

# ThreatQuotient



## CrowdStrike Falcon Insight EDR Operation

Version 1.2.1 rev-a

January 13, 2025

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

---

# Contents

- Warning and Disclaimer ..... 3
- Support ..... 4
- Integration Details..... 5
- Introduction ..... 6
- Prerequisites ..... 7
  - CrowdStrike API Client Configuration .....7
- Installation..... 9
- Configuration ..... 10
- Actions ..... 11
  - Create Policy ..... 12
    - Parameters ..... 13
  - Create Hash Policy ..... 14
    - Parameters ..... 15
  - Find Detections ..... 16
    - Parameters ..... 20
    - Action Mapping..... 21
- Change Log ..... 23

# 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](mailto: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      | 1.2.1             |
| Compatible with ThreatQ Versions | >= 4.35.0         |
| Support Tier                     | ThreatQ Supported |

# Introduction

The CrowdStrike Falcon Insight EDR Operation for ThreatQ enables analysts to find detections and create new detection policies.

The operation provides the following actions:

- **Create Policy** - creates a detection policy for a given indicator.
- **Create Hash Policy** - creates a detection policy for a given hash.
- **Find Detections** - finds detections associated with the selected indicator.

The operation is compatible with the following indicator types:

- FQDN
- IP Address
- IPv6 Address
- MD5
- SHA-256

# Prerequisites

The following is required in order to install and run the operation:

- Your CrowdStrike API URL.
- Your CrowdStrike Client ID.
- Your CrowdStrike Client Secret.
- [CrowdStrike API Client permissions configured](#).

## CrowdStrike API Client Configuration

Users are required to create a properly scoped API Client within CrowdStrike's Falcon platform in order use the operation. API Clients can be created and configured via the **API Clients and Keys** page under **Support**.

The CrowdStrike Falcon Insight EDR operation requires the following scope permissions:

- **Detections** - Read permission required.

Edit API client

Client name

Insight EDR OP

14 / 50

Description

0 / 255

dete

| Scope                        | Read                                | Write                    |
|------------------------------|-------------------------------------|--------------------------|
| Detections                   | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Third Party Detection Exc... | <input type="checkbox"/>            | <input type="checkbox"/> |

Cancel

Update client details

- **IOC Management** - Read/Write permissions required.

×

Edit API client

Client name

Insight EDR OP

14 / 50

Description

0 / 255

🔍

loc

Scope

Read

Write

IOC Management

☒

☒

IOCs (Indicators of Comp...

☐

☐

Cancel

Update client details



# 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 integration whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration 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 operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to [configure](#) and then [enable](#) the operation.

# 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

| PARAMETER                 | DESCRIPTION                     |
|---------------------------|---------------------------------|
| CrowdStrike Host          | Enter your CrowdStrike API URL. |
| CrowdStrike Client ID     | Your CrowdStrike Client ID.     |
| CrowdStrike Client Secret | Your CrowdStrike Client Secret. |

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

# Actions

The CrowdStrike Falcon Insight EDR Operation provides the following actions:

| ACTION                             | DESCRIPTION                                              | OBJECT TYPE | OBJECT SUBTYPE                                 |
|------------------------------------|----------------------------------------------------------|-------------|------------------------------------------------|
| <a href="#">Create Policy</a>      | Creates a detection policy for a given indicator.        | Indicator   | (FQDN, IP Address, IPv6 Address, MD5, SHA-256) |
| <a href="#">Create Hash Policy</a> | Creates a detection policy for a given hash.             | Indicator   | MD5, SHA-256                                   |
| <a href="#">Find Detections</a>    | Finds detections associated with the selected indicator. | Indicator   | (FQDN, IP Address, IPv6 Address, MD5, SHA-256) |

## Create Policy

Creates a detection policy for a given indicator.

