ThreatQuotient

CrowdStrike Insight EDR Action Bundle

Version 1.1.0

March 17, 2024

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	>= 5.6.0
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 Update IOC** - submits indicators to CrowdStrike Insight EDR to be updated with related threat intelligence.
- **CrowdStrike Insight EDR Export IOC** - 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.

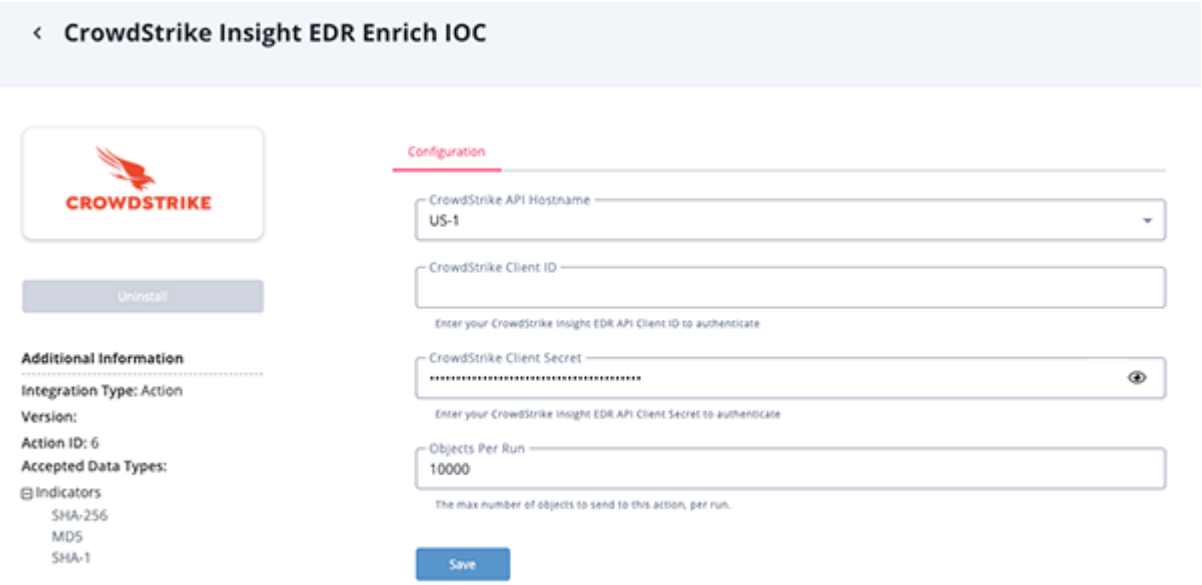
To configure the integration:

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

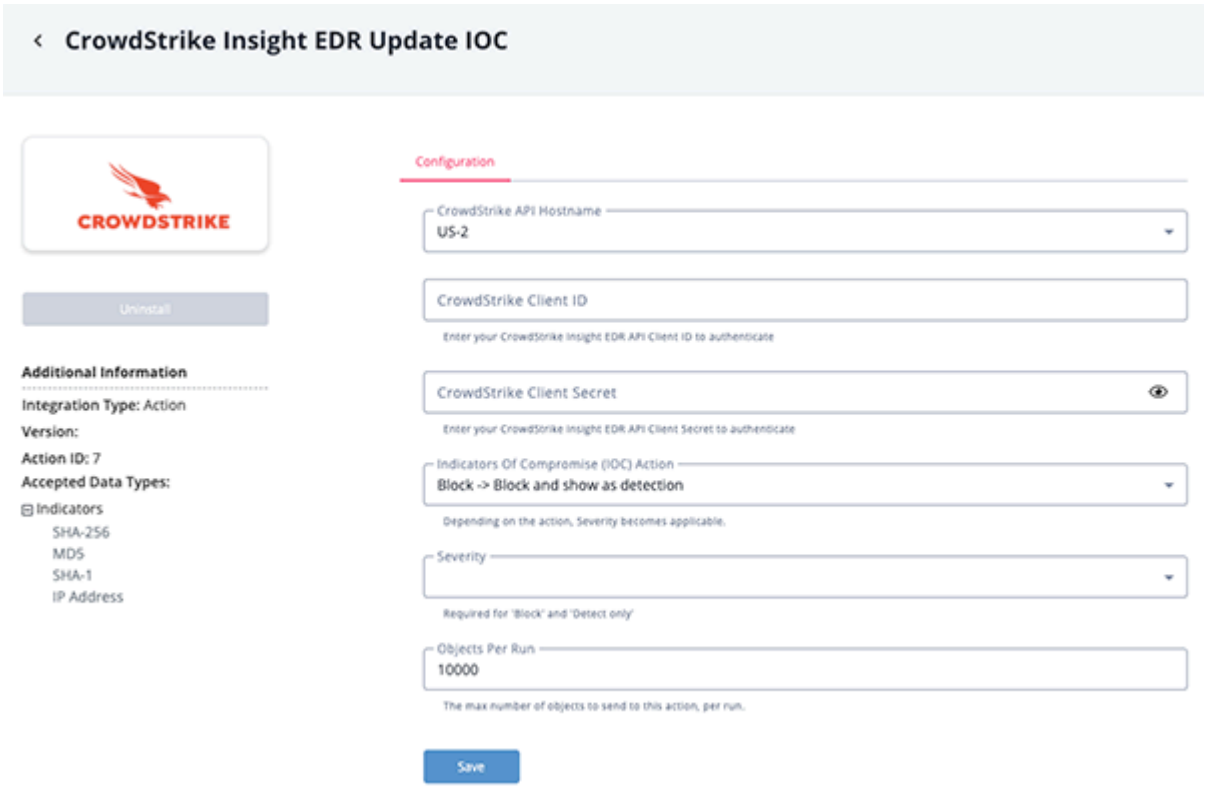
PARAMETER	DESCRIPTION
CrowdStrike API Hostname	Select the region to use for the CrowdStrike API. Option include: ◦ **US-1**: `api.crowdstrike.com` ◦ **US-2**: `api.us-2.crowdstrike.com` (Default) ◦ **EU-1**: `api.eu-1.crowdstrike.com` ◦ **US-GOV-1**: `api.laggar.gcw.crowdstrike.com`
CrowdStrike Client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

