

ThreatQuotient



SentinelOne Operation Guide

Version 1.1.1

October 31, 2022

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

Integration Details	5
Introduction	6
Installation	7
Configuration	8
Actions	9
Get Reputation	10
Blacklist	11
Add Exclusion	12
Query Incidents	13
Threats	13
Notes	17
Mitigate Threat	18
Create Firewall Rule	19
Check Endpoints	20
Hunt	21
Change Log	22

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 © 2022 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	1.1.1
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https:// marketplace.threatq.com/ details/sentinelone- operation

Introduction

The SentinelOne Operation for ThreatQuotient enables a user to interact with SentinelOne and decrease the time-to-mitigation for a given threat.

The operation provides the following actions:

- **Get Reputation** - gets a reputation for a given SHA-1 hash.
- **Blacklist** - blacklists a given SHA-1 hash.
- **Add Exclusion** - excludes a given SHA-1 hash.
- **Query Incidents** - fetches incidents/threats related to the given object.
- **Mitigate Threat** - apply a mitigation action to threats that match a given object.
- **Create Firewall Rule** - creates a firewall rule to allow or block a given host.
- **Check Endpoints** - checks to see if a CVE affects any applications installed on an endpoint.
- **Hunt** - generates a link to directly hunt an IOC in SentinelOne.

The operation is compatible with the following indicator types:

- SHA-1
- SHA-256
- MD5
- IP Address
- FQDN
- CIDR Block
- CVE

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 integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



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

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Hostname	Your SentinelOne Hostname.
API Token	Your SentinelOne API Token. You can find this token by logging into SentinelOne and navigating to the My User section.
Sites	A comma-separated list of site names to interact with.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Get Reputation	Gets a reputation for a given SHA-1 hash.	Indicators	SHA-1
Blacklist	Blacklists a given SHA-1 hash.	Indicators	SHA-1
Add Exclusion	Excludes a given SHA-1 hash.	Indicators	SHA-1
Query Incidents	Fetches incidents/threats related to the given object.	Indicators	SHA-1, MD5, SHA-256, File Path
Mitigate Threat	Apply a mitigation action to threats that match a given object.	Indicators	SHA-1, MD5, SHA-256, File Path
Create Firewall Rule	Creates a firewall rule to allow or block a given host.	Indicators	IP Address, FQDN, CIDR Block
Check Endpoints	Checks to see if a CVE affects any applications installed on an endpoint.	Indicators	CVE
Hunt	Generates a link to directly hunt an IOC in SentinelOne.	Indicators	SHA-1, MD5, SHA-256, File Path

Get Reputation

The Get Reputation action gets a reputation for a given SHA-1 hash.

GET https://{hostname}/web/api/v2.1/hashes/{sha1}/reputation

Sample Response:

```
{
  "data": {
    "rank": "5"
  }
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.data.rank	Indicator.Attribute	Rank	5

Blacklist

The Blacklist action blacklists a given SHA-1 hash.

POST `https://{hostname}/web/api/v2.1/restrictions`

This Action has the following Configuration options:

OPTION	DESCRIPTION
Operating Systems	The operating systems you want this blacklisted on.
Custom Description	Description for the blacklisted hash.

This Action contains no data mapping.

Add Exclusion

Excludes a given SHA-1 hash.

POST `https://{hostname}/web/api/v2.1/exclusions`

This Action has the following Configuration options:

OPTION	DESCRIPTION
Operating Systems	The operating systems you want this excluded on.
Custom Description	Description for the excluded hash.

This Action contains no data mapping.

Query Incidents

Fetches incidents/threats related to the given object. ThreatQuotient provides mapping for [Threats](#) and [Notes](#).

Threats

GET `https://{hostname}/web/api/v2.1/threats`

Sample Response:

```
{
  "agentDetectionInfo": {
    "accountId": "433241117337583618",
    "accountName": "SentinelOne",
    "agentDomain": "WORKGROUP",
    "agentIPv4": "192.168.104.136",
    "agentIPv6": "fe80::3860:a370:ae18:eb99",
    "agentLastLoggedInUserName": "IEUser",
    "agentMitigationMode": "protect",
    "agentOsName": "Windows 7",
    "agentOsRevision": "7601 SP1",
    "agentRegisteredAt": "2020-10-07T16:10:57.714972Z",
    "agentUuid": "d71b5dba05244409b9ba79eb55858370",
    "agentVersion": "3.1.4.50",
    "externalIp": "73.191.116.179",
    "groupId": "991892612147246915",
    "groupName": "Default Group",
    "siteId": "991892612138858306",
    "siteName": "Threat Quotient"
  },
  "agentRealtimeInfo": {
    "accountId": "433241117337583618",
    "accountName": "SentinelOne",
    "activeThreats": 0,
    "agentComputerName": "IEWIN7",
    "agentDecommissionedAt": true,
    "agentDomain": "WORKGROUP",
    "agentId": "997055331565582336",
    "agentInfected": false,
    "agentIsActive": false,
    "agentIsDecommissioned": true,
    "agentMachineType": "desktop",
    "agentMitigationMode": "protect",
    "agentNetworkStatus": "connected",
    "agentOsName": "Windows 7",
    "agentOsRevision": "7601 SP1",
    "agentOsType": "windows",
    "agentUuid": "d71b5dba05244409b9ba79eb55858370",
    "agentVersion": "3.1.4.50",
    "groupId": "991892612147246915",
    "groupName": "Default Group",
    "networkInterfaces": [
      {
```

```
    "id": "997055331565582337",
    "inet": [
      "192.168.104.149"
    ],
    "inet6": [
      "fe80::3860:a370:ae18:eb99"
    ],
    "name": "Local Area Connection 2",
    "physical": "00:0c:29:db:63:a7"
  }
],
"operationalState": "na",
"rebootRequired": false,
"scanAbortedAt": null,
"scanFinishedAt": "2020-10-15T19:36:33.252873Z",
"scanStartedAt": "2020-10-07T16:12:27.439966Z",
"scanStatus": "finished",
"siteId": "991892612138858306",
"siteName": "Threat Quotient",
"storageName": null,
"storageType": null,
"userActionsNeeded": []
},
"containerInfo": {
  "id": null,
  "image": null,
  "labels": null,
  "name": null
},
"id": "997073615157480015",
"indicators": [],
"kubernetesInfo": {
  "cluster": null,
  "controllerKind": null,
  "controllerLabels": null,
  "controllerName": null,
  "namespace": null,
  "namespaceLabels": null,
  "node": null,
  "pod": null,
  "podLabels": null
},
"mitigationStatus": [
  {
    "action": "quarantine",
    "actionsCounters": null,
    "agentSupportsReport": false,
    "groupNotFound": false,
    "lastUpdate": "2020-10-07T16:47:17.557790Z",
    "latestReport": null,
    "mitigationEndedAt": null,
    "mitigationStartedAt": null,
    "status": "success"
  },
  {
    "action": "kill",
    "actionsCounters": null,
    "agentSupportsReport": false,
    "groupNotFound": false,
    "lastUpdate": "2020-10-07T16:47:17.435805Z",
    "latestReport": null,
```