POST [https://{host}/iocs/entities/indicators/v1?ignore\\_warnings=true](https://{host}/iocs/entities/indicators/v1?ignore_warnings=true)

**Sample Response:**

```
{
  "meta": {
    "query_time": 0.210475806,
    "pagination": {
      "limit": 0,
      "total": 1
    },
    "powered_by": "ioc-manager",
    "trace_id": "cc9de49d-2153-4249-9403-28a0b199469e"
  },
  "errors": null,
  "resources": [
    {
      "id":
"7152cd6f5ea213c4028092e0b480b5e23addd441b79c4d91140010087301eaa3",
      "type": "ipv4",
      "value": "172.122.34.14",
      "source": "ThreatQAAAAA",
      "action": "detect",
      "severity": "high",
      "description": "Test description - aaa",
      "platforms": [
        "windows"
      ],
      "expiration": "2024-01-22T10:40:39.372Z",
      "expired": false,
      "deleted": false,
      "applied_globally": true,
      "from_parent": false,
      "created_on": "2023-05-10T11:26:54.197930075Z",
      "created_by": "457ce6add3ce437ca3879eba21c7240f",
      "modified_on": "2023-05-10T11:26:54.197930075Z",
      "modified_by": "457ce6add3ce437ca3879eba21c7240f"
    }
  ]
}
```

## Parameters

ThreatQ provides the following parameters for this Action:

| PARAMETER                    | DESCRIPTION                                                                                                                                                                                                                                                        |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy</b>                | Select an action to take when a host observes the custom IOC. Options include: <ul style="list-style-type: none"> <li>• <b>Detect</b> - Enable detections for this custom IOC (Default)</li> <li>• <b>None</b> - Disable detections for this custom IOC</li> </ul> |
| <b>IOC Expiration (Days)</b> | Enter a number representing the amount of days until the custom IOC expires. The default setting is 30 days.                                                                                                                                                       |
| <b>Source</b>                | Enter a source where this indicator originated. This can be used for tracking where this indicator was defined. The character limit is 200.                                                                                                                        |
| <b>Description</b>           | Enter a description to apply to the custom IOC. The default description is Custom IOC added manually from ThreatQ.                                                                                                                                                 |
| <b>Platforms</b>             | Enter the platforms where this indicator originated.                                                                                                                                                                                                               |
| <b>Severity</b>              | Select the IOC severity.                                                                                                                                                                                                                                           |

## Create Hash Policy

The Create Hash Policy action creates a detection policy for a given hash.

POST [https://{host}/iocs/entities/indicators/v1?ignore\\_warnings=true](https://{host}/iocs/entities/indicators/v1?ignore_warnings=true)

**Sample Response:**

```
{
  "meta": {
    "query_time": 5.86230334,
    "trace_id": "f93d42f9-34b9-47d7-9fe4-e7c5b8b21e48",
    "pagination": {
      "total": 1,
      "limit": 0
    },
    "powered_by": "ioc-manager"
  },
  "errors": null,
  "resources": [
    {
      "expired": false,
      "modified_on": "2023-10-03T14:42:45.402657088Z",
      "platforms": [
        "mac"
      ],
      "created_by": "457ce6add3ce437ca3879eba21c7240f",
      "id": "d9f2131da701e07dfc9f31ec9fd5ff3fea526b64463498673104e045537ba9b7",
      "applied_globally": true,
      "source": "ThreatQ",
      "deleted": false,
      "value": "ec84802bb2bb33c52c1f02e7a7b74c6ea6247611c410bf386a95dc1eb45e2347",
      "action": "detect",
      "type": "sha256",
      "description": "Custom IOC added manually from ThreatQ",
      "created_on": "2023-10-03T14:42:45.402657088Z",
      "modified_by": "457ce6add3ce437ca3879eba21c7240f",
      "severity": "high",
      "from_parent": false,
      "metadata": {
        "av_hits": -1,
        "signed": false
      }
    }
  ]
}
```