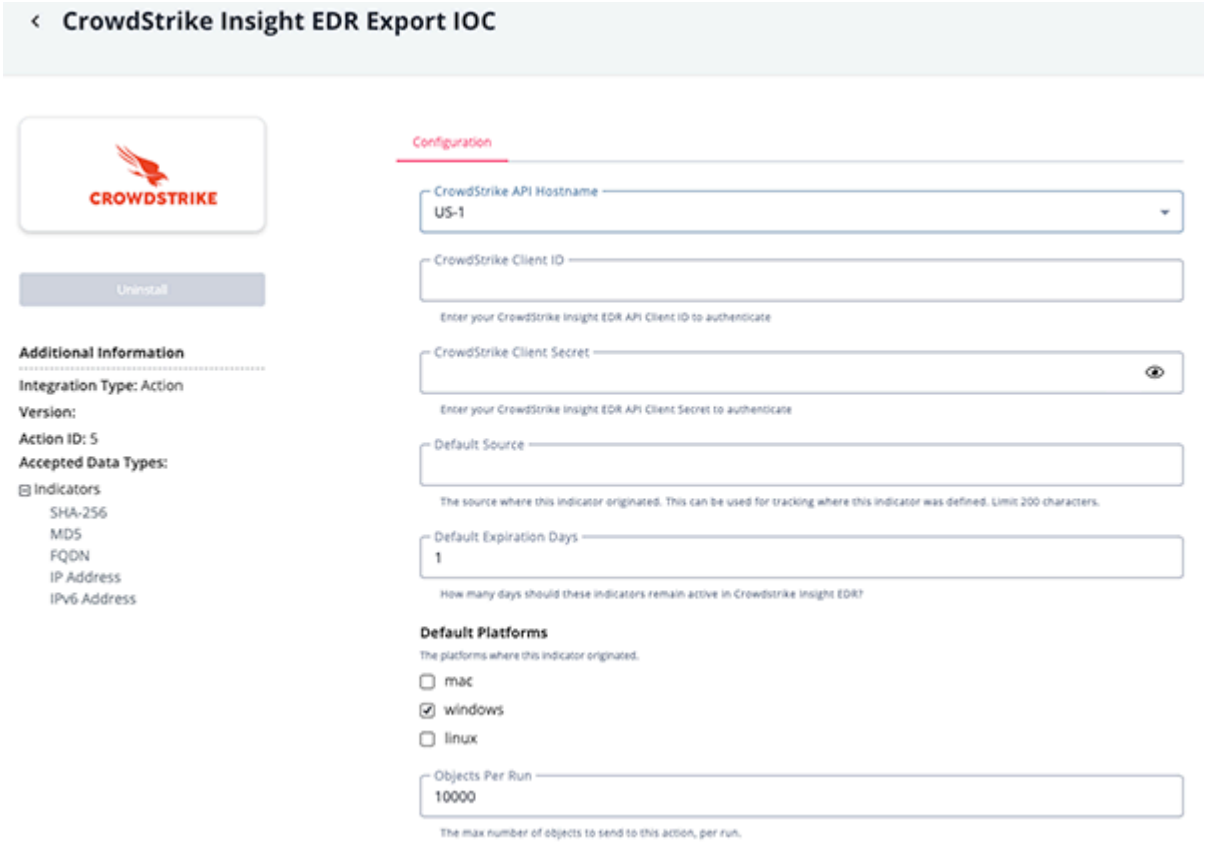
PARAMETER	DESCRIPTION
CrowdStrike API Hostname	Select the region to use for the CrowdStrike API. Option include: ◦ **US-1**: `api.crowdstrike.com` ◦ **US-2**: `api.us-2.crowdstrike.com` (Default) ◦ **EU-1**: `api.eu-1.crowdstrike.com` ◦ **US-GOV-1**: `api.laggar.gcw.crowdstrike.com`
CrowdStrike Client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

PARAMETER	DESCRIPTION
Severity	The severity to be updated. Options include: ◦ Critical ◦ High ◦ Medium ◦ Low ◦ Informational
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 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.
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.
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**.

