

ThreatQuotient



CrowdStrike Falcon Intelligence Action Bundle

Version 1.1.0

February 03, 2025

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	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Installation.....	8
Configuration	9
Enrich IOCs Action Parameters.....	9
Enrich Adversaries Action Parameters	11
Actions	13
CrowdStrike Falcon Intelligence - Enrich IOCs	14
CrowdStrike Falcon Intelligence - Enrich Adversaries.....	18
Enriched Data.....	19
CrowdStrike Falcon Intelligence - Enrich IOCs	19
CrowdStrike Falcon Intelligence - Enrich Adversaries.....	19
Known Issues / Limitations	20
Change Log	21

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 © 2025 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	1.1.0
-----------------------------	-------

Compatible with ThreatQ Versions	>= 6.5.0
----------------------------------	----------

ThreatQ TQO License Required	Yes
------------------------------	-----

Support Tier	ThreatQ Supported
--------------	-------------------

Introduction

The CrowdStrike Falcon Intelligence Action Bundle submits data collections of adversaries and indicators to CrowdStrike Falcon Intelligence for enrichment. The CrowdStrike API queries the submitted objects for enrichment and returns related threat intelligence to be ingested into the ThreatQ library.

The integration provides the following actions:

- **CrowdStrike - Enrich IOCS** - submits indicators to CrowdStrike to be enriched with related threat intelligence.
- **CrowdStrike Falcon Intelligence - Enrich Adversaries** - enriches adversaries with Mitre objects.

The actions are compatible with the following system object types:

- Adversaries
- Indicators
 - Malware
 - FQDN
 - IP Address
 - CIDR Block
 - Mutex
 - SHA-1
 - SHA-256
 - MD5
 - Email Address

The actions return the following object types:

- Adversaries
- Attack Patterns (Enrich Adversaries action only)
- Indicators (Enrich IOCs action only)
- Malware (Enrich IOCs action only)



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 CrowdStrike API Hostname.
- A CrowdStrike Client ID.
- A CrowdStrike Client Secret.
- Enrich IOCs action - a data collection containing at least one of the following indicator objects:
 - FQDN
 - IP Address
 - CIDR Block
 - Mutex
 - SHA-1
 - SHA-256
 - MD5
 - Email Address
- Enrich Adversaries action - a data collection containing the Adversary object type.

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
6. Select the actions to install, when prompted, and then click on **Install**.



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.

The action(s) will now be installed. You will still need to [configure](#) the action(s).

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.

Enrich IOCs Action Parameters

PARAMETER	DESCRIPTION
CrowdStrike API Host Name	Select the appropriate CrowdStrike host. Options include: ◦ US-1: <code>api.crowdstrike.com</code> ◦ US-2: <code>api.us-2.crowdstrike.com</code> (Default) ◦ EU-1: <code>api.eu-1.crowdstrike.com</code> ◦ US-GOV-1: <code>api.laggar.gcw.crowdstrike.com</code>
Client ID	Your CrowdStrike Client ID that will be used to authenticate with the CrowdStrike API.
Client Secret	Your CrowdStrike Secret key.
Supporting Context	Select the pieces of context to bring into ThreatQ. Options include: ◦ Related Threat Actors ◦ Related Malware ◦ Related Domains ◦ Related CIDR Blocks ◦ Related Mutexes

PARAMETER	DESCRIPTION
	◦ Related IPs ◦ Related SHA-256 Hashes ◦ Related SHA-1 Hashes ◦ Related MD5 Hashes ◦ Related Email Addresses ◦ Is Deleted ◦ Kill Chain Phase ◦ Confidence ◦ Threat Types ◦ Targets
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The max number of objects per run to send to this action. The max value for this parameter is 50,000.

< CrowdStrike Falcon Intelligence - Enrich IOCs



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 1

Configuration

CrowdStrike API Hostname

US-2

Select the region to use for the CrowdStrike API

Client ID

Enter your CrowdStrike Client ID to authentication with the API

Client Secret

Enter your CrowdStrike Client Secret to authentication with the API

Supporting Context

Select which pieces of context you want to bring into ThreatQ

- ☐ Related Threat Actors
- ☐ Related Malware
- ☐ Related Domains
- ☐ Related IPs
- ☐ Related SHA-256 Hashes
- ☐ Related SHA-1 Hashes
- ☐ Related MD5 Hashes
- ☐ Related Email Addresses
- ☐ Related CIDR Blocks
- ☐ Related Mutexes
- ☐ Is Deleted
- ☒ Kill Chain Phase
- ☒ Confidence
- ☒ Threat Types
- ☒ Targets

- ☒ Enable SSL Certificate Verification
- ☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Objects Per Run

10000

The max number of objects to send to this action, per run.

