

ThreatQuotient



CrowdStrike Falcon X Sandbox CDF User Guide

Version 1.1.2

August 01, 2023

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

Installation..... 7

Configuration 8

ThreatQ Mapping..... 9

 Falcon X Sandbox..... 9

 Falcon X Details (Supplemental) 10

Average Feed Run..... 14

 Falcon X Sandbox..... 14

Change Log 15

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 © 2023 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	1.1.2
Compatible with ThreatQ Versions	>= 4.43.0
Support Tier	ThreatQ Supported

Introduction

The CrowdStrike Falcon X Sandbox CDF ingests Reports, Indicators, Signatures, Malware and Attack Pattern objects based on submissions via the **CrowdStrike Falcon X Sandbox Operation**.

The integration provides the following feeds:

- **Falcon X Sandbox** - retrieves report ids which will further on be used in the Falcon X Details supplemental feed.
- **Falcon X Details (supplemental)** - called once per each report id returned by the Falcon X Sandbox feed.

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 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 feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

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 **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:



Confirm that you are using the same Host/Credentials for both this feed and its operation counterpart - CrowdStrike Falcon X Sandbox Operation.

PARAMETER

DESCRIPTION

API Hostname

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

The CrowdStrike Falcon X Client ID used for authentication.

Client Secret

The CrowdStrike Falcon X Secret used for authentication.

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.

ThreatQ Mapping

Falcon X Sandbox

The Falcon X Sandbox is the main feed used to retrieve report ids which will further on be used in the Falcon X Details supplemental feed.

GET <https://{HOST}/falconx/queries/reports/v1>

Sample Response:

```
{
  "meta": {
    "query_time": 0.008275485,
    "pagination": {
      "offset": 0,
      "limit": 10,
      "total": 86
    },
    "powered_by": "falconx-api",
    "trace_id": "02ac753f-e7a5-4d39-a339-ca9080d94860",
    "quota": {
      "total": 100,
      "used": 0,
      "in_progress": 0
    }
  },
  "resources": [
    "ace79a13936f4ec8ad4de36606814bfc_e332f0252af143b89ad44b973c05124b",
    "ace79a13936f4ec8ad4de36606814bfc_43d809df175f4ff9aa4fe47b2e1d3759",
    "ace79a13936f4ec8ad4de36606814bfc_f0f165f79cb4486f8ee0013a82221de5",
    "ace79a13936f4ec8ad4de36606814bfc_0b8a0f0ea902457ca8902afa26c0fa8d",
    "ace79a13936f4ec8ad4de36606814bfc_8815c0c3180d42b18dd202fe5182e757",
    "ace79a13936f4ec8ad4de36606814bfc_133535ec09784a7ea19b155aa1092b77",
    "ace79a13936f4ec8ad4de36606814bfc_cca86b85a5804038826880ac749d3274",
    "ace79a13936f4ec8ad4de36606814bfc_f325aac08bb1415ea0e5fbd35b7dbb39",
    "ace79a13936f4ec8ad4de36606814bfc_bcd04c21f18a44a39a4c44c1cca4a830",
    "ace79a13936f4ec8ad4de36606814bfc_eebc849ccc8646fba61f1580eeb384ec"
  ],
  "errors": []
}
```

Falcon X Details (Supplemental)

The Falcon X Details is the supplemental feed called once per each report id returned by the Falcon X Sandbox feed.