Action Functions

The bundle provides the following actions:

FUNCTION	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 Update IOC	Update IOCs using the CrowdStrike API.	Indicators	IP Address, SHA-1, SHA-256 and MD5
CrowdStrike Insight EDR Export IOC	Export IOCs using the CrowdStrike API.	Indicators	IP Address, FQDN, SHA-256, MD5

CrowdStrike Insight EDR Enrich IOC

This function 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 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 Indicators by IDs - supplemental

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


```
{
    "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"
        }
    ]
}
```


ThreatQ provides the following default mapping for this workflow:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.resources[].tags[]`	Indicator.Tags	N/A	N/A	N/A	N/A
`.resources[].action`	Indicator.Attribute	Action	`.resources[].created_on`	`No Action`	N/A
`.resources[].severity`	Indicator.Attribute	Severity	`.resources[].created_on`	`low`	N/A
`.resources[].applied_globally`	Indicator.Attribute	Applied Globally	`.resources[].created_on`	`true`	N/A
`.resources[].modified_on`	Indicator.Attribute	Modified	`.resources[].created_on`	`2020-01-01 00:30:10-00:00`	N/A
`.resources[].id`	Indicator.Attribute	ID	`.resources[].created_on`	`b96b67aef3d665e84fc93f9e732f15935d15ee7914cdbed80d38a6f564ba88e1`	N/A
`.resources[].platforms[]`	Related Malware.Value	Platforms	`.resources[].created_on`	`windows`	N/A

CrowdStrike Insight EDR Update IOC

This function enriches SHA-1, SHA-256, MD5 and IP Address IOCs using the 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 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"
    ]
}
```

Update Indicator - supplemental

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

```
{
    "errors": null,
    "meta": {
        "pagination": {
            "limit": 0,
            "total": 1
        },
        "powered_by": "ioc-manager",
        "query_time": 0.001333305,
        "trace_id": "97e50ec8-49fe-4663-b7b6-8f211ae5c9cb"
    },
    "resources": [
        {
           "id":
"b96b67aef3d665e84fc93f9e732f15935d15ee7914cdbed80d38a6f564ba88e2",
```

```
            "type": "md5",
            "value": "c200e0851b0355b85ecc27684f74ecb3",
            "source": "ThreatQ",
            "action": "prevent",
            "mobile_action": "no_action",
            "severity": "medium",
            "description": "Score: 0; Related Adversaries: Comfoo, FLYING
KITTEN, J41",
            "platforms": [
                "mac",
                "windows"
            ],
            "expired": false,
            "deleted": false,
            "applied_globally": true,
            "from_parent": false,
            "tags": [],
            "created_on": "2022-04-07T08:26:40.186338161Z",
            "created_by": "457ce6add3ce437ca3879eba21c7240f",
            "modified_on": "2023-01-09T11:44:02.084191705Z",
            "modified_by": "457ce6add3ce437ca3879eba21c7240f"
        }
    ]
}
```


ThreatQ provides the following default mapping for this workflow:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.resources[].tags[]`	Indicator.Tags	N/A	N/A	N/A	N/A
`.resources[].action`	Indicator.Attribute	Action	`.resources[].created_on`	`No Action`	N/A
`.resources[].severity`	Indicator.Attribute	Severity	`.resources[].created_on`	`medium`	N/A
`.resources[].applied_globally`	Indicator.Attribute	Applied Globally	`.resources[].created_on`	`true`	N/A
`.resources[].modified_on`	Indicator.Attribute	Modified	`.resources[].created_on`	`2022-04-07 08:26:40-00:00`	N/A
`.resources[].id`	Indicator.Attribute	ID	`.resources[].created_on`	`b96b67aef3d665e84fc93f9e732f15935d15ee7914cdbed80d38a6f564ba88e1`	N/A
`.resources[].platforms[]`	Related Malware.Value	Platforms	`.resources[].created_on`	`windows`	N/A

CrowdStrike Insight EDR Export IOC

The Export IOC action exports the IOC to the CrowdStrike Insight EDR platform.

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

Sample Request:

```
{
   "type": "md5",
   "value": "c2ffb650839873a332125e7823d36f9e",
   "expiration": "2020-01-09T00:30:10.800012000Z",
   "source": "ThreatQ",
   "description": [],
   "platforms": [
                "windows",
                "linux",
                "mac"
            ],
   "applied_globally": true,
}
```

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

CrowdStrike Insight EDR Update IOC

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

Known Issues / Limitations

- When running the CrowdStrike Insight EDR Update IOC action for IP Address Indicators, only the **Detect only** and **No action** options for the Indicators of Compromise (IOC) Action field are valid.

Change Log

- **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