Enrich Adversaries Action Parameters

PARAMETER	DESCRIPTION
CrowdStrike API Host Name	Select the appropriate CrowdStrike host. Options 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
Client ID	Your CrowdStrike Client ID that will be used to authenticate with the CrowdStrike API.

PARAMETER	DESCRIPTION
Client Secret	Your CrowdStrike Secret key.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	The max number of objects per run to send to this action. The max value for this parameter is 50,000.



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 2

Accepted Data Types:

Adversaries

Configuration

CrowdStrike API Hostname
US-2

Client ID

Secret

☒ Enable SSL Certificate Verification
☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Objects Per Run
1000
The number of objects to process per run of the workflow.

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

Actions

The integration provides the following actions:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
CrowdStrike Falcon Intelligence - Enrich IOCs	Enriches IOCs using CrowdStrike API.	Indicators	FQDN, IP Address, CIDR Block, Mutex, SHA-1, SHA-256, MD5 and Email Address
CrowdStrike Falcon Intelligence - Enrich Adversaries	Enrich adversaries with MITRE objects	Adversaries	N/A

CrowdStrike Falcon Intelligence - Enrich IOCs

The CrowdStrike Falcon Intelligence - Enrich IOCs action enriches FQDN, IP Address, CIDR Block, Mutex, SHA-1, SHA-256, MD5 and Email Address IOCs using CrowdStrike API.

POST <https://{{host}}/intel/entities/indicators/GET/v1>

Sample Body

```
{
  "ids": ["hash_sha1_c4ac414413dec7dc13436aa8c74f5592bb723eea",
"hash_md5_96a6a7a27dde12ca623d679f25fc20e0"]
}
```

Sample Response:

```
{
  "errors": [
    {
      "code": 404,
      "id": "ip_address_162.214.188.105",
      "message": "Not Found"
    },
    {
      "code": 404,
      "id": "ip_address_45.79.91.89",
      "message": "Not Found"
    },
    {
      "code": 404,
      "id": "ip_address_178.128.23.9",
      "message": "Not Found"
    }
  ],
  "meta": {
    "pagination": {
      "limit": 47,
      "offset": 0,
      "total": 47
    },
    "powered_by": "msa-api",
    "query_time": 0.66362254,
    "trace_id": "66137048-39cf-46c0-afcb-17336f2fb14e"
  },
  "resources": [
    {
      "_marker": "16151501302eb1797d155befd4b8703126cef89e31",
      "actors": [
        "DOPPELSPIDER"
      ],
      "deleted": false,

```

```

"domain_types": [],
"id": "ip_address_51.178.161.32",
"indicator": "51.178.161.32",
"ip_address_types": [],
"kill_chains": [
  "C2"
],
"labels": [
  {
    "created_on": 1595643899,
    "last_valid_on": 1595643899,
    "name": "ThreatType/Criminal"
  },
  {
    "created_on": 1595643899,
    "last_valid_on": 1595643899,
    "name": "Actor/DOPPELSPIDER"
  },
  {
    "created_on": 1595643899,
    "last_valid_on": 1595643899,
    "name": "ThreatType/Downloader"
  },
  {
    "created_on": 1595643898,
    "last_valid_on": 1595644319,
    "name": "MaliciousConfidence/Low"
  },
  {
    "created_on": 1595643898,
    "last_valid_on": 1595644319,
    "name": "KillChain/C2"
  },
  {
    "created_on": 1595643899,
    "last_valid_on": 1595643899,
    "name": "Malware/DoppelDridex"
  },
  {
    "created_on": 1595643899,
    "last_valid_on": 1595643899,
    "name": "ThreatType/Banking"
  }
],
"last_updated": 1615150130,
"malicious_confidence": "low",
"malware_families": [
  "DoppelDridex"
],
"published_date": 1595643898,

```

```

        "relations": [
            {
                "created_date": 1615150129,
                "id":
"hash_sha256_2182a1acbee8bee31f667e412f347addcc8bd1118133b97eeb75f03503b839ce",
                "indicator":
"2182a1acbee8bee31f667e412f347addcc8bd1118133b97eeb75f03503b839ce",
                "last_valid_date": 1615150129,
                "type": "hash_sha256"
            },
            {
                "created_date": 1615150129,
                "id": "hash_sha1_5c7de95d8c8e6fc59dfb7964982a8b5e3b00483c",
                "indicator": "5c7de95d8c8e6fc59dfb7964982a8b5e3b00483c",
                "last_valid_date": 1615150129,
                "type": "hash_sha1"
            },
            {
                "created_date": 1615150129,
                "id": "hash_md5_3306b016f87113678b4ab148c9018acc",
                "indicator": "3306b016f87113678b4ab148c9018acc",
                "last_valid_date": 1615150129,
                "type": "hash_md5"
            }
        ],
        "reports": [],
        "targets": [],
        "threat_types": [
            "Criminal",
            "Downloader",
            "Banking"
        ],
        "type": "ip_address",
        "vulnerabilities": []
    }
]
}

