ThreatQuotient

VMware CB Cloud Enterprise EDR CDF User Guide

Version 1.0.1

October 18, 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

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	1.0.1
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

VMWare Carbon Black Cloud Enterprise EDR ingests threat intelligence data from the following endpoint:

- `https://defense.conferdeploy.net/threathunter/feedsearch/v1/orgs/ {{org_id}}/search`

An Organization ID, API ID and API Secret Key are used for HTTP authentication (in the `X-Auth-Token` HTTP Header).

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:

PARAMETER	DESCRIPTION
Carbon Black Hostname	VMWare CB Cloud Enterprise EDR hostname.
ORG ID	VMWare CB Cloud Enterprise EDR account Organization ID.
API ID	VMWare CB Cloud Enterprise EDR account API ID.
API Secret Key	VMWare CB Cloud Enterprise EDR account API secret key.

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

VMWare CB Enterprise EDR Reports

Sample Response:


```
{
    "took": 1,
    "timed_out": false,
    "hits": {
        "total": 1,
        "max_score": null,
        "hits": [
            {
                "_index": "report_index-2018.11.17-1",
                "_type": "_doc",
                "_id": "0FbiTt9eQKWQqjh0viwqA",
                "_score": null,
                "_source": {
                    "severity": 8,
                    "access": "private",
                    "iocs": [
                        {
                            "field": "process_hash",
                            "values": [
                                "7c3d70d49af6e4c7b4aad3623fdcf65b"
                            ],
                            "link": null,
                            "match_type": "equality",
                            "id": "c6ee778750efb8f5493975197548cfc6"
                        }
                    ],
                    "link": "https://ui.threatstream.com/detail/
7c3d70d49af6e4c7b4aad3623fdcf65b",
                    "description": "7c3d70d49af6e4c7b4aad3623fdcf65b was first
seen on 2020-01-30T13:37:38, and last updated on 2020-01-30T13:37:38",
                    "title": "itype=mal_md5, source=iDefense test campaign -
Richard",
                    "tags": [
                        "FD-4304 - CrowdStrike IoC - iMcD",
                        "apt_domain"
                    ],
                    "source_label": "Custom",
                    "id": "0FbiTt9eQKWQqjh0viwqA",
                    "timestamp": 1580391458,
                   "feed": {
                        "feed_category": "Partner",
```

```
                        "feed_summary": "Sample threatstream feed to group
reports by id",
                        "feed_id": "0FbiTt9eQKWQqjh0viwqA",
                        "feed_name": "ThreatStream_ID",
                        "feed_provider_url": "https://ui.threatstream.com"
                    },
                    "telemetry": {
                        "global_hit_rate_1d": 0,
                        "global_hit_rate_1w": 0
                    }
                },
                "sort": [
                    "0FbiTt9eQKWQqjh0viwqA"
                ]
            }
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.link	report.attribute	Link	"https://ui.threatstream.com/detail/7c3d70d49af6e4c7b4aad3623fdcf65b"		
.title	report.value	Report Title	"itype=mal_md5, source=iDefense test campaign - Richard"		
.id	report.attribute	ID	"1237abc7bca7356566677ac"		
.description	report.description	Report Description	"3d70d49af6e4c7b4aad3623fdcf65b was first seen on 2020-01-30T13:37:38 ..."		
.tags	report.attribute, indicator.attribute	Tag	["FD-4304 - CrowdStrike IoC - iMcD", "apt_domain"]		
.access	report.attribute, indicator.attribute	Access			
.severity	report.attribute, indicator.attribute	Severity	8		
.source_label	report.attribute, indicator.attribute	Source Label	"Custom"		
.feed.feed_category	report.attribute, indicator.attribute	Feed Category	"Comercial"		
.timestamp	report.published_at, indicator.published_at	Report Published At, Indicator Published At	"2020-10-01 12:12:12"		
.feed.feed_summary	report.attribute, indicator.attribute	Feed Summary	" Sample threatstream feed to group reports by id"		
.feed.feed_id	report.attribute, indicator.attribute	Feed Id	"12121"		
.feed.feed_name	report.attribute, indicator.attribute	Feed Name	"ThreatStream_ID"		
.feed.feed_provider_url	report.attribute, indicator.attribute	Feed Provider Url	"http://ui.threat.com"		
.iocs[].link	indicator.attribute	Link	null		
.iocs[].id	indicator.attribute	Id	"c6ee778750efb8f5493975197548cfc6"		
.iocs[].match_type	indicator.attribute	Match Type	"equality"		
.iocs[].values	indicator.value	Indicator Value	["7c3d70d49af6e4c7b4aad3623fdcf65b", "7c3d70d49af6e4c7b4aad3623fdcf35b"]		
.iocs[].field	indicator.type	Indicator Type	"MD5" / "IPv4" / "FQDN"		
.telemetry.global_hit_rate_1w	report.attribute, indicator.attribute	Global Hit Rate 1w	0		
.telemetry.global_hit_rate_1d	report.attribute, indicator.attribute	Global Hit Rate 1d	0		

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.

VMWare Carbon Black Cloud Enterprise EDR

METRIC	RESULT
Run Time	45 minutes
Indicators	21,304
Indicator Attributes	24,200
Reports	7,492
Report Attributes	89,923V

Change Log

- **Version 1.0.1**
  - Technical Improvements
- **Version 1.0.0**
  - Initial release