ThreatQuotient

VMware Carbon Black Cloud Platform Alerts Guide

Version 1.0.0

Monday, July 13, 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, July 13, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.25.0`

Introduction

The VMWare Carbon Black Cloud Platform Alerts integration for ThreatQ allows a user to ingest alerts from their Carbon Black Cloud instance in ThreatQ.

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 Platform Alerts** integration 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 feeds 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 Cloud Platform API Host	Enter the FQDN for your Carbon Black Cloud Platform instance (i.e., without protocol)
Organization ID	Your Organization Key, as displayed in the Carbon Black Cloud Platform instance.
API ID	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.

5. Click on **Save Changes**.
6. Click on the toggle switch next to the feed name to enable it.

ThreatQ Mapping

VMWare Carbon Black Cloud Platform Alerts

This feed will ingest alerts as incidents from a VMware Carbon Black Cloud instance. It will also ingest and relate any indicators, MITRE Att&ck Attack Patterns, and TTPs.

```
GET https://{{user_fields.api_host}}/appservices/v6/orgs/{{user_fields.org_key}}/alerts/_search
```


```
{
    "num_found": 107,
    "results": [
        {
            "blocked_threat_category": "UNKNOWN",
            "category": "MONITORED",
            "create_time": "2020-04-13T12:56:25.905Z",
            "created_by_event_id": "2a18cf757d8611eab-abcb989b304c3ec",
            "device_id": 3350047,
            "device_location": "OFFSITE",
            "device_name": "GL-AV-731XM-1",
            "device_os": "WINDOWS",
            "device_os_version": "Server 2012 R2 x64",
            "device_username": "sakshi.rawal@logrhythm.com",
            "first_event_time": "2020-04-13T12:55:30.768Z",
            "group_details": {
                "count": 1,
                "total_devices": 1
            },
```

```
            "id": "33500472a18cf757d8611eababcb989b304c3ec",
            "kill_chain_status": [
                "INSTALL_RUN"
            ],
            "last_event_time": "2020-04-13T12:55:30.768Z",
            "last_update_time": "2020-04-13T12:56:25.905Z",
            "legacy_alert_id": "QME48KBB",
            "not_blocked_threat_category": "NON_MALWARE",
            "notes_present": false,
            "org_key": "7DESJ9GN",
            "policy_applied": "NOT_APPLIED",
            "policy_id": 36161,
            "policy_name": "documentation CB5788",
            "process_name": "java.exe",
            "reason": "A hidden process for java.exe has been
detected. This may indicate the presence of a Rootkit.",
            "reason_code": "R_HIDDEN",
            "run_state": "RAN",
            "sensor_action": null,
            "severity": 4,
            "tags": null,
            "target_value": "LOW",
            "threat_activity_c2": "NOT_ATTEMPTED",
            "threat_activity_dlp": "NOT_ATTEMPTED",
            "threat_activity_phish": "NOT_ATTEMPTED",
            "threat_cause_actor_name": null,
            "threat_cause_actor_process_pid": "79792-
132312531086826897-0",
            "threat_cause_actor_sha256":
```

```
"fafc81c87ae51525893d7e77c52f1aaed9444f1cb8f67601ba23c7e0530ee-
5db",
            "threat_cause_cause_event_id":
"2a18cf757d8611eababcb989b304c3ec",
            "threat_cause_reputation": "TRUSTED_WHITE_LIST",
            "threat_cause_threat_category": "NON_MALWARE",
            "threat_cause_vector": "UNKNOWN",
            "threat_id": "992881090b32cabfa37ab44be4d419b2",
            "threat_indicators": [
                {
                    "process_name": "java.exe",
                    "sha256":
"fafc81c87ae51525893d7e77c52f1aaed9444f1cb8f67601ba23c7e0530ee-
5db",
                    "ttps": [
                        "MITRE_T1158_HIDDEN_FILES_AND_
DIRECTORIES"
                    ]
                },
                {
                    "process_name": "java.exe",
                    "sha256":
"fafc81c87ae51525893d7e77c52f1aaed9444f1cb8f67601ba23c7e0530ee-
5db",
                    "ttps": [
                        "HIDDEN_PROCESS"
                    ]
                }
            ],
```

```
            "type": "CB_ANALYTICS",
            "workflow": {
                "changed_by": "Carbon Black",
                "comment": null,
                "last_update_time": "2020-04-
13T12:56:25.905Z",
                "remediation": null,
                "state": "OPEN"
            }
        },
        {
            "blocked_threat_category": "NON_MALWARE",
            "category": "THREAT",
            "create_time": "2020-04-10T19:25:18.779Z",
            "created_by_event_id":
"fe021e807b6011ea8b807b3f272bca5a",
            "device_id": 3238121,
            "device_location": "OFFSITE",
            "device_name": "DESKTOP-7I73LFA",
            "device_os": "WINDOWS",
            "device_os_version": "Windows 10 x64",
            "device_username": "rfortress@vmware.com",
            "first_event_time": "2020-04-10T19:23:15.464Z",
            "group_details": {
                "count": 3,
                "total_devices": 1
            },
            "id": "3238121fe021e807b6011ea8b807b3f272bca5a",
            "kill_chain_status": [
```

```
                "INSTALL_RUN"
            ],
            "last_event_time": "2020-04-12T23:18:42.072Z",
            "last_update_time": "2020-04-10T19:26:20.740Z",
            "legacy_alert_id": "HNZW3ZEZ",
            "not_blocked_threat_category": "UNKNOWN",
            "notes_present": false,
            "org_key": "7DESJ9GN",
            "policy_applied": "APPLIED",
            "policy_id": 6529,
            "policy_name": "Restrictive_Windows_Workstation",
            "process_name": "sample.exe",
            "reason": "The application sample.exe was detected
running. A Terminate Policy Action was applied.",
            "reason_code": "T_POL_TERM : sample.exe",
            "run_state": "RAN",
            "sensor_action": "DENY",
            "severity": 3,
            "tags": null,
            "target_value": "MEDIUM",
            "threat_activity_c2": "NOT_ATTEMPTED",
            "threat_activity_dlp": "NOT_ATTEMPTED",
            "threat_activity_phish": "NOT_ATTEMPTED",
            "threat_cause_actor_name": null,
            "threat_cause_actor_process_pid": "5180-
1585321534989-1",
            "threat_cause_actor_sha256":
"87e2a0bec31622be040c81657f-
b1dfac1624a854e9e78abf88edcc078a322298",
```

```
            "threat_cause_cause_event_id":
"fe021e807b6011ea8b807b3f272bca5a",
            "threat_cause_reputation": "NOT_LISTED",
            "threat_cause_threat_category": "NEW_MALWARE",
            "threat_cause_vector": "UNKNOWN",
            "threat_id": "e9f3d0e42410a0effd5aab1648db9653",
            "threat_indicators": [
                {
                    "process_name": "explorer.exe",
                    "sha256": "c5e88d778c0b118d49-
bef467ed059c09b61deea505d2a3d5ca1dcc0a5cdf752f",
                    "ttps": [
                        "POLICY_DENY"
                    ]
                },
                {
                    "process_name": "explorer.exe",
                    "sha256": "c5e88d778c0b118d49-
bef467ed059c09b61deea505d2a3d5ca1dcc0a5cdf752f",
                    "ttps": [
                        "RUN_UNKNOWN_APP"
                    ]
                },
                {
                    "process_name": "sample.exe",
                    "sha256": "87e2a0bec31622be040c81657f-
b1dfac1624a854e9e78abf88edcc078a322298",
                    "ttps": [
                        "UNKNOWN_APP"
```

```
                    ]
                },
                {
                    "process_name": "sample.exe",
                    "sha256": "87e2a0bec31622be040c81657f-
b1dfac1624a854e9e78abf88edcc078a322298",
                    "ttps": [
                        "POLICY_TERMINATE"
                    ]
                }
            ],
            "type": "CB_ANALYTICS",
            "workflow": {
                "changed_by": "Carbon Black",
                "comment": null,
                "last_update_time": "2020-04-
10T19:25:18.779Z",
                "remediation": null,
                "state": "OPEN"
            }
        }
    ]
}
```

