ThreatQuotient

Fidelis Elevate Alerts CDF Guide

Version 1.2.0

June 24, 2021

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.

Contents

Versioning

- Current integration version: `1.2.0`
- Supported on ThreatQ versions >= `4.25.0`

Introduction

The Fidelis Elevate Alerts CDF for ThreatQ enables a ThreatQ user to ingest alerts from Fidelis based on configurable severity and score thresholds.

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 **OSINT** option from the *Category* dropdown (optional).
3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Fidelis Hostname / IP	The Hostname or IP Address for your Fidelis Server.
Username	Your Fidelis username to authenticate.
Password	Your Fidelis password to authenticate.
Score Threshold	The minimum score threshold to filter ingested alerts by (0-100).
Severity Filter	The severity levels to ingest.
Verify SSL	Verify the SSL certificate of the Fidelis Server. If you are using a self-signed certificate, you will most likely leave this box unchecked.
Timezone Offset (hrs)	The number of hours to offset requests to match time of the Fidelis server.

This setting will need to be updated periodically to account for any daylight saving time changes.

5. Review the **Settings** configuration, 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

Fidelis Alerts

Pulling Alerts from a Fidelis instance is a multi-step process involving three requests:

- `POST https://<Host>/j/rest/v2/access/token/` - Authentication endpoint
- `GET https://<Host>/j/rest/v2/alert/column/` - Endpoint returning information about the data columns the Fidelis instance uses
- `POST https://<Host>/j/rest/v1/alert/search/` - Ultimate data polling endpoint

