ThreatQuotient

A Securonix Company

VMware CB Cloud Platform Alerts CDF

Version 2.0.0

July 20, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	2.0.0
Compatible with ThreatQ Versions	>= 4.25.0
Support Tier	ThreatQ Supported

Introduction

The **VMware Carbon Black Cloud Platform Alerts CDF** enables ThreatQ to ingest Carbon Black Cloud Platform v7 alerts directly into ThreatQ as Incident objects. During ingestion, the integration automatically extracts and relates associated indicators, MITRE ATT&CK attack patterns, and TTPs, providing analysts with enriched context to support investigation and response.

The integration provides the following feed:

- **VMWare Carbon Black Cloud Platform Alerts** - ingests VMware Carbon Black Cloud alerts as Incident objects and automatically extracts and relates associated indicators, MITRE ATT&CK attack patterns, and TTPs within ThreatQ.

The integration ingests the following system objects:

- Attack Patterns
- Incidents
  - Incident Attributes
- Indicators
  - Indicators Attributes
- TTPs

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. 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 Cloud Platform API Host	Enter the FQDN for your Carbon Black Cloud Platform instance (i.e., without protocol).
Organization Key	Your Organization Key, as displayed in the Carbon Black Cloud Platform instance.
API Key	Your API ID, as displayed in the Carbon Black Cloud Platform instance.
API Secret Key	Your API Secret Key, as displayed in the Carbon Black Cloud Platform instance.
Query	An optional Carbon Black search query to filter the incoming alerts. See the Carbon Black documentation for information on how to write a Carbon Black query.
Minimum Severity	The minimum severity for an alert to be ingested in ThreatQ.

PARAMETER	DESCRIPTION
Target Values	One or more target values to filter the incoming alerts.
Categories	One or more categories to filter the incoming alerts.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

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 Cloud Platform Alerts

The VMware Carbon Black Cloud Platform Alerts feed ingests alerts from a VMware Carbon Black Cloud instance as Incident objects in ThreatQ and automatically extracts and relates associated indicators, MITRE ATT&CK attack patterns, and TTPs to provide enriched investigative context.

```
POST https://{{user_fields.api_host}}/api/alerts/v7/orgs/
{{user_fields.org_key}}/alerts/_search
```

