ThreatQuotient

SentinelOne Action Guide

Version 1.0.0

December 20, 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

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	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/sentinelone-action

Introduction

The SentinelOne action contains three functions that provide you with the ability to add/remove hashes to blacklist/whitelist and mitigate actions on indicators.

> Credentials and other configurations should be obtained from the SentinelOne instance. These are intended for bulk and/or automated execution of SentinelOne features.

The action provides the following functions:

- **SentinelOne Blacklist or Whitelist** - adds SHA-1 hashes to either the blacklist or the whitelist on the SentinelOne platform.
- **SentinelOne Mitigate Threats** - performs mitigation actions on indicators on the SentinelOne platform.
- **SentinelOne Delete Hashes** - removes SHA-1 hashes from either the blacklist or the whitelist on the SentinelOne platform.

The action is compatible with SHA-1 and File Path indicator types and returns indicators and indicator attributes.

> 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 the following indicator objects:
  - SHA-1
  - File Path
- Your SentinelOne SiteID.
- Your SentinelOne Username.
- Your SentinelOne Password associated with the username.
- Your SentinelOne Hostname.

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action 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 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:

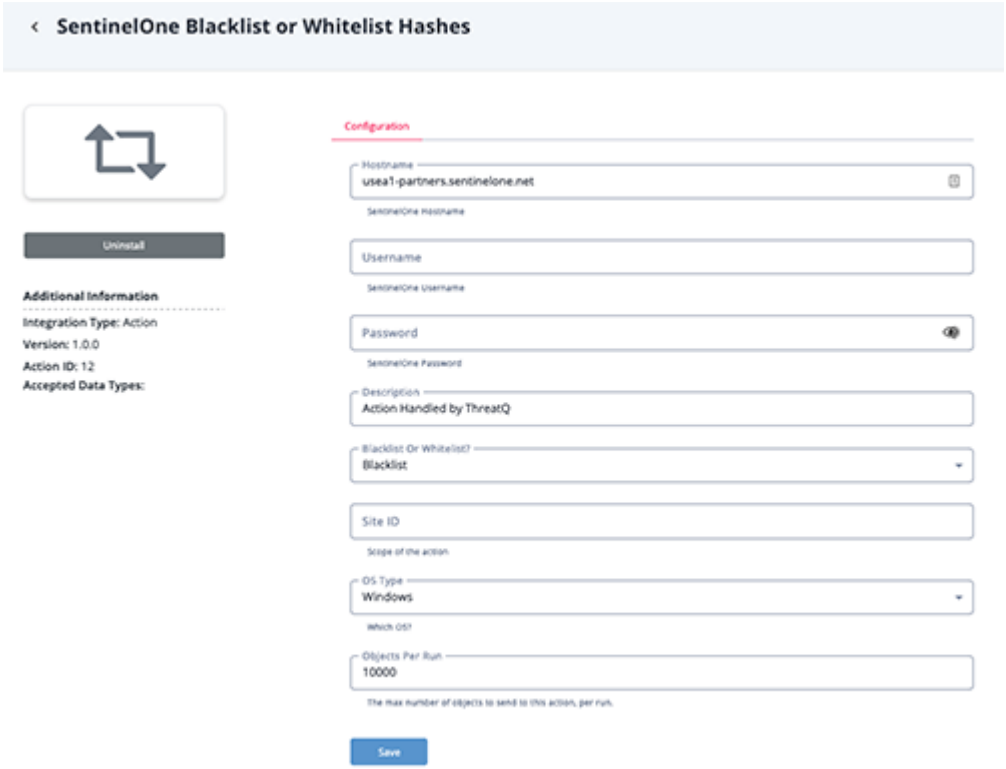
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

