ThreatQuotient

A Securonix Company

CrowdStrike Insight EDR Action Bundle

Version 1.2.1

July 13, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	1.2.1
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The CrowdStrike Insight EDR Bundle provides action that submit data collections containing IP Address, SHA-1, SHA-256 and MD5 IOCs to CrowdStrike Insight EDR. The integration queries the submitted objects for enrichment and returns related threat intelligence to be ingested into the ThreatQ library.

The action can perform the following functions:

- **CrowdStrike Insight EDR Enrich IOC** - submits indicators to CrowdStrike Insight EDR to be enriched with related threat intelligence.
- **CrowdStrike Insight EDR Export IOC** - updates, enriches, and exports indicators to CrowdStrike Insight EDR.

The action is compatible with the following indicator types:

- FQDN
- IP Address
- SHA-1
- SHA-256
- MD5

The action returns enriched indicator type system objects.

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:
  - FQDN
  - IP Address
  - SHA-1
  - SHA-256
  - MD5

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:

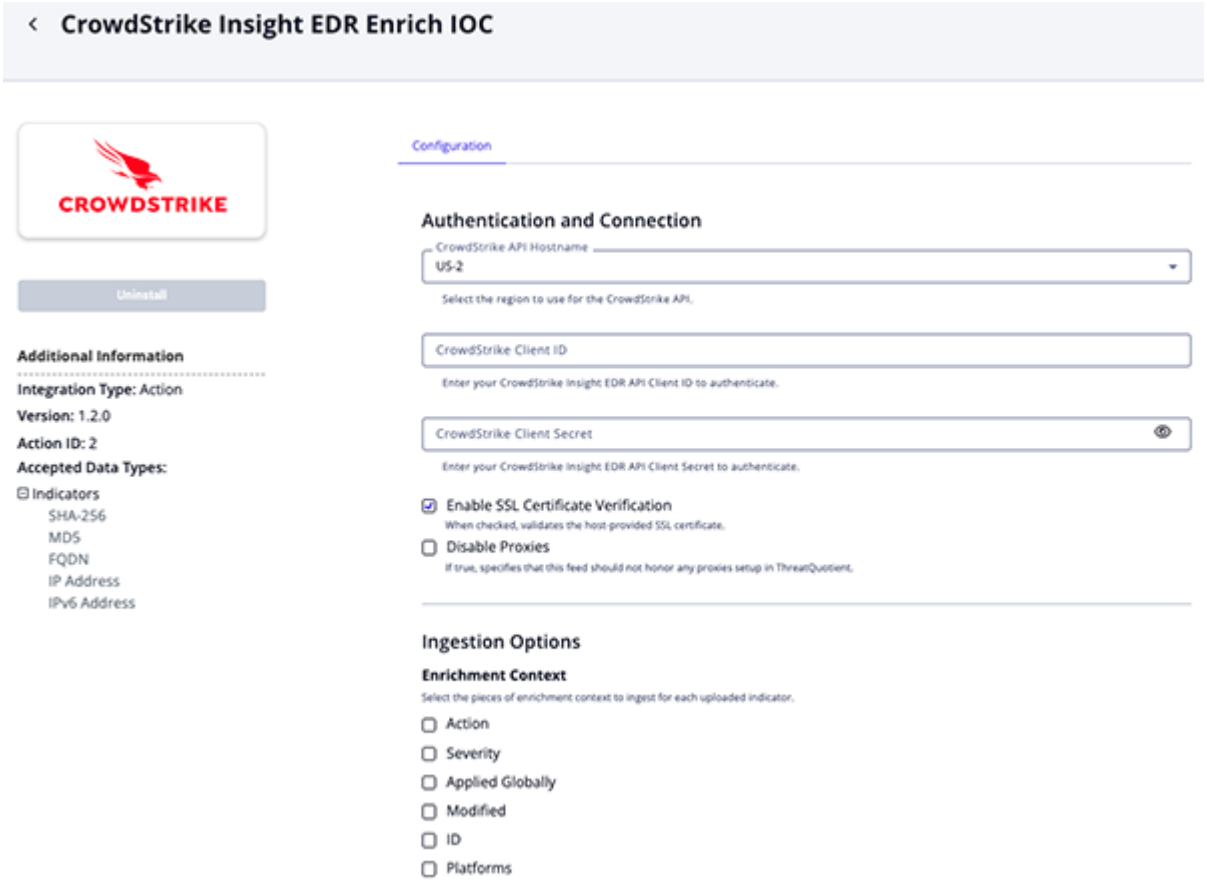
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   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.

