# ThreatQuotient

# VMware Carbon Black EDR CDF

**Version 1.0.0**

April 01, 2024

**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 ... 10
VMware Carbon Black EDR ... 10
Average Feed Run ... 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.

# 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** | >= 5.20.0 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The VMware Carbon Black EDR CDF for ThreatQ enables the automatic ingestion of Triage Alerts from VMware Carbon Black EDR into the ThreatQ platform.

The integration provides the following feed:

- **VMware Carbon Black EDR -** enables the automatic ingestion of Triage Alerts.

The integration ingests the following system objects:

- Assets
- Events
- Indicators

# 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 yaml 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 yaml file into the dialog box
    - Select **Click to Browse** to locate the integration yaml 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. 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.

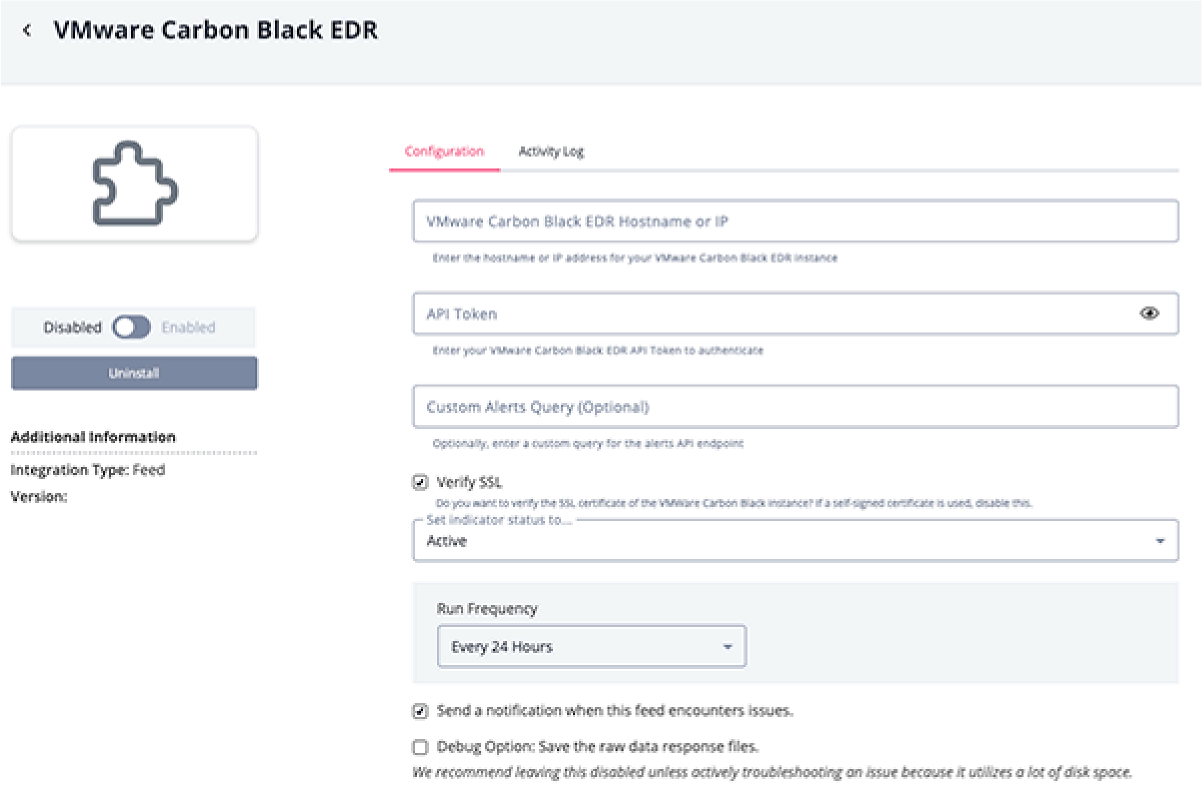
To configure the integration:

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 |
|---|---|
| **VMware Carbon Black EDR Hostname or IP** | Enter the hostname or IP address for your VMware Carbon Black EDR instance. |
| **API Token** | Enter your VMware Carbon Black EDR API Token to authenticate. |
| **Custom Alerts Query** | Optional - enter a custom query for the alerts API endpoint. |
| **Verify SSL** | Enable/Disable the Verify SSL feature.  This option should be disabled if you are using a self-signed certificate. |



VMware Carbon Black EDR

Disabled ○ Enabled

Uninstall

**Additional Information**

Integration Type: Feed

Version:

Configuration | Activity Log

VMware Carbon Black EDR Hostname or IP

Enter the hostname or IP address for your VMware Carbon Black EDR instance

API Token

Enter your VMware Carbon Black EDR API Token to authenticate

Custom Alerts Query (Optional)

Optionally, enter a custom query for the alerts API endpoint

☑ Verify SSL

Do you want to verify the SSL certificate of the VMware Carbon Black instance? If a self-signed certificate is used, disable this.

Set indicator status to...: Active

Run Frequency: Every 24 Hours

☑ Send a notification when this feed encounters issues.

□ Debug Option: Save the raw data response files.

*We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.*

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 Carbon Black EDR

The VMware Carbon Black EDR feed automatically ingests triage alerts and context from VMware Carbon Black EDR into the ThreatQ platform.