## Parameters

ThreatQ provides the following parameters for this Action:

| PARAMETER             | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy                | <p>Select an action to take when a host observes the custom IOC. Options include:</p> <ul style="list-style-type: none"> <li>• <b>Detect</b> - Enable detections for this custom IOC (Default)</li> <li>• <b>Prevent</b> - Block the IOC and show it as a detection at the selected severity</li> <li>• <b>Allow</b> - Allow the IOC but do not detect it</li> <li>• <b>None</b> - Disable detections for this custom IOC</li> </ul> |
| IOC Expiration (Days) | Enter a number representing the amount of days until the custom IOC expires. The default setting is 30 days.                                                                                                                                                                                                                                                                                                                         |
| Source                | Enter a source where this indicator originated. This can be used for tracking where this indicator was defined. The character limit is 200.                                                                                                                                                                                                                                                                                          |
| Description           | Enter a description to apply to the custom IOC. The default description is Custom IOC added manually from ThreatQ.                                                                                                                                                                                                                                                                                                                   |
| Platforms             | Enter the platforms where this indicator originated.                                                                                                                                                                                                                                                                                                                                                                                 |
| Severity              | Select the IOC severity.                                                                                                                                                                                                                                                                                                                                                                                                             |

## Find Detections

The Find Detections action adds a tag to a device in CrowdStrike Insight EDR.

GET <https://api.crowdstrike.com/detects/queries/detects/v1>

**Sample Response:**

```
{
  "meta": {
    "query_time": 0.016146192,
    "pagination": {
      "offset": 0,
      "limit": 100,
      "total": 0
    },
    "powered_by": "msa-api",
    "trace_id": "f201ae68-7104-4d90-8279-19f40125c1d8"
  },
  "resources": [
    "<id>",
    "<id2>"
  ],
  "errors": []
}
```

POST <https://api.crowdstrike.com/detects/entities/summaries/GET/v1>

**POST Body:**

```
{
  "ids": ["<id>", "<id2>"]
}
```

**Response:**

```
{
  "meta": {
    "query_time": 0.016374054,
    "powered_by": "msa-api",
    "trace_id": "08a7c526-0fcc-44c0-bf8d-368b3a661cd7"
  },
  "resources": [
    {
      "cid": "e5d4a79a091448bfb80afc724b3cf952",
      "created_timestamp": "2021-08-31T00:20:57.828992776Z",
      "detection_id": "ldt:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
      "device": {
        "device_id": "4c3db6145a704a179a6dacd924f6e8cc",
        "cid": "e5d4a79a091448bfb80afc724b3cf952",
        "agent_load_flags": "0",
        "agent_local_time": "2021-08-12T12:08:19.328Z",

```



```

    "agent_version": "6.27.14105.0",
    "bios_manufacturer": "Xen",
    "bios_version": "4.2.amazon",
    "config_id_base": "65994753",
    "config_id_build": "14105",
    "config_id_platform": "3",
    "external_ip": "54.89.138.42",
    "hostname": "WIN10DETECTION",
    "first_seen": "2021-02-09T16:06:00Z",
    "last_seen": "2021-08-31T00:08:11Z",
    "local_ip": "172.17.0.31",
    "mac_address": "02-7d-30-2b-bc-f7",
    "machine_domain": "csanfr.local",
    "major_version": "10",
    "minor_version": "0",
    "os_version": "Windows 10",
    "platform_id": "0",
    "platform_name": "Windows",
    "product_type": "1",
    "product_type_desc": "Workstation",
    "site_name": "Default-First-Site-Name",
    "status": "normal",
    "system_manufacturer": "Xen",
    "system_product_name": "HVM domU",
    "groups": [
        "47582c7801a4431e8d81d85aae570cd4"
    ],
    "modified_timestamp": "2021-08-31T00:10:03Z",
    "instance_id": "i-084e546a6695e1412",
    "service_provider": "AWS_EC2",
    "service_provider_account_id": "390847698897"
  },
  "behaviors": [
    {
      "device_id": "4c3db6145a704a179a6dacd924f6e8cc",
      "timestamp": "2021-08-31T00:20:17Z",
      "behavior_id": "5702",
      "filename": "runningdiskpartmg16.exe",
      "filepath": "\\Device\\HarddiskVolume2\\Users\\demo\\
\\Desktop\\Malware\\runningdiskpartmg16.exe",
      "alleged_filetype": "exe",
      "cmdline": "c:\\Users\\demo\\Desktop\\Malware\\
\\runningdiskpartmg16.exe -k",
      "scenario": "NGAV",
      "objective": "Falcon Detection Method",
      "tactic": "Machine Learning",
      "tactic_id": "CSTA0004",
      "technique": "Sensor-based ML",
      "technique_id": "CST0007",
      "display_name": ""
    }
  ]