Given input data about which columns to request, the Alert Search endpoint returns JSON data like the following:


```
[
    {
        "alertTotal": 1,
        "cancelled": false,
        "duration": 199,
        "fromTime": "2020-05-01 18:58:00",
        "referenceTime": "2020-05-19 14:59:02",
        "retrieveTime": "2020-05-19 14:59:02",
        "total": 1,
        "totalUnknown": false,
        "toTime": "2020-05-19 14:59:02",
        "aaData": [
            {
                "ACTION": "alert",
                "AGG_ALERT_ID": "4",
                "AGG_DESCRIPTION": "non-DNSSEC Response",
                "AGG_ENTITY": "192.168.0.27",
                "AGG_LABEL": [],
                "AGG_TICKET_OWNER_NAME": "",
                "AGG_TICKET_RESOLUTION": "",
                "AGG_TICKET_STATUS": "New",
                "AGG_THREAT_SCORE": "15",
                "ALERT_ID": "34",
                "ALERT_TYPE": "DNS",
                "APPLICATION_USER": "",
                "ASSET_COVERAGE_SCORE": "1",
                "ASSET_ENDPOINT_ID": "",
                "ASSET_ID": "2",
                "ASSET_IMPORTANCE_SCORE": "5",
                "ASSET_NAME": "",
                "ASSET_OS": [
                    "CentOs 6.5"
                ],
                "ASSET_RISK_SCORE": "1",
                "ASSET_ROLE": [],
```

```
                "ASSET_SERVICE": [],
                "ASSET_SEVERITY_SCORE": "1",
                "ASSET_TYPE": "",
                "CLIENT_IP": "192.168.0.27",
                "CLIENT_PORT": "57287",
                "COMPONENT_NAME": "Sensor",
                "COMPRESSION": "0",
                "DEST_COUNTRY_NAME": "unknown",
                "DEST_DEVICE_ID": "",
                "DEST_DOMAIN_NAME": "",
                "DEST_IP": "192.168.0.27",
                "DEST_PORT": "57287",
                "DEST_USER_NAME": "",
                "ENDPOINT_ACTION": "",
                "ENTROPY": "",
                "EXECUTION_FORENSIC_STATUS": "Not Submitted",
                "FIDELIS_SCORE": "15",
                "FILE_NAME": "",
                "FILE_TYPE": "",
                "FROM": "",
                "HOST_ACTIVITY": "Not Applicable",
                "HOST_IP": "192.168.0.27",
                "INSERT_TIME": "2020-05-16 11:10:36",
                "MALWARE_NAME": "Unknown",
                "MALWARE_TYPE": "",
                "MD5": "",
                "OTHER_ASSET_ID": "4",
                "PCAP_FILENAME": "",
                "PCAP_TIMESTAMP": "",
                "PROTOCOL": "DNS",
                "RULE_NAME": "non-DNSSEC Response",
                "SHA256": "",
                "SERVER_IP": "192.168.0.10",
                "SERVER_PORT": "53",
                "SESSION_ID": "6827344568705352741",
                "SEVERITY": "Low",
                "SRC_COUNTRY_NAME": "unknown",
                "SRC_DEVICE_ID": "",
                "SRC_DOMAIN_NAME": "",
                "SRC_IP": "192.168.0.10",
                "SRC_PORT": "53",
                "SRC_USER_NAME": "",
                "SUBJECT": "",
                "TARGET": "",
                "THREAT_SCORE": "",
                "TO": "",
                "UUID": "fbaf8a96-9748-11ea-a4a6-005056ac167a",
                "USER_RATING": "No Rating",
                "VLAN_ID": "",
                "WITH_MALWARE": "No"
            },
            ...
        ]
    }
]
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].aaData[].ACTION	Attribute	Action	[].aaData[].INSERT_TIME	alert	N/A
[].aaData[].AGG_DESCRIPTION	Attribute	Description	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].AGG_TICKET_OWNER_NAME	Attribute	Ticket Owner	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].AGG_TICKET_RESOLUTION	Attribute	Ticket Resolution	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].AGG_TICKET_STATUS	Attribute	Ticket Status	[].aaData[].INSERT_TIME	New	N/A
[].aaData[].AGG_THREAT_SCORE	Attribute	Threat Score	[].aaData[].INSERT_TIME	75	N/A
[].aaData[].ALERT_ID	Attribute	Alert ID	[].aaData[].INSERT_TIME	55	N/A
[].aaData[].ALERT_ID / [].COMPONENT_NAME / [].AGG_DESCRIPTION / [].WITH_MALWARE	Event.Title	Fidelis Alert	N/A	Alert: 1 - Sensor detected -> Extremely large packet	The event title is built using a number of fields
[].aaData[].ALERT_TYPE	Attribute	Alert Type	[].aaData[].INSERT_TIME	DNS	N/A
[].aaData[].ASSET_COVERAGE_SCORE	Attribute	Asset Coverage Score	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_IMPORTANCE_SCORE	Attribute	Asset Importance Score	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_NAME	Attribute	Asset Name	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_OS	Attribute	Asset Operating System	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_RISK_SCORE	Attribute	Asset Risk Score	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_ROLE	Attribute	Asset Role	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_SERVICE	Attribute	Asset Service	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_SEVERITY_SCORE	Attribute	Asset Severity Score	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].ASSET_TYPE	Attribute	Asset Type	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].CLIENT_IP	Attribute	Client IP	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].CLIENT_PORT	Attribute	Client Port	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].COMPONENT_NAME	Attribute	Component Name	[].aaData[].INSERT_TIME	N/A	N/A
[].aaData[].DEST_COUNTRY_NAME	Attribute	Destination Country	[].aaData[].INSERT_TIME	N/A	Only ingested if the Client IP does not match the Dest IP
[].aaData[].DEST_DOMAIN_NAME	Indicator.Value	FQDN	[].aaData[].INSERT_TIME	N/A	Only ingested if Client IP does not match the Dest IP
[].aaData[].DEST_IP	Indicator.Value	IP Address	[].aaData[].INSERT_TIME	N/A	Only ingested if Client IP does

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					not match the Dest IP
[]aaData[].DEST_PORT	Attribute	Port	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].DEST_USER_NAME	Indicator.Value	Username	[]aaData[].INSERT_TIME	N/A	Only ingested if Client IP does not match the Dest IP
[]aaData[].ENDPOINT_ACTION	Attribute	Endpoint Action	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].EXECUTION_FORENSIC_STATUS	Attribute	Execution Forensic Status	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].FIDELIS_SCORE	Attribute	Fidelis Score	[]aaData[].INSERT_TIME	75	N/A
[]aaData[].FILE_NAME	Indicator.Value	Filename	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].FILE_TYPE	Attribute	File Type	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].HOST_ACTIVITY	Attribute	Host Activity	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].MD5	Indicator.Value	MD5	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].MALWARE_NAME	Malware.Value	N/A	[]aaData[].INSERT_TIME	Unknown	Only ingested if the value is *not* Unknown
[]aaData[].MALWARE_TYPE	Attribute	Malware Type	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].RULE_NAME	Attribute	Associated Rule	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].SEVERITY	Attribute	Severity	[]aaData[].INSERT_TIME	High	N/A
[]aaData[].SHA256	Indicator.Value	SHA-256	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].SRC_COUNTRY_NAME	Attribute	Source Country	[]aaData[].INSERT_TIME	N/A	Only ingested if the Client IP does not match the Source IP
[]aaData[].SRC_DOMAIN_NAME	Indicator.Value	FQDN	[]aaData[].INSERT_TIME	N/A	Only ingested if Client IP does not match the Source IP
[]aaData[].SRC_IP	Indicator.Value	IP Address	[]aaData[].INSERT_TIME	N/A	Only ingested if Client IP does not match the Source IP
[]aaData[].SRC_PORT	Attribute	Port	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].SRC_USER_NAME	Indicator.Value	Username	[]aaData[].INSERT_TIME	N/A	Only ingested if Client IP does not match the Source IP
[]aaData[].SUBJECT	Attribute	Subject	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].TARGET	Attribute	Target	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].USER_RATING	Attribute	User Rating	[]aaData[].INSERT_TIME	N/A	N/A
[]aaData[].WITH_MALWARE	Attribute	With Malware	[]aaData[].INSERT_TIME	N/A	N/A

Average Feed Run

Ingestion time relies on the size of the Fidelis sensor deployment and will vary between instances.

Change Log

- **Version 1.2.0**
  - Added support for offsetting the timezone. See the Configuration section for more details.
- **Version 1.1.1**
  - Updated the alert search query to pull all alerts.
  - Removed the OAuth authentication feature that would cause feed run errors to occur.
- **Version 1.1.0**
  - Refactored feed usage for new Token Auth.
- **Version 1.0.0**
  - Initial Release