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 []created_time	Alert: Recorded Future - 2020-07-05T18:35:33.808Z	The creation time of the alert is concatenated to the "reason"
.results[].first_event_time	Incident.StartedAt	N/A	N/A	2020-07-05T18:35:33.080Z	N/A
.results[].last_event_time	Incident.EndedAt	N/A	N/A	2020-07-05T18:35:33.080Z	N/A
.results[].category	Indicator.Attribute, Incident.Attribute	Category	.results []created_time	THREAT	`UNKNOWN` values are not ingested
.results[].kill_chain_status[]	Indicator.Attribute, Incident.Attribute	Kill Chain Status	.results []created_time	INSTALL_RUN	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.results[].severity	Indicator.Attribute, Incident.Attribute	Severity	.results[].created_time	9	N/A
.results[].tags[]	Indicator.Attribute, Incident.Attribute	Tag	.results[].created_time	.results[].created_time	N/A
.results[].target_value	Indicator.Attribute, Incident.Attribute	Target Value	.results[].created_time	HIGH	`UNKNOWN` values are not ingested
.results[].threat_activity_c2	Indicator.Attribute, Incident.Attribute	C2 Activity	.results[].created_time	Yes	`UNKNOWN` values are not ingested
.results[].threat_activity_dlp	Indicator.Attribute, Incident.Attribute	DLP Activity	.results[].created_time	No	`UNKNOWN` values are not ingested