`GET https://{host_or_ip}/api/v2/alert`

**Sample Response:**

```
{
    "results": [
        {
            "unique_id": "ae524e9e-7ef4-42cc-a78e-295e902771cb",
            "created_time": "2021-12-09T20:20:31.477Z",
            "alert_type": "watchlist.hit.ingress.process",
            "status": "Unresolved",
            "sensor_criticality": 3,
            "feed_rating": 3,
            "ioc_confidence": 0.5,
            "report_score": 100,
            "os_type": "windows",
            "username": "DESKTOP-RIS67BS\\Admin",
            "process_name": "curl.exe",
            "process_path": "c:\\windows\\system32\\curl.exe",
            "modload_count": 14,
            "filemod_count": 0,
            "regmod_count": 0,
            "netconn_count": 1,
            "childproc_count": 0,
            "crossproc_count": 1,
            "md5": "1c3645ebddbe2da6a32a5f9fb43a3c23",
            "sha256":
"0ba1c44d0ee5b34b45b449074cda51624150dc16b3b3c38251df6c052adba205",
            "process_unique_id": "00000003-0000-2640-01d7-
ed3a0d3d7414-017da0dac3ea",
            "feed_name": "abusech",
            "feed_id": 10,
            "watchlist_name": "feodoipblocklist",
            "watchlist_id": "feodoipblocklist",
            "ioc_type": "ipv4",
            "ioc_value": "158.69.118.130",
            "ioc_attr": "{\"local_ip\":\"-1062727933\",\"protocol\":\"TCP\",
\"remote_ip\":\"-1639614846\",\"port\":\"49927\",\"local_port\":\"49927\",
\"remote_port\":\"80\",\"direction\":\"Outbound\"}",
            "process_id": "00000003-0000-2640-01d7-ed3a0d3d7414",
            "segment_id": 1639081231338,
            "hostname": "desktop-ris67bs",
            "group": "default group",
            "sensor_id": 3,
            "comms_ip": "10.13.0.1",
            "interface_ip": "192.168.15.3",
            "alert_severity": 67.5,
            "_version_": 1718701241451675600,
            "total_hosts": 0,
            "description": "Feodo IP Blocklist",
            "link": "https://feodotracker.abuse.ch/downloads/ipblocklist.csv",
            "report_ignored": false
        }
    ],
    "facets": {},
    "filtered": {},
    "highlights": [],
    "elapsed": 0.016037702560424805,
    "start": 0,
    "total_results": 10,
    "terms": [
        "created_time:[2021-12-01T22:15:00 TO 2021-12-09T23:00:00]"
    ],
    "all_segments": true,
    "comprehensive_search": true,
    "incomplete_results": false
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].ioc_confidence` | Indicator/ Event.Attribute | IOC Confidence | `results[].created_time` | 0.5 | N/A |
| `results[].ioc_type` | Indicator/ Event.Attribute | IOC Type | `results[].created_time` | ipv4 | N/A |
| `results[].report_score` | Indicator/ Event.Attribute | Report Score | `results[].created_time` | 100 | N/A |
| `results[].[process_id/ segment_id]` | Indicator/ Event.Attribute | Process Link | `results[].created_time` | https://{host}/#/analyze/00000003-0000-2640-01d7-ed3a0d3d7414/1639081231338 | Keys are concatenated together to form the link |
| `results[].interface_ip` | Asset.Attribute | IP Address | `results[].created_time` | 192.168.15.3 | For Assets Only |
| `results[].comms_ip` | Asset.Attribute | Comms IP Address | `results[].created_time` | 10.13.0.1 | For Assets Only |
| `results[].os_type` | Asset.Attribute | Operating System | `results[].created_time` | windows | For Assets Only |
| `results[].hostname` | Asset.Attribute | Hostname | `results[].created_time` | desktop-ris67bs | For Assets Only |
| `results[].group` | Asset.Attribute | Host Group | `results[].created_time` | default group | For Assets Only |
| `results[].sensor_criticality` | Asset.Attribute | Host Criticality | `results[].created_time` | 3 | For Assets Only |
| `results[].alert_severity` | Event.Attribute | Severity | `results[].created_time` | 67.5 | For Events Only |
| `results[].alert_type` | Event.Attribute | Alert Type | `results[].created_time` | watchlist.hit.ingress.process | For Events Only |
| `results[].status` | Event.Attribute | Status | `results[].created_time` | Unresolved | For Events Only |
| `results[].feed_name` | Event.Attribute | Feed Name | `results[].created_time` | abusech | For Events Only |
| `results[].feed_rating` | Event.Attribute | Feed Rating | `results[].created_time` | 3 | For Events Only |
| `results[].watchlist_name` | Event.Attribute | Watchlist Name | `results[].created_time` | feodoipblocklist | For Events Only |
| `results[].netconn_count` | Event.Attribute | Network Connections | `results[].created_time` | 1 | For Events Only |
| `results[].md5` | Related Indicator.Value | MD5 | `results[].created_time` | 1c3645ebddbe2da6a32a5f9fb43a3c23 | Added with the Review Status |
| `results[].sha256` | Related Indicator.Value | SHA-256 | `results[].created_time` | 0ba1c44d0ee5b34b45b449074cda51624150dc16b3b3c38251df6c052adba205 | Added with the Review Status |
| `results[].process_name` | Related Indicator.Value | Filename | `results[].created_time` | curl.exe | Added with the Review Status |
| `results[].process_path` | Related Indicator.Value | File Path | `results[].created_time` | c:\windows\system32\curl.exe | Added with the Review Status |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| `results[].ioc_value` | Related Indicator.Value | Based on `data.ioc_type` | `results[].created_time` | 158.69.118.130 | N/A |
| `results[].username` | Related Indicator.Value | Username | `results[].created_time` | DESKTOP-RIS67BS\ Admin | N/A |
| `results[].[hostname/interface_ip]` | Related Asset.Value | N/A | `results[].created_time` | desktop-ris67bs<br>192.168.15.3 | N/A |
| `results[].[process_name/alert_type / hostname / watchlist_name / alert_severity /unique_id]` | Event.Title | Alert | `results[].created_time` | Process curl.exe triggered a watchlist hit ingress process alert on host desktop-ris67bs | Keys are concatenated together, conditionally |
| `results[].ioc_attr` | Event.Description | N/A | `results[].created_time` | N/A | Concatenated to form HTML & JSON Prettified |

# 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.

| METRIC | RESULT |
|---|---|
| **Run Time** | 1 minute |
| **Asset** | 1 |
| **Asset Attributes** | 6 |
| **Events** | 10 |
| **Event Attributes** | 110 |
| **Indicators** | 15 |
| **Indicator Attributes** | 72 |

# Change Log

- **Version 1.0.0**
  - Initial release