ThreatQuotient

Devo Alerts CDF Guide

Version 1.0.0

May 15, 2023

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

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	>= 4.40.0
Support Tier	ThreatQ Supported

Introduction

The Devo Alerts CDF for ThreatQ enables the automatic ingestion of incidents from Devo to ThreatQ.

The integration provides the following feeds:

- **Devo Alerts** - ingests the incidents from Devo Platform.
- **Devo Alert Details (Supplemental)** - returns all the information available about the incident.

The integration ingests the following system objects:

- Events
- Indicators

Prerequisites

The following is required by the integration:

- An active Devo license.
- A valid API token.

> As of this publication, any token type is for valid for the Devo API

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.

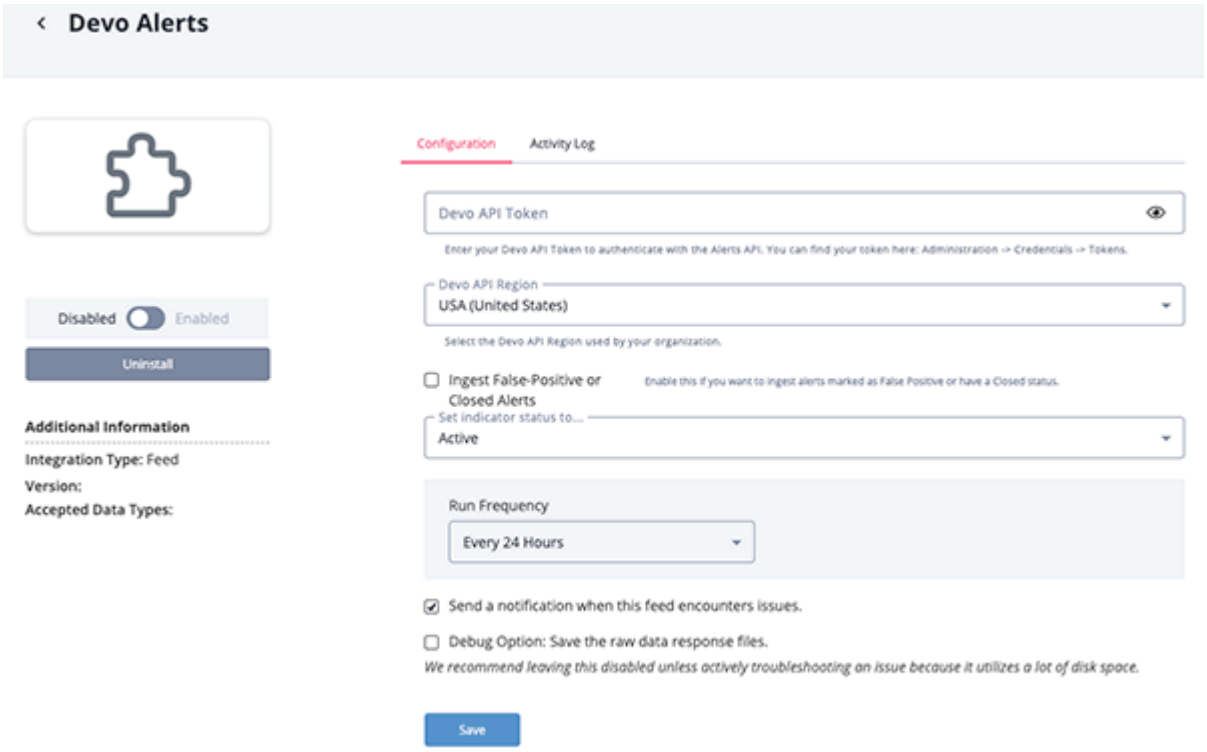
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **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
Devo API Token	Your Devo API Token to authenticate with the Alerts API. You can find your tokenby navigating to **Administration > Credentials > Tokens** in your Devo portal.
Devo API Region	Select the Devo API Region used by your organization. Options include: ◦ USA (United States) - **(default)** ◦ EU (Europe) ◦ CAN (Canada) ◦ ES (Spain) ◦ APAC (Asian-Pacific)
Ingest False-Positive or Closed Alerts	When enabled, the integration will ingest alerts marked as False Positive or have a Closed status. This option is disabled by default.