CrowdStrike Insight EDR Enrich IOC Parameters

PARAMETER	DESCRIPTION
CrowdStrike API Hostname	Select the region to use for the CrowdStrike API. Option include: ◦ **US-1**: `api.crowdstrike.com` ◦ **US-2**: `api.us-2.crowdstrike.com` (Default) ◦ **EU-1**: `api.eu-1.crowdstrike.com` ◦ **US-GOV-1**: `api.laggar.gcw.crowdstrike.com`
CrowdStrike Client ID	Your CrowdStrike Client ID.
CrowdStrike Client Secret	Your CrowdStrike Client Secret.

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Enrichment Context	Select the pieces of enrichment context to ingest for each uploaded indicator. Options include: ◦ Action ◦ Severity ◦ Applied Globally ◦ Modified ◦ ID ◦ Platforms
Objects Per Run	The max number of objects per run to send to this action. The max value for this parameter is 10,000.

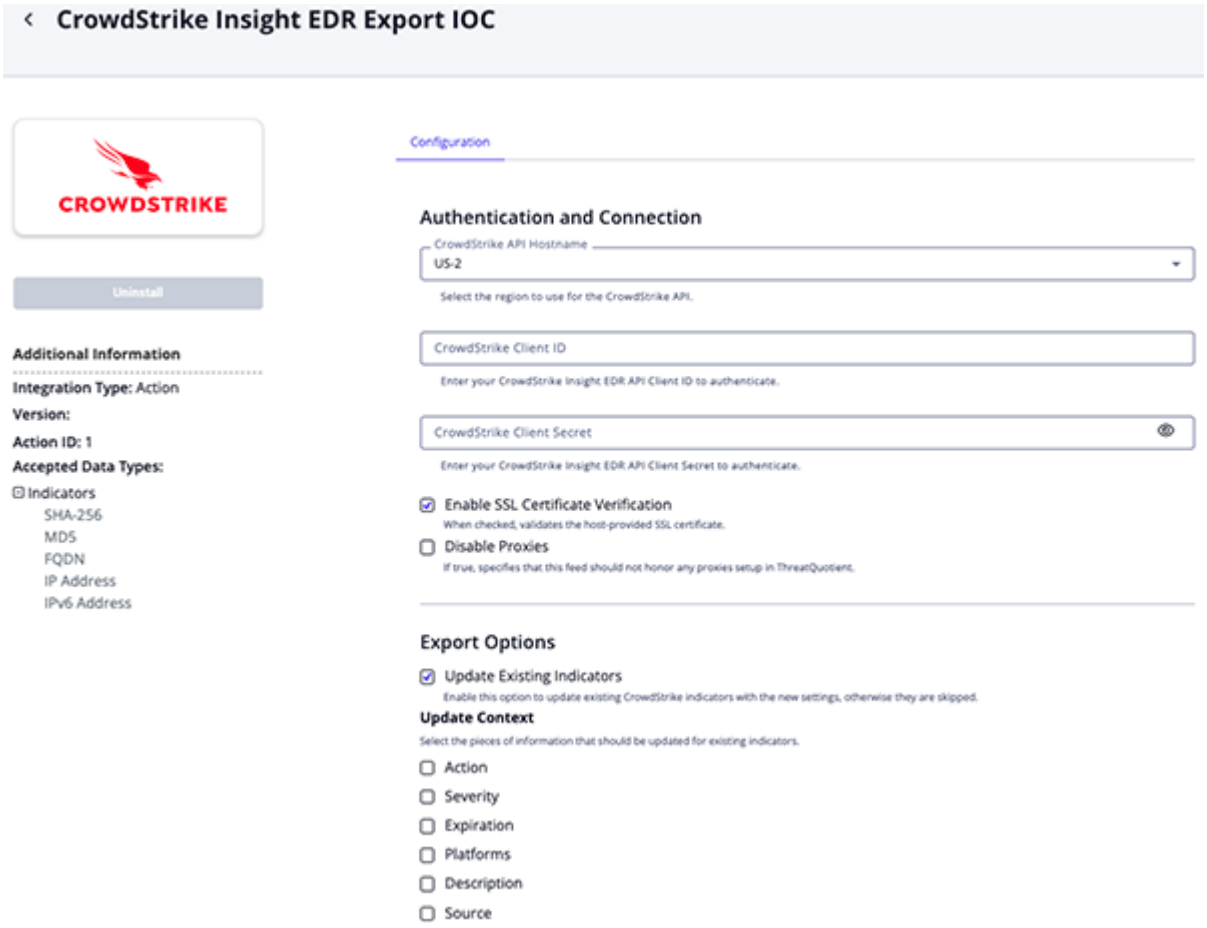

CrowdStrike Insight EDR Enrich IOC
CROWDSTRIKE
Uninstall
Additional Information
Integration Type: Action
Version: 1.2.0
Action ID: 2
Accepted Data Types:
Indicators
SHA-256
MD5
FQDN
IP Address
IPv6 Address
Configuration
Authentication and Connection
CrowdStrike API Hostname
US-2
Select the region to use for the CrowdStrike API.
CrowdStrike Client ID
Enter your CrowdStrike Insight EDR API Client ID to authenticate.
CrowdStrike Client Secret
Enter your CrowdStrike Insight EDR API Client Secret to authenticate.
Enable SSL Certificate Verification
When checked, validates the host-provided SSL certificate.
Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.
Ingestion Options
Enrichment Context
Select the pieces of enrichment context to ingest for each uploaded indicator.
Action
Severity
Applied Globally
Modified
ID
Platforms

CrowdStrike Insight EDR Export IOC Parameters

PARAMETER	DESCRIPTION
CrowdStrike API Hostname	Select the region to use for the CrowdStrike API. Option include: ◦ **US-1**: `api.crowdstrike.com` ◦ **US-2**: `api.us-2.crowdstrike.com` (Default) ◦ **EU-1**: `api.eu-1.crowdstrike.com` ◦ **US-GOV-1**: `api.laggar.gcw.crowdstrike.com`
CrowdStrike Client ID	Your CrowdStrike Client ID.
CrowdStrike Client Secret	Your CrowdStrike Client Secret.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Update Existing Indicators	Enable this parameter to update existing CrowdStrike indicators with the new settings. Disable this this parameter to skip updating existing indicators. This parameter is enabled by default.