Sample Response:


```
{
    "num_found": 133,
    "num_available": 133,
    "results": [
        {
            "org_key": "7DESJ9GN",
            "alert_url": "https://defense.conferdeploy.net/alerts?
s[c][query_string]=id:2c80295b-794c-11f1-9582-02e2b52abb6d",
            "id": "2c80295b-794c-11f1-9582-02e2b52abb6d",
            "type": "CB_ANALYTICS",
            "first_event_timestamp": "2026-07-09T09:25:35.000Z",
            "last_event_timestamp": "2026-07-09T09:25:35.000Z",
            "severity": 3,
            "reason": "Suspicious PowerShell activity detected.",
            "device_id": 123456,
            "device_name": "DESKTOP-7I73LFA",
            "device_location": "OFFSITE",
            "device_os": "WINDOWS",
            "device_os_version": "Windows 10 x64",
            "device_username": "rfortress@vmware.com",
            "device_target_value": "MEDIUM",
            "policy_applied": "APPLIED",
            "policy_name": "Restrictive_Windows_Workstation",
            "reason_code": "T_POL_TERM : powershell.exe",
            "run_state": "RAN",
            "sensor_action": "DENY",
            "process_name": "c:\\windows\\system32\
\windowspowershell\\v1.0\\powershell.exe",
```

```
            "process_sha256":
"23ba78d652dd1f9eba61270af662a3602135895ee1b248f59f0d91e05837b967",
            "process_effective_reputation": "NOT_LISTED",
            "process_username": "SYSTEM",
            "attack_tactic": "TA0002",
            "attack_technique": "T1204.002",
            "ttps": [
                "MITRE_T1204_USER_EXECUTION",
                "MITRE_T1204_002_MALICIOUS_FILE"
            ]
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].reason	Incident.Value	Incident	.results[].first_event_timestamp	Suspicious PowerShell activity detected.	Used as the incident title/ value.
.results[].first_event_timestamp	Incident.StartedAt	N/A	N/A	2026-07-09T09:25:35.000Z	Start time for the incident.
.results[].last_event_timestamp	Incident.EndedAt	N/A	N/A	2026-07-09T09:25:35.000Z	End time for the incident.
.results[].severity	Indicator.Attribute, Incident.Attribute	Severity	.results[].first_event_timestamp	3	Ingested as a numeric severity.
.results[].device_target_value	Indicator.Attribute, Incident.Attribute	Target Value	.results[].first_event_timestamp	MEDIUM	Derived from the Carbon Black target value.
.results[].device_id	Incident.Attribute	Device ID	.results[].first_event_timestamp	123456	N/A
.results[].device_name	Incident.Attribute	Device Name	.results[].first_event_timestamp	DESKTOP-7I73LFA	N/A
.results[].device_location	Incident.Attribute	Device Location	.results[].first_event_timestamp	OFFSITE	N/A
.results[].device_os	Incident.Attribute	Device Operating System	.results[].first_event_timestamp	WINDOWS	N/A
.results[].device_os_version	Incident.Attribute	Device Operating System Version	.results[].first_event_timestamp	Windows 10 x64	N/A
.results[].device_username	Incident.Attribute	Device Username	.results[].first_event_timestamp	rfortress@vmware.com	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].policy_applied	Incident.Attribute	Policy Applied	.results[].first_event_timestamp	Yes	Converted from APPLIED or NOT APPLIED.
result[].device_policy	Incident.Attribute	Policy Name	.results[].first_event_timestamp	Restrictive_Windows_Workstation	N/A
.results[].reason_code	Incident.Attribute	Reason Code	.results[].first_event_timestamp	T_POL_TERM : powershell.exe	N/A
.results[].run_state	Incident.Attribute	Run State	.results[].first_event_timestamp	RAN	N/A
.results[].sensor_action	Incident.Attribute	Sensor Action	.results[].first_event_timestamp	DENY	N/A
.results[].process_name	Incident.Attribute	Process Involved	.results[].first_event_timestamp	powershell.exe	N/A
.results[].process_sha256	Indicator.Value	SHA-256	.results[].first_event_timestamp	23ba78d652dd1f9eba61270af662a3602135895ee1b248f59f0d91e05837b967	N/A
.results[].process_sha256	Related Indicator.Value	SHA-256	.results[].first_event_timestamp	23ba78d652dd1f9eba61270af662a3602135895ee1b248f59f0d91e05837b967	Related from the incident.
.results[].attack_tactic	Incident.Attribute	MITRE Tactic	.results[].first_event_timestamp	TA0002	Requires MITRE ATT&CK data already ingested in ThreatQ.
.results[].attack_technique	Incident.Attribute	MITRE Technique	.results[].first_event_timestamp	T1204.002	Requires MITRE ATT&CK data already ingested in ThreatQ.
.results[].ttps[]	Related AttackPattern.Value	Attack Pattern	N/A	MITRE_T1204_002_MALICIOUS_FILE	Only related when the matching attack pattern exists in ThreatQ.
.results[].ttps[]	Related TTP.Value	TTP	N/A	HIDDEN_PROCESS	Non-MITRE TTPs are ingested as TTPs.

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
Attack Pattern	2
Incident	132
Incident Attributes	2,734
Indicators	5
Incident Attributes	28
TTPs	2

Known Issues / Limitations

MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK CDF feeds in order for MITRE ATT&CK attack patterns extracted from an Incident to be related to the Incident object. MITRE ATT&CK attack patterns are ingested from the following feeds:

- MITRE Enterprise ATT&CK
- MITRE Mobile ATT&CK
- MITRE ICS ATT&CK

Change Log

- **Version 2.0.0**
  - Updated the integration to use the VMware Carbon Black Cloud v7 Alerts API, replacing the deprecated v6 endpoint. The integration also includes updated parsing and object mapping to support the v7 response format, with enhanced ingestion of MITRE ATT&CK-related data.
- **Version 1.0.3**
  - Updated attributes.
  - Added new SHA-256 indicators.
- **Version 1.0.2**
  - Deleted empty request parameter which resulted in API error response.
- **Version 1.0.1**
  - Change UI configuration parameter from `Organization ID` to `Organization Key`
- **Version 1.0.0**
  - Initial release