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

Devo Alerts

The Devo Alerts feed periodically pulls alerts from Devo, into ThreatQ

Sample Response:

```
GET https://{{ region }}/alerts/v1/alerts/list
```


```
[
    {
        "id": 92133628,
        "domain": "threatquotient",
        "priority": 10,
        "context": "my.alert.threatquotient.Suspiciously_Large_POST_Requests",
        "category": "my.context",
        "srcPort": null,
        "srcIp": null,
        "srcHost": null,
        "dstIp": null,
        "dstPort": null,
        "dstHost": null,
        "protocol": null,
        "username": null,
        "application": null,
        "engine": "pilot-4-pro-cloud-custom-aws-us-east-1",
        "extraData": "{\"count\":\"49\",\"eventdate\":\"2022-08-02+14%3A00%3A00.0\"}",
        "alertDate": null,
        "creationDate": null,
        "status": 100,
        "ack_status_date": null,
        "createDate": 1659450636000,
        "updateDate": 1659455802000,
        "scaled": false,
        "digest": "6c8c322006f9c38d6c726972cbfc59a58e91f120",
        "uniquedigest": "fbeb2fef7b04391d0365b1b791d15e76e8a3fda8",
        "contexto": null,
        "postAlertAction": null,
        "contextLabel": null,
        "contextSubscription": null,
        "shouldSend": false,
        "recoveryId": null,
        "skipAntiflooding": false,
        "useCreationDate": false,
        "alertOwner": null,
        "fullExtraData": null,
        "alertType": null,
        "alertMitreTactics": null,
        "alertMitreTechniques": null,
        "alertPriority": null,
        "alertDefinition": {
            "id": "187427",
```

```
            "creationDate": 1659450388000,
            "name": "Suspiciously Large POST Requests",
            "message": "Large POST Requests",
            "description": "This is the alert description",
            "categoryId": "3593",
            "subcategory": "lib.my.threatquotient.Suspicious_Sighting",
            "subcategoryId": "3431",
            "isActive": true,
            "isFavorite": false,
            "isAlertChain": false,
            "alertCorrelationContext": {
                "id": "41646",
                "nameId": "my.alert.threatquotient.Suspiciously_Large_POST_Requests",
                "ownerEmail": "zach.shames@threatq.com",
                "querySourceCode": "from demo.ecommerce.data\n\twhere method = \"POST\"\n    and statusCode = 200\n
and bytesTransferred > 3000\n  select isnotnull(`lu/ThreatQ_Blacklist_IP_Address/threatq_link`(str(clientIpAddress)))
as `ThreatQ Match`,\n    `lu/ThreatQ_Blacklist_IP_Address/score`(str(clientIpAddress)) as `ThreatQ Score`,\n    `lu/
ThreatQ_Blacklist_IP_Address/malware_family`(str(clientIpAddress)) as `Malware Family`,\n    `lu/
ThreatQ_Blacklist_IP_Address/adversary`(str(clientIpAddress)) as Adversary,\n    `lu/ThreatQ_Blacklist_IP_Address/
tags`(str(clientIpAddress)) as `ThreatQ Tags`",
                "priority": 5,
                "correlationTrigger": {
                    "kind": "several",
                    "period": 1800000,
                    "threshold": 10,
                    "keys": []
                }
            },
            "actionPolicyId": []
        },
        "allExtraDataFields": {
            "count": "49",
            "eventdate": "2022-08-02+14%3A00%3A00.0"
        },
        "tags": null,
        "entities": null,
        "commentsList": null,
        "alertLabel": "[threatquotient:my.alert.threatquotient.Suspiciously_Large_POST_Requests:92133628]"
    }
]
```


ThreatQ provides the following default mapping for feed:

> The following data paths are based on each item within the response list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.alertDefinition.name`, `.alertDefinition.message`, `.alertDefinition.subcategory`, `.priority`, `.id`	Event Title	Alert	`.createDate`	`Devo Alert: {{ data.alertDefinition.name }} - {{ data.alertDefinition.message }} - {{ data.alertDefinition.subcategory }} (Priority: {{ data.priority }}; ID: {{ data.id }})`	Keys are formatted into a template
`.tags[]`	Event Tags	N/A	N/A	N/A	Added if `.tags` return by `Devo Alert Details` are empty