```

```

        "description": "This file meets the machine learning-based
on-sensor AV protection's high confidence threshold for malicious files.",
        "severity": 70,
        "confidence": 70,
        "ioc_type": "hash_sha256",
        "ioc_value":
"4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
        "ioc_source": "library_load",
        "ioc_description": "\\Device\\HarddiskVolume2\\Users\\demo\\
\\Desktop\\Malware\\runningdiskpartmg16.exe",
        "user_name": "WIN10DETECTION$",
        "user_id": "S-1-5-18",
        "control_graph_id":
"ctg:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
        "triggering_process_graph_id":
"pid:4c3db6145a704a179a6dacd924f6e8cc:656468848626",
        "sha256":
"4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
        "md5": "d1c27ee7ce18675974edf42d4eea25c6",
        "parent_details": {
            "parent_sha256":
"9077b1aa0afb8db329fded0e51085de1c51b22a986162f29037fca404a80d512",
            "parent_md5": "",
            "parent_cmdline": "C:\\Windows\\system32\\
\\services.exe",
            "parent_process_graph_id":
"pid:4c3db6145a704a179a6dacd924f6e8cc:476751454426"
        },
        "pattern_disposition": 2304,
        "pattern_disposition_details": {
            "indicator": false,
            "detect": false,
            "inddet_mask": false,
            "sensor_only": false,
            "rooting": false,
            "kill_process": false,
            "kill_subprocess": false,
            "quarantine_machine": false,
            "quarantine_file": false,
            "policy_disabled": true,
            "kill_parent": false,
            "operation_blocked": false,
            "process_blocked": true,
            "registry_operation_blocked": false,
            "critical_process_disabled": false,
            "bootup_safeguard_enabled": false,
            "fs_operation_blocked": false,
            "handle_operation_downgraded": false,
            "kill_action_failed": false,
            "blocking_unsupported_or_disabled": false,

```

```

        "suspend_process": false,
        "suspend_parent": false
    }
},
"email_sent": true,
"first_behavior": "2021-08-31T00:20:17Z",
"last_behavior": "2021-08-31T00:20:18Z",
"max_confidence": 70,
"max_severity": 70,
"max_severity_displayname": "High",
"show_in_ui": true,
"status": "new",
"hostinfo": {
    "domain": ""
},
"seconds_to_triaged": 0,
"seconds_to_resolved": 0,
"behaviors_processed": [
    "pid:4c3db6145a704a179a6dacd924f6e8cc:656471670052:5702"
]
}
]
}

```

## Parameters

ThreatQ provides the following parameter for this Action:

| PARAMETER | DESCRIPTION                                                                                                                                                                                                                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timeframe | <ul style="list-style-type: none"><li>• Select a timeframe to look for detections within<ul style="list-style-type: none"><li>◦ 1 Day</li><li>◦ 3 Days</li><li>◦ 7 Days (Default)</li><li>◦ 1 Month</li><li>◦ 3 Months</li><li>◦ 6 Months</li><li>◦ 1 Year</li><li>◦ No Timeframe</li></ul></li></ul> |

## Action Mapping

ThreatQ provides the following default mapping for this action:



All mappings are based on each item within the resources list in the API response.