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.results[].threat_activity_phish	Indicator.Attribute, Incident.Attribute	Phishing Activity	.results[].created_time	No	`UNKNOWN` values are not ingested
.results[].threat_cause_reputation	Indicator.Attribute, Incident.Attribute	Threat Cause Reputation	.results[].created_time	ADAPTIVE_WHITE_LIST	`UNKNOWN` values are not ingested
.results[].threat_cause_threat_category	Indicator.Attribute, Incident.Attribute	Threat Cause Threat Category	.results[].created_time	NEW_MALWARE	`UNKNOWN` values are not ingested
.results[].threat_cause_actor_name	Indicator.Attribute, Incident.Attribute	Threat Cause Actor Name	.results[].created_time	Virus: Mimikatz	N/A
.results	Indicator.Attribute,	Threat	.results	WEB	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
[].threat_cause_vector	Incident.Attribute	Cause Vector	[].created_time		
.results[].blocked_threat_category	Indicator.Attribute, Incident.Attribute	Blocked Threat Category	.results[].created_time	NEW_MALWARE	`UNKNOWN` values are not ingested
.results[].device_id	Incident.Attribute	Device ID	.results[].created_time	12345	N/A
.results[].device_location	Incident.Attribute	Device Location	.results[].created_time	OFFSITE	`UNKNOWN` values are not ingested
.results[].device_name	Incident.Attribute	Device Name	.results[].created_time	GL-AV-731XM-1	`UNKNOWN` values are not ingested
.results	Incident.Attribute	Device Oper-	.results	WINDOWS	`UNKNOWN` values are

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
[].device_os		ating System	[].created_time		not ingested
.results[].device_os_version	Incident.Attribute	Device Operating System Version	.results[].created_time	Server 2012 R2 x64	`UNKNOWN` values are not ingested
.results[].device_username	Incident.Attribute	Device Username	.results[].created_time	sakshi.rawal@logrhythm.com	`UNKNOWN` values are not ingested
.results[].not_blocked_threat_category	Incident.Attribute	Not Blocked Threat Category	.results[].created_time	NON_MALWARE	N/A
.results[].policy_applied	Incident.Attribute	Policy Applied	.results[].created_time	Yes	Always one of `Yes`, `No`, converted from `APPLIED` or `NOT APPLIED`; `UNKNOWN`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					values are not inges-ted
.results []policy_name	Incident.Attribute	Policy Name	.results []created_ time	documentation CB5788	`UNKNOWN` values are not ingested
.results []reason	Incident.Attribute	Reason	.results []created_ time	Recorded Future	`UNKNOWN` values are not ingested
.results []reason_code	Incident.Attribute	Reason Code	.results []created_ time	R_HIDDEN	`UNKNOWN` values are not ingested
.results[].run_ state	Incident.Attribute	Run State	.results []created_ time	RAN	`UNKNOWN` values are not ingested
.results	Incident.Attribute	Sensor	.results	DENY	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
[].sensor_action		Action	[].created_time		
.results[].threat_indicators[].process_name	Incident.Attribute	Process Involved	.results[].created_time	explorer.exe	N/A
.results[].type	Incident.Attribute	Carbon Black Type	.results[].created_time	CB_ANALYTICS	N/A
.results[].group_details.count	Incident.Attribute	Group Count	.results[].created_time	2	N/A
.results[].first_event_time	Incident.Attribute	First Event Time	.results[].created_time	2020-07-05T18:35:33.080Z	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.results[].id	Incident.Attribute	Alert Link	.results[].created_time	N/A	Formatted from user fields and response data
.results[].threat_cause_actor_sha256	Indicator.Value	SHA-256	.results[].created_time	FA4F71314F1D8587604B79149880618B95017F0CCF11E2DDC372BCCC32A7CF8B	N/A
.results[].threat_indicators[].ttps[]	AttackPattern.Value	Attack Pattern	N/A	T1075 - Pass the Hash	Only related to an Incident if the ThreatQ instance has available MITRE ATT&CK Attack Pattern data.
.results[].threat_indicators[].ttps[]	TTP.Value	TTP	N/A	RUN_UNKNOWN_APP	Non-MITRE Attack TTPs

Average Feed Run

Average Feed Run results for VMWare Carbon Black Cloud Platform Alerts.

The metrics provided below are with the minimum severity set to 5 with all categories and target values selected.

Metric	Result
Run Time	< 1 minute
Indicators	7
Indicator Attributes	70
Incidents	55
Incident Attributes	1050
TTPs	70

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.

Known Issues/Limitations

MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK 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 PRE-ATT&CK

Change Log

- **Version 1.0.0**
  - Initial release