```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.resources.threat_types[]</code>	Indicator.Attribute	Threat Type	<code>.resources.published_date</code>	Criminal	If enabled
<code>.resources.deleted</code>	Indicator.Attribute	Is Disabled	<code>.resources.published_date</code>	True	If enabled
<code>.resources.kill_chains[]</code>	Indicator.Attribute	Kill Chain Phase	<code>.resources.published_date</code>	C2	If enabled
<code>.resources.malicious_confidence</code>	Indicator.Attribute	Confidence	<code>.resources.published_date</code>	low	If enabled
<code>.resources.targets[]</code>	Indicator.Attribute	Target	<code>.resources.published_date</code>	N/A	If enabled
<code>.resources.actors[]</code>	Related Adversary.Name	N/A	<code>.resources.published_date</code>	DOPPLESPIDER	If enabled
<code>.resources.malware_families[]</code>	Related Malware.Value	N/A	<code>.resources.published_date</code>	DoppelDrindex	If enabled
<code>.resources.relations[]</code> <code>.indicator</code>	Related Indicator.Value	Based on <code>.resources.type</code>	<code>.resources.published_date</code>	2182a1acbee8bee31f667e412f347addcc8bd118133b97eeb75f03503b839ce	If enabled

CrowdStrike Falcon Intelligence - Enrich Adversaries

The CrowdStrike Falcon Intelligence - Enrich Adversaries action enriches submitted Adversaries with MITRE objects.

GET <https://{HOST}/intel/queries/mitre/v1>

Sample Body

```
{
  "meta": {
    "query_time": 0.055441907,
    "powered_by": "msa-api",
    "trace_id": "a3a0f49d-928d-4c52-81d7-25a1f86af876"
  },
  "resources": [
    "fancy-bear_TA0001_T1078",
    "fancy-bear_TA0042_T1588.006",
    "fancy-bear_TA0043_T1589",
    "fancy-bear_TA0043_T1589.001",
    "fancy-bear_TA0043_T1589.002",
    "fancy-bear_TA0043_T1591",
    "fancy-bear_TA0043_T1595",
    "fancy-bear_TA0043_T1598",
    "fancy-bear_TA0043_T1598.003"
  ],
  "errors": []
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[]	Related Attack Pattern.Value	N/A	N/A	T1078	N/A

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 Falcon Intelligence - Enrich IOCs

METRIC	RESULT
Run Time	1 minute
Indicators	510
Indicator Attributes	2,448
Malware	4
Adversaries	4

CrowdStrike Falcon Intelligence - Enrich Adversaries

METRIC	RESULT
Run Time	1 minute
Adversaries	1
Attack Patterns	7

Known Issues / Limitations

- CrowdStrike may occasionally respond with a 403 Forbidden error even if the provided access token is still valid. CrowdStrike has attributed this to possible load balancing issues with their servers. In the event of receiving one of these errors, ThreatQ will attempt to reauthenticate on the first 403 Forbidden received, and usually proceed without incident. If it occurs a consecutive time, however, the feed run will complete with errors.
- The new MITRE filter uses cache memory to load all MITRE ATTCK data, with the cache being refreshed every 24 hours.

Change Log

- **Version 1.1.0**
 - Renamed the **CrowdStrike** action to the **CrowdStrike Falcon Intelligence - Enrich IOCs** action.
 - Added a new action: **CrowdStrike Falcon Intelligence - Enrich Adversaries**.
 - Added the following new configuration parameters to the CrowdStrike Falcon Intelligence - Enrich IOCs action:
 - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
 - **Disable Proxies** - determine if the action should honor proxy settings set in the ThreatQ UI.
 - Added **Known Issues / Limitations** chapter to the guide regarding CrowdStrike server balancing issues and the new MITRE filter cache refresh timing.
 - Renamed integration from **CrowdStrike Action** to **CrowdStrike Falcon Intelligence Action Bundle**.
 - Updated minimum ThreatQ version to 6.5.0.
- **Version 1.0.0**
 - Initial release