| FEED DATA PATH                | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|-------------------------------|-----------------|--------------------------------------|----------------|----------|-------|
| .detection_id                 | Attribute       | CrowdStrike Detection ID             | N/A            | N/A      | N/A   |
| .email_sent                   | Attribute       | Email Sent                           | N/A            | N/A      | N/A   |
| .max_severity                 | Attribute       | Max Severity                         | N/A            | N/A      | N/A   |
| .max_severity_displayname     | Attribute       | Severity                             | N/A            | N/A      | N/A   |
| .max_confidence               | Attribute       | Max Confidence                       | N/A            | N/A      | N/A   |
| .status                       | Attribute       | Detection Status                     | N/A            | N/A      | N/A   |
| .first_behavior               | Attribute       | First Behavior                       | N/A            | N/A      | N/A   |
| .last_behavior                | Attribute       | Last Behavior                        | N/A            | N/A      | N/A   |
| .seconds_to_triaged           | Attribute       | Seconds to Triaged                   | N/A            | N/A      | N/A   |
| .seconds_to_resolved          | Attribute       | Seconds to Resolved                  | N/A            | N/A      | N/A   |
| .device.device_id             | Attribute       | CrowdStrike Device ID                | N/A            | N/A      | N/A   |
| .device.external_ip           | Attribute       | Device External IP Address           | N/A            | N/A      | N/A   |
| .device.local_ip              | Attribute       | Device IP Address                    | N/A            | N/A      | N/A   |
| .device.hostname              | Attribute       | Device Hostname                      | N/A            | N/A      | N/A   |
| .device.machine_domain        | Attribute       | Device Domain                        | N/A            | N/A      | N/A   |
| .device.os_version            | Attribute       | Device Operating System              | N/A            | N/A      | N/A   |
| .device.hoststatusname        | Attribute       | Device Status                        | N/A            | N/A      | N/A   |
| .behaviors[].filename         | Indicator Value | Filename                             | N/A            | N/A      | N/A   |
| .behaviors[].filepath         | Indicator Value | File Path                            | N/A            | N/A      | N/A   |
| .behaviors[].md5              | Indicator Value | MD5                                  | N/A            | N/A      | N/A   |
| .behaviors[].sha256           | Indicator Value | SHA-256                              | N/A            | N/A      | N/A   |
| .behaviors[].severity         | Attribute       | Severity                             | N/A            | N/A      | N/A   |
| .behaviors[].confidence       | Attribute       | Confidence                           | N/A            | N/A      | N/A   |
| .behaviors[].ioc_source       | Attribute       | IOC Source                           | N/A            | N/A      | N/A   |
| .behaviors[].ioc_description  | Attribute       | IOC Description                      | N/A            | N/A      | N/A   |
| .behaviors[].user_name        | Attribute       | Affected User                        | N/A            | N/A      | N/A   |
| .behaviors[].alleged_filetype | Attribute       | Alleged File Type                    | N/A            | N/A      | N/A   |
| .behaviors[].scenario         | Attribute       | Detection Scenario                   | N/A            | N/A      | N/A   |
| .behaviors[].tactic           | Attribute       | Detection Tactic                     | N/A            | N/A      | N/A   |
| .behaviors[].technique        | Attribute       | Detection Technique                  | N/A            | N/A      | N/A   |
| .behaviors[].description      | Attribute       | Behavior Description                 | N/A            | N/A      | N/A   |

---

| FEED DATA PATH       | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|----------------------|----------------|--------------------------------------|----------------|----------|-------|
| .behaviors[].cmdline | Attribute      | Executed Command                     | N/A            | N/A      | N/A   |

# Change Log

- **Version 1.2.1 rev-a**
  - Guide Update - added a new Prerequisites section to the guide.
- **Version 1.2.1**
  - Replaced the **API Host Name** configuration field with a new **CrowdStrike Host** field. This allows you to type in your CrowdStrike Host opposed to selecting from a pre-defined dropdown.
- **Version 1.2.0**
  - Added a new action, **Create Hash Policy**, for MD5 and SHA-256 type indicators, that provides you with two additional policy options:
    - **Prevent** - Block the IOC and show it as a detection at the selected severity
    - **Allow** - Allow the IOC but do not detect it
- **Version 1.1.0**
  - Added **API Host** configuration option.
  - Updated the API endpoint, which has been deprecated, for the **Create Policy** action.
  - Added **Platforms** and **Severity** configuration options for the **Create Policy** action.
  - Resolved a conversion issue with the **Find Detections** action.
  - Updated Support Tier from **Not Actively Support** to **ThreatQ Supported**.
- **Version 1.0.0**
  - Initial release