ThreatQuotient

CrowdStrike 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/crowdstrike-action

Introduction

The CrowdStrike action submits a data collection containing FQDN, IP Address, CIDR Block, Mutex, SHA-1, SHA-256, MD5, and Email Address IOCs to CrowdStrike.

The CrowdStrike API queries the submitted objects for enrichment and returns related threat intelligence to be ingested into the ThreatQ library in the form of Adversaries, Indicators, and Malware.

The action provides the following function:

- **CrowdStrike** - submits indicators to CrowdStrike to be enriched with related threat intelligence.

The action is compatible with the following indicator types:

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

The action returns the following object types:

- Adversaries
- Indicators
- Malware

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 at least one of the following indicator objects:
  - FQDN
  - IP Address
  - CIDR Block
  - Mutex
  - SHA-1
  - SHA-256
  - MD5
  - Email Address

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.

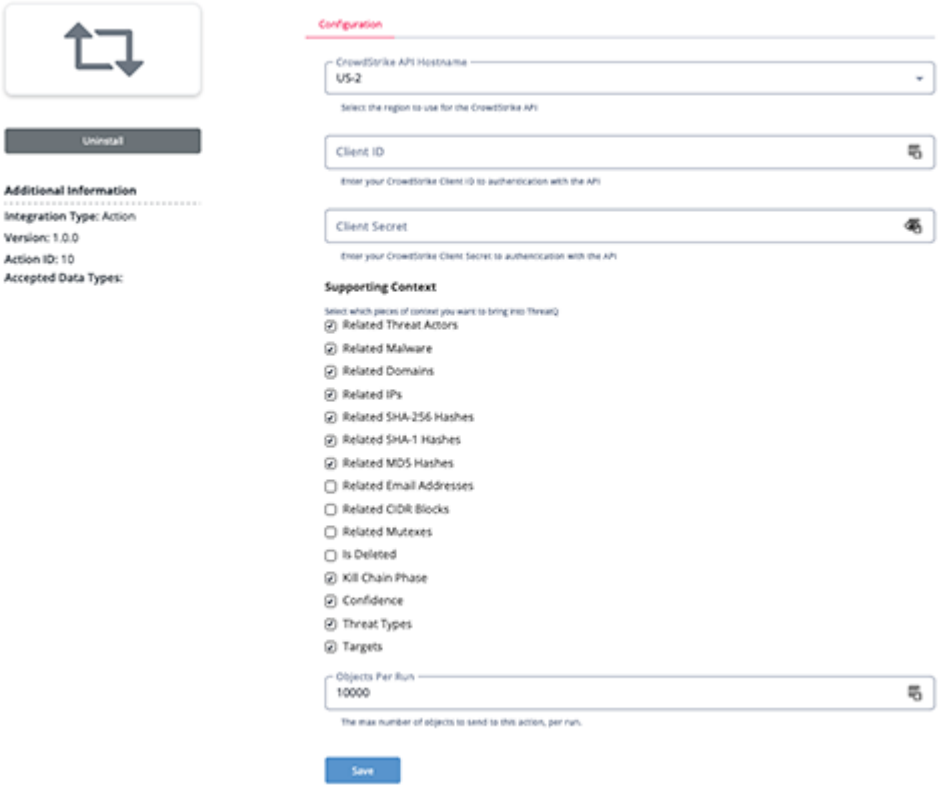
To configure the integration:

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.

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.
Client Secret	Your CrowdStrike Secret key.
Supporting Context	Select the pieces of context to bring into ThreatQ. Options include:

PARAMETER	DESCRIPTION
	◦ 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
Objects Per Run	The max number of objects per run to send to this action. 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 function:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Crowdstrike	Enriches IOCs using Crowdstrike API.	Indicators	FQDN, IP Address, CIDR Block, Mutex, SHA-1, SHA-256, MD5 and Email Address

CrowdStrike

The CrowdStrike function 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 function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.resources.threat_types[]`	Indicator.Attribute	Threat Type	`.resources.published_date`	`Criminal`	If enabled
`.resources.deleted`	Indicator.Attribute	Is Disabled	`.resources.published_date`	`True`	If enabled
`.resources.kill_chains[]`	Indicator.Attribute	Kill Chain Phase	`.resources.published_date`	`C2`	If enabled
`.resources.malicious_confidence`	Indicator.Attribute	Confidence	`.resources.published_date`	`low`	If enabled
`.resources.targets[]`	Indicator.Attribute	Target	`.resources.published_date`	N/A	If enabled
`.resources.actors[]`	Related Adversary.Name	N/A	`.resources.published_date`	`DOPPLESPIDER`	If enabled
`.resources.malware_families[]`	Related Malware.Value	N/A	`.resources.published_date`	`DoppelDridex`	If enabled
`.resources.relations[].indicator`	Related Indicator.Value	Based on `.resources.type`	`.resources.published_date`	`2182a1acbee8bee31f667e412f347addcc8bd1118133b97eeb75f03503b839ce`	If enabled

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.

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

Use Case Example

1. A user submits a data collection using the CrowdStrike action to the CrowdStrike API with a data collection containing 350 system objects:
    - 100 MD5
    - 75 SHA-1
    - 75 SHA-256
2. The CrowdStrike API queries the submitted data.
3. The action returns the submitted data collection enriched the following:
    - 99 Indicators
    - 30 Indicator Attributes
    - 20 Adversaries
    - 3 Malware

Change Log

- **Version 1.0.0**
  - Initial release