Update Context	Select the pieces of information that should be updated for existing indicators. Options include: ◦ Action ◦ Severity ◦ Platforms ◦ Description

PARAMETER	DESCRIPTION
	◦ Expiration ◦ Source This parameter is only accessible if you have enabled the **Update Existing Indicators** parameter.
Default Source	Enter the original source of the indicator. This be used for tracking where an indicator was defined. The maximum character limit is 200 characters.
Default Expiration Days	Enter the number of days the indicators should remain active in CrowdStrike Insight EDR.
Default Platforms	Select the platform where the indicator originated. Options include: mac, windows, and linux.
Indicators of Compromise (IOC) Action	The action to be updated. Options include: ◦ Block -> Block and show as detection ◦ Block, hide detection -> Block and detect, but hide from Activity > Detections ◦ Detect Only -> Show as a detection and take no other action ◦ Allow -> Allow, do not detect ◦ No action > Save indicator in IOC Management, but take no action The only available options will be `Detect Only` and `No Action` if the input collection contains IP Address, IPv6 Address, or FQDN indicator types. See if the Known Issues / Limitations section for more details.

PARAMETER	DESCRIPTION
Severity	Select the severity for the uploaded indicators. Options include: ◦ Critical ◦ High ◦ Medium ◦ Low ◦ Informational
Include Attributes in Descriptions	Enable this parameter to append the selected ThreatQ attribute values to the description of each exported CrowdStrike IOC.
Description Attribute Names	Enter the names of the ThreatQ attributes to append to the CrowdStrike IOC description, with one attribute name per line. All values associated with each specified attribute name are included in the exported IOC description. This parameter is only accessible if you have enabled the **Include Attributes in Descriptions** parameter.
Enrich Indicators	Enable this parameter to enrich the indicators with upload information. This parameter is disabled by default.
Objects Per Run	The max number of objects per run to send to this action. The max value for this parameter is 10,000.