SentinelOne Blacklist or Whitelist

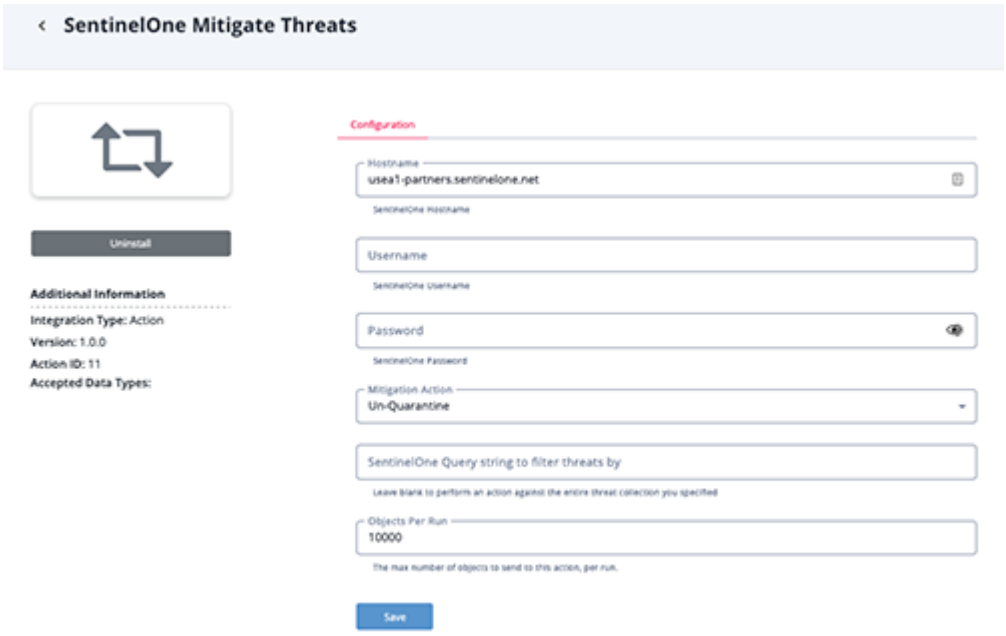
PARAMETER	DESCRIPTION
Hostname	Your SentinelOne Hostname.
Username	Your SentinelOne Username.
Password	Your SentinelOne Password.
Objects Per Run	The number of objects to send to this action per run. The max value for this parameter is 50,000.
Description	Enter a description to be added to the indicators. The default description is **Action Handled by ThreatQ**.

PARAMETER	DESCRIPTION
Blacklist or Whitelist?	Select how to ingest the Indicator. Options include Blacklist and Whitelist.
Site ID	The scope of the action.
OS Type	Select the OS type to use. Options include: ◦ Legacy Windows ◦ Windows ◦ Mac ◦ Linux



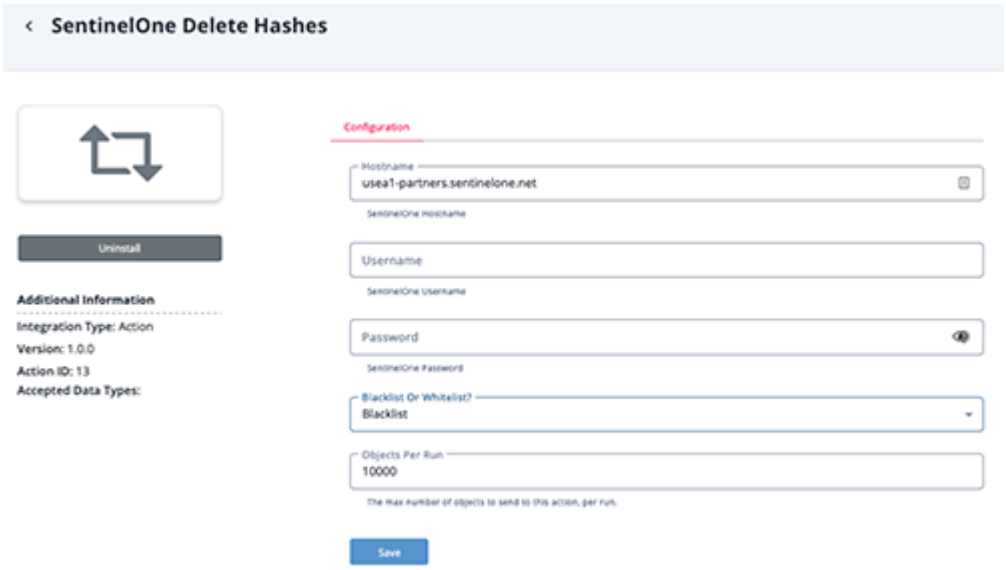
SentinelOne Mitigate Threats

PARAMETER	DESCRIPTION
Hostname	Your SentinelOne Hostname.
Username	Your SentinelOne Username.
Password	Your SentinelOne Password.
Mitigation Action	Select the mitigation action for SentinelOne. Options include: ◦ Quarantine ◦ Kill ◦ Remediate ◦ Rollback Remediate ◦ Disconnect from Network ◦ Un_Quarantine
SentinelOne Query string to filter threats by	Add additional filter criteria for SentinelOne. You can leave this parameter blank to run the action against the entire threat collection you have specified.
Objects Per Run	The number of objects to send to this action per run. The max value for this parameter is 50,000.



