ThreatQuotient

VMware Carbon Black Cloud Enterprise EDR Guide

Version 1.0.0

Monday, April 20, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Monday, April 20, 2020

Contents

Versioning

- Current Integration Version: `1.0.0`
- Supported on ThreatQ Version: >= `4.34.0`

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 feed:

The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **VMware Carbon Black Cloud Enterprise EDR** feed file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

   The feed will be added to the **Commercial** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
Carbon Black Host-name	VMware CB Cloud Enterprise EDR host-name.
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. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable it.

ThreatQ Mapping

VMware CB Enterprise EDR Reports

JSON response sample


```
{
    "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/7c3d70d49af6e4c7b4aad3623f
dcf65b",
                    "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"
                ]
            }
        ]
    }
}
```

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
.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	"Custom"
.severity	report.attribute, indicator.attribute	Severity	
.source_label	report.attribute, indicator.attribute	Source Label	
.feed.feed_category	report.attribute, indicator.attribute	Feed Category	"Comercial"

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
.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"

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
.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

Metric	Result
Run Time (per 1 day)	45 minutes
Indicators	21304
Indicator Attributes	242000
Reports	7492
Report Attributes	89923

Change Log

- **Version 1.0.0**
  - Initial Release