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

Actions

The bundle provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
CrowdStrike Insight EDR Enrich IOC	Enriches IOCs using the CrowdStrike API.	Indicators	SHA-1, SHA-256 and MD5
CrowdStrike Insight EDR Export IOC	Exports, updates, and enriches IOCs using the CrowdStrike API.	Indicators	IP Address, FQDN, SHA-256, MD5

CrowdStrike Insight EDR Enrich IOC

The CrowdStrike Insight EDR Enrich IOC action enriches SHA-1, SHA-256 and MD5 IOCs using CrowdStrike Insight EDR API.

The following endpoint fetches the resource ID that will be used on a supplemental call to get all the info.

```
GET https://<host>:<port>/iocs/queries/indicators/v1
```

Sample Parameters

```
{
  "filter": "value:'85.195.206.7'"
}
```

Sample Response

```
{
    "errors": null,
    "meta": {
        "pagination": {
            "after":
"czMmYxNTkzNWQxNWVlNzkxNGNkYmVkODBkMzhhNmY1NjRiYTg4ZTEiXQ==",
            "limit": 100,
            "offset": 1,
            "total": 1
        },
        "powered_by": "ioc-manager",
        "query_time": 0.099,
        "trace_id": "c01423a1-3f69-434f-84e0-f7bc558ff01a"
    },
    "resources": [

"b96b67aef3d665e84fc93f9e732f15935d15ee7914cdbed80d38a6f564ba88e2"
    ]
}
```

Get Existing IOCs - Supplemental

The Get Existing IOCs supplemental feed is used to retrieve the IOC values.

```
GET https://<host>:<port>/iocs/entities/indicators/v1
```

Parameters

```
{
  "ids":
"f9755ed63476fd41a1f92304c007111c79f609db98ff1281df16d919fbd20c0a"
}
```

Sample Response

```
{
    "errors": null,
    "meta": {
        "pagination": {
            "limit": 0,
            "total": 1
        },
        "powered_by": "ioc-manager",
        "query_time": 0.001333305,
        "trace_id": "97e50ec8-49fe-4663-b7b6-8f211ae5c9cb"
    },
    "resources": [
        {
            "action": "no_action",
            "applied_globally": true,
            "created_by": "457ce6add3ce437ca3879eba21c7240f",
            "created_on": "2020-01-01T00:30:10.800012000Z",
            "deleted": false,
            "expired": false,
            "from_parent": false,
            "id":
"b96b67aef3d665e84fc93f9e732f15935d15ee7914cdbed80d38a6f564ba88e1",
            "metadata": {},
            "mobile_action": "no_action",
            "modified_by": "059c817c5d4242abac7d7468c2413e77",
            "modified_on": "2020-01-01T00:30:10.800012000Z",
            "platforms": [
                "windows",
                "linux",
                "mac"
            ],
            "severity": "low",
            "source": "ThreatQ",
            "tags": [],
            "type": "md5",
            "value": "c2ffb650839873a332125e7823d36f9e"
        }
```

```
    ]
}
```

CrowdStrike Insight EDR Export IOC

The Export IOC action exports, updates, and enriches IP Address, IPv6 Address, FQDN, SHA-256 and MD5 IOCs using CrowdStrike's Insight EDR API.

The CrowdStrike API enforces strict validation rules that will cause the upload of an entire batch of 100 indicators to fail if a single entry is invalid. See the Known Issues / Limitations section for more details.

Create New Indicators - `POST https://<host>:<port>/iocs/entities/indicators/v1`

Update Existing Indicators - `PATCH https://<host>:<port>/iocs/entities/indicators/v1`

The indicator description is generated by concatenating the indicator score, related adversary names, and Malware Family attribute values.

Sample Request:

```
{
  "indicators": [
    {
      "action": "detect",
      "type": "ipv4",
      "value": "85.195.206.7",
      "expiration": "2026-01-15T14:38:27.015Z",
      "source": "ThreatQ",
      "severity": "high",
      "description": "Score: 9; Related Adversaries: Agrius",
      "platforms": [
        "mac"
      ],
      "applied_globally": true
    }
  ]
}
```

IOC Action Mapping

The table demonstrates how CrowdStrike Actions are mapping as attributes in ThreatQ.