```

        "mitigationEndedAt": null,
        "mitigationStartedAt": null,
        "status": "success"
    }
},
"threatInfo": {
    "analystVerdict": "true_positive",
    "analystVerdictDescription": "True positive",
    "automaticallyResolved": true,
    "browserType": null,
    "certificateId": "",
    "classification": "Malware",
    "classificationSource": "Static",
    "cloudFilesHashVerdict": "black",
    "collectionId": "433377870883088367",
    "confidenceLevel": "malicious",
    "createdAt": "2020-10-07T16:47:17.291955Z",
    "detectionEngines": [
        {
            "key": "sentinelone_cloud",
            "title": "SentinelOne Cloud"
        }
    ],
    "detectionType": null,
    "engines": [
        "SentinelOne Cloud"
    ],
    "externalTicketExists": false,
    "externalTicketId": null,
    "failedActions": false,
    "fileExtension": ".COM",
    "fileExtensionType": "Executable",
    "filePath": "\\Device\\HarddiskVolume1\\ProgramData\\Microsoft\\Windows Defender\\LocalCopy\\
\\{85788613-96DC-4825-8C8B-EF33773578C5}-eicar.com",
    "fileSize": 0,
    "fileVerificationType": "NotSigned",
    "identifiedAt": "2020-10-07T16:47:17.165000Z",
    "incidentStatus": "resolved",
    "incidentStatusDescription": "Resolved",
    "initiatedBy": "agent_policy",
    "initiatedByDescription": "Agent Policy",
    "initiatingUserId": null,
    "initiatingUsername": null,
    "isFileless": false,
    "isValidCertificate": false,
    "maliciousProcessArguments": null,
    "md5": null,
    "mitigatedPreemptively": false,
    "mitigationStatus": "Mitigated",
    "mitigationStatusDescription": "Mitigated",
    "originatorProcess": null,
    "pendingActions": false,
    "processUser": "",
    "publisherName": "",
    "reachedEventsLimit": false,
    "rebootRequired": false,
    "sha1": "3395856ce81f2b7382dee72602f798b642f14140",
    "sha256": null,
    "storyline": "EB3E27295CBE7F6E",
    "threatId": "997073615157480015",
    "threatName": "{85788613-96DC-4825-8C8B-EF33773578C5}-eicar.com",

```

```

    "updatedAt": "2020-11-27T00:03:57.033276Z"
  },
  "whiteningOptions": [
    "hash"
  ]
}

```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.agentRealtimeInfo.agentComputerName	Indicator.Attribute	Agent Computer Name	IEWIN7
.agentRealtimeInfo.agentDomain	Indicator.Attribute	Agent Domain	WORKGROUP
.agentRealtimeInfo.agentMachineType	Indicator.Attribute	Agent Machine Type	desktop
.agentRealtimeInfo.agentIsInfected	Indicator.Attribute	Agent Is Infected	False
.agentRealtimeInfo.agentIsActive	Indicator.Attribute	Agent Is Active	False
.agentRealtimeInfo.agentIsDecommissioned	Indicator.Attribute	Is Decommissioned	True
.agentRealtimeInfo.agentMitigationMode	Indicator.Attribute	Mitigation Mode	protect
.agentRealtimeInfo.agentNetworkStatus	Indicator.Attribute	Agent Network Status	connected
.agentRealtimeInfo.agentOsName	Indicator.Attribute	Agent Operating System	Windows 7
.agentRealtimeInfo.siteName	Indicator.Attribute	Site Name	Threat Quotient
.threatInfo.classification	Indicator.Attribute	Classification	Malware
.threatInfo.confidenceLevel	Indicator.Attribute	Confidence Level	malicious
.threatInfo.engines[]	Indicator.Attribute	Engine	SentinelOne Cloud
.threatInfo.incidentStatusDescription	Indicator.Attribute	Incident Status	Resolved
.threatInfo.initiatedByDescription	Indicator.Attribute	Initiated By	Agent Policy
.threatInfo.mitigatedPreemptively	Indicator.Attribute	Mitigated Preemptively	False
.threatInfo.mitigationStatusDescription	Indicator.Attribute	Mitigation Status	Mitigated
.threatInfo.threatName	Indicator.Attribute	Threat Name	{85788613-96DC-4825-8C8B-EF33773578C5}-eicar.com
.threatInfo.detectionType	Indicator.Attribute	Detection Type	N/A
.threatInfo.fileVerificationType	Indicator.Attribute	Signature Verification	NotSigned
.threatInfo.analystVerdictDescription	Indicator.Attribute	Analyst Verdict	True positive
.threatInfo.cloudFilesHashVerdict	Indicator.Attribute	Cloud Verdict	black
.threatInfo.fileExtension	Indicator.Attribute	File Extension	COM
.threatInfo.fileExtensionType	Indicator.Attribute	File Type	Executable
.threatInfo.md5	Related Indicator.Value	MD5	N/A
.threatInfo.sha1	Related Indicator.Value	SHA-1	3395856ce81f2b7382dee72602f798b642f14140
.threatInfo.sha256	Related Indicator.Value	SHA-256	N/A

Notes

GET `https://{hostname}/web/api/v2.1/threats/{threat_id}/notes`

Sample Response:

```
{
  "data": [
    {
      "edited": "boolean",
      "text": "Discovered using analysis",
      "id": "225494730938493804",
      "creator": "John Doe",
      "updatedAt": "2018-02-27T04:49:26.257525Z",
      "createdAt": "2018-02-27T04:49:26.257525Z",
      "creatorId": "225494730938493804"
    }
  ]
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.data[].text	Indicator.Attribute	Analyst Note	Discovered using analysis

Mitigate Threat

The Mitigate Threat action applies a mitigation action to threats that match a given object.

POST `https://{hostname}/web/api/v2.1/threats/mitigate/{ioc}`

This Action has the following Configuration option:

OPTION	DESCRIPTION
Mitigation Action	The mitigation action to take on a given threat.

Action contains no data mapping.

Create Firewall Rule

The Create Firewall Rule creates a firewall rule to allow or block a given host.

POST `https://{hostname}/web/api/v2.1/firewall-control`

This Action has the following Configuration options:

OPTION	DESCRIPTION
Rule Name	The Name for this Firewall rule.
Description	The Description for this rule.
Site	Site name within to create the rule.
Action	The Action to take.
Operating Systems	One or more operating systems for this rule to apply to.
Direction	The Direction to apply this rule.
Enabled	Enable the rule immediately.

This Action contains no data mapping.

Check Endpoints

The Check Endpoints action checks to see if a CVE affects any applications installed on an endpoint.

GET `https://{hostname}/web/api/v2.1/installed-applications/cves`

Sample Response:

```
{
  "data": [
    {
      "score": "8.4",
      "cveId": "CVE-2018-3204",
      "link": "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3204",
      "publishedAt": "string",
      "id": "225494730938493804",
      "updatedAt": "2018-02-27T04:49:26.257525Z",
      "createdAt": "2018-02-27T04:49:26.257525Z",
      "riskLevel": "none",
      "description": "Vulnerability in the Oracle Business Intelligence Enterprise Edition"
    }
  ]
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.data[].description	Indicator.Attribute	Description	Vulnerability in the Oracle...
.data[].link	Indicator.Attribute	Reference	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3204
.data[].riskLevel	Indicator.Attribute	Risk Level	none
.data[].score	Indicator.Attribute	Score	8.4

Hunt

The Hunt action generates a link to directly hunt an IOC in SentinelOne.

There are no requests sent to SentinelOne for this action.

Action contains no data mapping.

Change Log

- **Version 1.1.1**
 - Added improved error handling to resolve ambiguous `BAD REQUEST` errors for the **Create Firewall Rule** action.
 - Updated the mitigation functions to resolve the `NOT FOUND` error encountered with the **Mitigate Threat** action.
- **Version 1.1.0**
 - Added new [Configuration](#) parameter: **Hostname**.
 - Updated the **Create Firewall Rule** action:
 - Added `site` user field.
 - Resolved a bug that prevented rules from being created.
 - Performed minor cosmetic updates.
- **Version 1.0.1**
 - Switches to API Token-based authentication
- **Version 1.0.0**
 - Initial version