SentinelOne Delete Hashes

PARAMETER	DESCRIPTION
Hostname	Your SentinelOne Hostname.
Username	Your SentinelOne Username.
Password	Your SentinelOne Password.
Blacklist or Whitelist?	Select which list to remove hashes from in SentinelOne. Options include Blacklist and Whitelist.
Objects Per Run	The number of objects to send to this action per run. The max value for this parameter is 50,000.



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

Action Functions

The action provides the following functions:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
SentinelOne Blacklist or Whitelist Hashes	Adds SHA-1 hashes to either the blacklist or the whitelist on the SentinelOne platform.	Indicators	SHA-1
SentinelOne Mitigate Threats	Allows an analyst to perform mitigation actions on indicators on the SentinelOne platform.	Indicators	SHA-1, File Paths
SentinelOne Delete Hashes	Removes SHA-1 hashes from either the blacklist or the whitelist on the SentinelOne platform.	Indicators	SHA-1

SentinelOne Blacklist or Whitelist Hashes

The SentinelOne BlackList or Whitelist Hashes function adds SHA-1 hashes to either the Blacklist or Whitelist (specified by the user) on the SentinelOne platform.

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

Sample Request:

```
{
  "data": {},
  "filter": {
    "contentHash__contains": [
      "1af5d01cbcfa335c0f0983386d178dc09956e1cc"
    ],
    "query": "string",
    "filePath__contains": [
    ]
  }
}
```

Sample Response:

```
{
    "data": {
        "affected": 1
    }
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data.osType`	Indicator.Attribute	Blacklisted / Whitelisted in SentinelOne	N/A	`macos`	Value generated by the request and not by the response.

SentinelOne Mitigate Threats

The SentinelOne BlackList Mitigate Threats function provides you with the ability to perform mitigation actions on indicators on the SentinelOne platform.

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

Sample Request:

```
{
  "data": {},
  "filter": {
    "contentHash__contains": [
      "1af5d01cbcfa335c0f0983386d178dc09956e1cc"
    ],
    "query": "string",
    "filePath__contains": [
    ]
  }
}
```

Sample Response:

```
{
    "data": {
        "affected": 1
    }
}
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
`.data.affected`	Indicator.Attribute	Computers Affected by mitigation:	N/A	`Computers Affected by mitigation: 1`

SentinelOne Delete Hashes

The SentinelOne Delete Hashes function provides you with the ability to perform mitigation actions on indicators in the SentinelOne platform.

```
GET https://{{hostname}}/web/api/v2.1/{{action_type}}?value__contains={{indicator_values}}
&includeChildren=true
```

Sample Response:

```
{
    "data": [
        {
            "createdAt": "2021-10-26T15:05:00.042035Z",
            "description": "Action handled Via ThreatQ",
            "id": "1275336012951168745",
            "includeChildren": false,
            "includeParents": false,
            "notRecommended": "NONE",
            "osType": "windows",
            "scope": {
                "siteIds": [
                    "123987123987"
                ]
            },
            "scopeName": "site",
            "scopePath": "Global\\Threat Quotient\\Default site",
            "source": "user",
            "type": "black_hash",
            "updatedAt": "2021-10-26T15:05:00.041536Z",
            "userId": "12345678909875",
            "userName": "Our User",
            "value": "7eb2197d6fd80c31bd04d3a7fb8c725eb9789013"
        }
    ],
    "pagination": {
        "nextCursor": null,
        "totalItems": 1
    }
}
```

Supplemental Call

The following are request and response examples for the supplemental call to delete the hash from the SentinelOne list.

```
DELETE https://{{hostname}}/web/api/v2.1/{{action_type}}
```

Sample Request

```
{
    "data":{
        "ids":"1275336012951168745"
    }
}
```

Sample Response

```
{
    "data": {
        "affected": 1
    }
}
```

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.

SentinelOne Blacklist or Whitelist Hashes

METRIC	RESULT
Run Time	2 minutes
Indicators	17
Indicator Attributes	14

Change Log

- **Version 1.0.0**
  - Initial release