CROWDSTRIKE ACTION	THREATQ ATTRIBUTE
prevent	Block
prevent_no_ui	Block, hide detection
detect	Detect Only
allow	Allow
no_action	No action

Shared Mapping

ThreatQuotient provides the following default mapping for both actions:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value`	Indicator.Value	`.type`	`.created_on`	`85.195.206.7`	Type mapped according to `Crowdstrike Indicators Mapping`
`.action`	Indicator.Attribute	Action	`.created_on`	`Detect Only`	User-configurable. Updatable. Mapped according to `CrowdStrike Action Mapping`
`.severity`	Indicator.Attribute	Severity	`.created_on`	`high`	User-configurable. Updatable
`.applied_globally`	Indicator.Attribute	Applied Globally	`.created_on`	`true`	User-configurable. Updatable
`.modified_on`	Indicator.Attribute	Modified	`.created_on`	`2025-12-16 14:38:31-00:00`	User-configurable. Updatable. Timestamp formatted.
`.id`	Indicator.Attribute	ID	`.created_on`	`178967922e345af7fe06bd657eef5b12bba3743a4448889d63d2711285d55de3`	User-configurable.
`.platforms[]`	Indicator.Attribute	Platforms	`.created_on`	`mac`	User-configurable.

CrowdStrike Indicator Type Mapping

The following table shows how CrowdStrike indicator types are mapping in ThreatQ.

CROWDSTRIKE INDICATOR TYPE	THREATQ INDICATOR TYPE
sha256	SHA-256
md5	MD5
domain	FQDN
ipv4	IP Address
ipv6	IPv6 Address

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.

CrowdStrike Insight EDR Enrich IOC

METRIC	RESULT
Run Time	1 minute
Indicators	205
Indicator Attributes	1,224

Known Issues / Limitations

- **CrowdStrike Insight EDR Export IOC** - The CrowdStrike API enforces strict validation rules that will cause the upload of an entire batch of 100 indicators to fail if a single entry is invalid. Since there is no programmatic workaround for these API-level constraints, ensure your data and configurations avoid the following scenarios to prevent bulk upload failures:
    - If the input collection contains indicators of type: IP Address, IPv6 Address or FQDN the only available options for the user configuration **Indicators of Compromise (IOC) Action** are:
        - `Detect only -> Show as a detection and take no other action`
        - `No action -> Save indicator in IOC Management, but take no action`

Change Log

- **Version 1.2.1**
  - **CrowdStrike Insight EDR Export IOC -** Added support for exporting selected ThreatQ attribute values to the CrowdStrike IOC Description field through the new **Include Attributes in Descriptions** and **Description Attribute Names** configuration parameters. When a selected attribute appears multiple times on an indicator, all associated values are preserved and included in the exported description.
- **Version 1.2.0**
  - Improved the search process for existing indicators within CrowdStrike through bulk search functionality.
  - Removed the **CrowdStrike Insight EDR Update IOC** action and migrated its functionality into the **CrowdStrike Insight EDR Export IOC** action.
  - Added the following configuration parameters to all actions:
    - **Enable SSL Certificate Verification** - configure if the action should validate the host-provided SSL certificate.
    - **Disable Proxies** - configure if the action should honor proxies set in the ThreatQ UI.
  - Added the following new configuration parameters to the **CrowdStrike Insight EDR Export IOC** action:
    - **Update Existing Indicators** - configure if the action should update existing CrowdStrike indicators with the new settings.
    - **Update Context** - determine if pieces of information that should be updated for existing indicators.
    - **Indicators of Compromise Action** - select the action for the uploaded indicators.
    - **Severity** - select the severity for the uploaded indicators.
  - Added the following new configuration parameter to the **CrowdStrike Insight EDR Enrich IOC** action:
    - **Enrichment Context** - select the pieces of enrichment context to ingest for each uploaded indicator.
- **Version 1.1.0**
  - Added new action to the bundle: **CrowdStrike Insight EDR Export IOC**.
  - Improved existing actions to meet updated standards.

- **Version 1.0.0**
  - Initial release