startDate": 1695642985743,
  "tags": [
    "malicious_traffic"
  ],
  "status": "Open",
  "assignee": "username@org",
  "flag": false,
  "tasks": [],
  "customFields": {}
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
_id	Indicator.Attribute	The Hive Case URL	N/A	{{THE_HIVE_URL}}/cases/~23423/details	N/A
number	Indicator.Attribute	The Hive Case Number	N/A	22	N/A

Severity Mapping

THE HIVE ID	THREATQ ATTRIBUTE VALUE
1	Low
2	Medium
3	High
2	Critical

TLP (Traffic Light Protocol) Mapping (4.x, 5.1x)

The Hive 4.x and 5.1.x do not support TLP 2.0.

THE HIVE ID	THREATQ TLP VALUE
0	WHITE
1	GREEN
2	AMBER
2	AMBER+STRICT
3	RED

TLP (Traffic Light Protocol) Mapping (5.2x)

The Hive v5.2 and later supports TLP 2.0.

THE HIVE ID	THREATQ TLP VALUE
0	WHITE

THE HIVE ID	THREATQ TLP VALUE
1	GREEN
2	AMBER
3	AMBER+STRICT
4	RED

PAP (Permissible Actions Protocol) Mapping

The Hive 4.x and 5.1.x do not support TLP 2.0.

THE HIVE ID	THREATQ TLP VALUE
0	WHITE
1	GREEN
2	AMBER
3	RED

The Hive Add Observable To Case (supplemental)

The Hive Add Observable to Case supplemental function adds the indicators from the ThreatQ collection as observables to the newly created case.

```
POST {{THE_HIVE_URL}}/api/v1/case/{{CASE_ID}}/observable
```

Sample Request:

```
{
  "dataType": "ip",
  "data": "1.2.3.4",
  "tlp": 2,
  "ioc": false,
  "sighted": false,
  "ignoreSimilarity": false,
  "tags": [
    "ddos"
  ]
}
```

Sample Response:

```
{
  "_createdAt": 1695649235959,
  "_createdBy": "username@org",
  "_id": "~327692408",
  "_type": "Observable",
  "data": "1.2.3.4",
  "dataType": "ip",
  "extraData": {},
  "ioc": false,
  "reports": {},
  "sighted": false,
  "startDate": 1695649235959,
  "tags": [
    "ddos"
  ],
  "tlp": 2
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
_id	Indicator.Attribute	The Hive Observable URL	N/A	{{THE_HIVE_URL}}/cases/{{CASE_ID}}/observables/~327692408	N/A

Object Type Mapping

THE HIVE TYPE	THREATQ OBJECT TYPE
other	Adversary
other	Asset
other	Attack Pattern
other	Campaign
other	Course of Action
other	Exploit Target
user-agent	Identity
See Indicator Mapping Table	Indicator
other	Intrusion Set
other	Malware
other	Report
other	Tool
other	TTP
other	Vulnerability

Indicator Mapping

The Hive to ThreatQ indicator mapping is as follows:

THE HIVE TYPE	THREATQ INDICATOR TYPE
autonomous-system	ASN
ip	IP Address
ip	IPv6 Address
ip	CIDR Block
hash	MD5
hash	SHA-1
hash	SHA-256
hash	SHA-512
hash	SHA-384
fqdn	FQDN
url	URL
mail	Email Address
mail-subject	Email Subject
filename	Filename

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.

METRIC	RESULT
Run Time	24 minutes
Indicators	100
Indicator Attributes	300
Adversaries	100
Adversary Attributes	300
Asset	100
Asset Attributes	300
Attack Patterns	100
Attack Pattern Attributes	300
Campaigns	100
Campaign Attributes	300
Course of Action	100
Course of Action Attributes	300

METRIC	RESULT
Exploit Targets	100
Exploit Target Attributes	300
Identities	100
Identity Attributes	300
Intrusion Sets	100
Intrusion Set Attributes	300
Malware	100
Malware Attributes	300
Reports	100
Report Attributes	300
Tools	100
Tool Attributes	300
TTP	100
TTP Attributes	300
Vulnerabilities	100
Vulnerability Attributes	300

Known Issues / Limitations

- The option **Append case name with object value** appends the value of the objects only if their total length is less than 400 characters.

Change Log

- **Version 1.1.1**
  - Added support for The Hive v5.2.x which includes support for TLP 2.0.
- **Version 1.1.0**
  - Added support for the following object types: Adversary, Asset, Attack Pattern, Campaign, Course of Action, Exploit Target, Identity, Intrusion Set, Malware, Report, Tool, TTP, and Vulnerability.
  - Updated minimum ThreatQ version to 5.20.0.
- **Version 1.0.0**
  - Initial release