GET <https://{HOST}/falconx/queries/reports/v1>

Sample Response:

```
{
  "meta": {
    "query_time": 0.008275485,
    "pagination": {
      "offset": 0,
      "limit": 10,
      "total": 86
    },
    "powered_by": "falconx-api",
    "trace_id": "02ac753f-e7a5-4d39-a339-ca9080d94860",
    "quota": {
      "total": 100,
      "used": 0,
      "in_progress": 0
    }
  },
  "resources": [
    "ace79a13936f4ec8ad4de36606814bfc_e332f0252af143b89ad44b973c05124b",
    "ace79a13936f4ec8ad4de36606814bfc_43d809df175f4ff9aa4fe47b2e1d3759",
    "ace79a13936f4ec8ad4de36606814bfc_f0f165f79cb4486f8ee0013a82221de5",
    "ace79a13936f4ec8ad4de36606814bfc_0b8a0f0ea902457ca8902afa26c0fa8d",
    "ace79a13936f4ec8ad4de36606814bfc_8815c0c3180d42b18dd202fe5182e757",
    "ace79a13936f4ec8ad4de36606814bfc_133535ec09784a7ea19b155aa1092b77",
    "ace79a13936f4ec8ad4de36606814bfc_cca86b85a5804038826880ac749d3274",
    "ace79a13936f4ec8ad4de36606814bfc_f325aac08bb1415ea0e5fbd35b7dbb39",
    "ace79a13936f4ec8ad4de36606814bfc_bcd04c21f18a44a39a4c44c1cca4a830",
    "ace79a13936f4ec8ad4de36606814bfc_eebc849ccc8646fba61f1580eeb384ec"
  ],
  "errors": []
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
resources[].sandbox[].submit_name	Report.Name	N/A	'malware-ransom-cerber'	To create the Report Name we add 'Falcon X Report' before the key ('Falcon X Report malware-ransom-cerber').
resources[].created_timestamp	Report.published_at	N/A	'2020-09-25T17:12:55Z'	
resources[].sandbox[].sha256	Related.Indicator	SHA-256	'b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66'	
resources[].sandbox[].environment_description	Report.Attribute	Environment Description	'Windows 7 64 bit'	
resources[].sandbox[].file_size	Report.Attribute	File Size	'218112'	
resources[].sandbox[].file_type	Report.Attribute	File Type	'PE32 executable (GUI) Intel 80386, for MS Windows'	
resources[].sandbox[].file_type_short[]	Report.Attribute	File Type Short	'peexe'	
resources[].sandbox[].submission_type	Report.Attribute	Submission Type	'file'	
resources[].sandbox[].verdict	Report.Attribute	Verdict	'malicious'	
resources[].sandbox[].threat_score	Report.Attribute	Threat Score	'61'	
resources[].sandbox[].incidents[].name	Report.Attribute	Incident Name	'Fingerprint'	
resources[].sandbox[].incidents[].details	Report.Attribute	Incident Detail	'Reads the active computer name'	
resources[].sandbox[].classification[]	Report.Attribute	Classification	'"61.7% (.EXE) Win64 Executable (generic)'"	
resources[].sandbox[].contacted_hosts[].country	Report.Attribute and Related Indicator.Attribute	Host Country	'United States'	
resources[].sandbox[].contacted_hosts[].address	Related Indicator	IP Address	'54.214.246.97'	
resources[].sandbox[].contacted_hosts[].port	Related Indicator.Attribute	Port	'80'	
resources[].sandbox[].contacted_hosts[].protocol	Related Indicator.Attribute	Protocol	'TCP'	
resources[].sandbox[].contacted_hosts.associated_runtime.name	Related Indicator.Indicator	Filename	'malware-ransom-cerber.exe'	
resources[].sandbox[].extracted_interesting_strings[].filename	Related Indicator	Filename	'b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66.bin'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
resources[].sandbox[].extracted_interesting_strings[].process	Related Indicator	Filename	'malware-ransom-cerber.exe'	
resources[].sandbox[].signatures.name	Related Signature.Name	Custom	'Creates mutants'	
resources[].sandbox[].signatures.description	Related Signature.Value and Related Signature.Description	N/A	""\Sessions\1\BaseNamedObjects\DBWinMutex"\n "DBWinMutex"	
resources[].sandbox[].signatures.category	Related Signature.Attribute	Category	'General'	
resources[].sandbox[].signatures.identifier	Related Signature.Attribute	Identifier	'mutant-0'	
resources[].sandbox[].signatures.type	Related Signature.Attribute	Type	'4'	
resources[].sandbox[].signatures.relevance	Related Signature.Attribute	Relevance	'3'	
resources[].sandbox[].signatures.origin	Related Signature.Attribute	Origin	'Created Mutant'	
resources[].sandbox[].processes.name	Related Indicator	Filename	'malware-ransom-cerber.exe'	
resources[].sandbox[].processes.process_flags[].name	Related Indicator.Attribute	Name	'Network Activity'	
resources[].sandbox[].processes.sha256	Related Indicator.Indicator	SHA-256	'b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66'	
resources[].sandbox[].processes.registry[].path	Related Indicator.Registry	Registry Key	'HKLM\SYSTEM\CONTROLSET001\CONTROL\MUI\UILANGUAGES\EN-US\TYPE'	
resources[].sandbox[].processes.registry[].key	Related Indicator.Registry.Attribute	Key	'TYPE'	
resources[].sandbox[].processes.registry[].value	Related Indicator.Registry.Attribute	Value	'00000000040000000400000091000000'	
resources[].sandbox[].processes.file_accesses[].path	Related Indicator.Indicator	File Path	'\DEVICE\NETBT_TCPIP_{C3450F58-7060-4AEA-B0A0-C245927D78D0}'	
resources[].sandbox[].mitre_attacks[].attack_id	Related Attack_pattern	Attack Pattern	'T1179'	
resources[].malquery[].resources[].family	Related Malware	Malware	'Adload'	
resources[].malquery[].resources[].file_size	Related Malware.Attribute	File Size	'245248'	
resources[].malquery[].resources[].file_type	Related Malware.Attribute	File Type	'PE32'	
resources[].malquery[].input	Related Malware.Indicator	SHA-256 or URL	'b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66'	Type determined based on 'type'.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
resources[].malquery[].resources[].sha256	Related Malware.Indicator	SHA-256	'89fd45344d44ebf2062a5c7052f1293a0d1ae148818528cd64ab63914c3d8e71'	
resources[].malquery[].resources[].md5	Related Malware.Indicator	MD5	'054973ed2d69bdc969ff018e3bb3d610'	
resources[].malquery[].resources[].sha1	Related Malware.Indicator	SHA-1	'5583c5c0435dae9807966294ac8809d32c3a9fbb'	
resources[].threat_graph.indicators[].value	Related Indicator	SHA-256	'b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66'	

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Falcon X Sandbox

METRIC	RESULT
Run Time	6 minutes
Reports	41
Report Attributes	530
Indicators	2,104
Indicator Attributes	1,261
Attack Patterns	15
Malware	15
Malware Attributes	91
Signatures	329
Signature Attributes	1,597

Change Log

- **Version 1.1.2**
 - Updated the CDF to only ingest response data that has been submitted by the **CrowdStrike Falcon X Sandbox Operation**, which is identified by the **submit_name** attribute.
- **Version 1.1.1**
 - Updated the **API Host** configuration parameter to function as dropdown option.
- **Version 1.1.0**
 - Added a new **API Host** configuration parameter that will allow you to enter a CrowdStrike host. See step 4 in the [Configuration](#) chapter for more information.
- **Version 1.0.0**
 - Initial release