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.domain`	Event Attribute	Domain	`.createDate`	`threatquotient`	N/A
`.priority`	Event Attribute	Priority	`.createDate`	`Normal`	The float is mapped to string. Opts: Very Low, Low, Normal, High, Very High
`.alertDefinition.name`	Event Attribute	Alert Definition Name	`.createDate`	`Suspiciously Large POST Requests`	N/A
`.alertDefinition.message`	Event Attribute	Alert Definition Message	`.createDate`	`Large POST Requests`	N/A
`.alertDefinition.description`	Event Attribute	Alert Definition Description	`.createDate`	`This is the alert description`	N/A
`.alertDefinition.subcategory`	Event Attribute	Alert Definition Subcategory	`.createDate`	`Suspicious Sighting`	The last value after splitting by `.` and `_` is replaced by space `
`.allExtraDataFields.count`	Event Attribute	Event Count	`.createDate`	49	N/A
`.commentsList`	Event Attribute	Annotation	`.createDate`	N/A	Added if `.commentsList` return by `Devo Alert Details` are empty
`.alertMitreTactics`	Event Attribute	Tactic	`.createDate`	N/A	N/A
`.alertMitreTechniques`	Event Attribute	Technique	`.createDate`	N/A	N/A
`.srcHost`	Event Attribute	Source Host	`.createDate`	N/A	N/A
`.dstHost`	Event Attribute	Destination Host	`.createDate`	N/A	N/A
`.application`	Event Attribute	Application	`.createDate`	N/A	N/A
`.id`	Event Attribute	Devo Query Link	`.createDate`	`{{ api_region }}/#/loxcope/alert/goToQuery?id={{ .id }}`	ID is formatted into a template
`.dstIp`	Related Indicator Value	N/A	`.createDate`	N/A	N/A
`.srcIp`	Related Indicator Value	N/A	`.createDate`	N/A	N/A
`.protocol`	Related Indicator Attribute	Protocol	`.createDate`	N/A	Only applied to `.dstIp` and `srcIp`
`.dstPort`	Related Indicator Attribute	Port	`.createDate`	N/A	Only applied to `.dstIp`
`.srcPort`	Related Indicator Attribute	Port	`.createDate`	N/A	Only applied to `.srcIp`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.allExtraDataFields`	Event Description	N/A	N/A	N/A	Formatted into `<pre>` tags & JSON-formatted

Devo Alert Details (Supplemental)

The Devo Alert Details supplemental feed fetches the full context for a given alert, by ID.

```
GET https://{{ region }}/alerts/v1/alerts/get?id={{ alert_id }}&tags=true&annotations=true
```

Sample Response:


```
{
    "id": 92133628,
    "domain": "threatquotient",
    "priority": 10,
    "context": "my.alert.threatquotient.Suspiciously_Large_POST_Requests",
    "category": "my.context",
    "srcPort": null,
    "srcIp": null,
    "srcHost": null,
    "dstIp": null,
    "dstPort": null,
    "dstHost": null,
    "protocol": null,
    "username": null,
    "application": null,
    "engine": "pilot-4-pro-cloud-custom-aws-us-east-1",
    "extraData": "{\"count\":\"49\",\"eventdate\":\"2022-08-02+14%3A00%3A00.0\"}",
    "alertDate": null,
    "creationDate": null,
    "status": 100,
    "ack_status_date": null,
    "createDate": 1659450636000,
    "updateDate": 1659455802000,
    "scaled": false,
    "digest": "6c8c322006f9c38d6c726972cbfc59a58e91f120",
    "uniquedigest": "fbeb2fef7b04391d0365b1b791d15e76e8a3fda8",
    "contexto": null,
    "postAlertAction": null,
    "contextLabel": null,
    "contextSubscription": null,
    "shouldSend": false,
    "recoveryId": null,
    "skipAntiflooding": false,
    "useCreationDate": false,
    "alertOwner": null,
    "fullExtraData": null,
    "alertType": null,
    "alertMitreTactics": null,
    "alertMitreTechniques": null,
    "alertPriority": null,
    "alertDefinition": null,
    "allExtraDataFields": null,
    "tags": null,
    "entities": null,
    "commentsList": [
        {
            "id": 160512,
            "author": {
```

```
                "id": 43709,
                "user": {
                    "id": "94b7d52a-e590-42d6-96eb-43e21e58154f",
                    "email": "zach.shames@threatq.com",
                    "username": "Zach Shames",
                    "telephone": "",
                    "pwd": "03i5ip401y5FrSXRdpHv2y8RMom424m/rDloi/
5tspM=$Z8r4L6LUh45WkWKH18S87rAJeorqHwsqOfMA9HovqAk=",
                    "status": 0,
                    "validation_token": null,
                    "defaultDomain": "threatquotient",
                    "updateDate": 1659447389000,
                    "creationDate": 1658956699000,
                    "otpSecret": null,
                    "loginAttempts": 0,
                    "recoveryAttempts": 0
                },
                "domain": {
                    "id": "a7c2c8f7-efed-4148-9eda-e2b7b08c8248",
                    "name": "threatquotient",
                    "status": 0,
                    "type": 11,
                    "updateDate": 1658952948000,
                    "creationDate": 1658952948000,
                    "subscribed": 0,
                    "daysLeft": 30,
                    "showLanding": true,
                    "reseller": null,
                    "groupId": null,
                    "alertsLastReseted": null
                },
                "lastTimeLogged": 1659447394000,
                "status": 0,
                "creationDate": 1658953155000,
                "updateDate": 1659456938000,
                "pwd": null,
                "validationToken": null,
                "roleCustom": null,
                "rolesCustom": null,
                "externalId": null,
                "owner": false,
                "alertsLastVisited": 1659456938000
            },
            "msg": "This is the annotation's description\nN/A",
            "ack": "{\"ackUserList\":[\"94b7d52a-e590-42d6-96eb-43e21e58154f\"]}",
            "creationDate": 1659456970000,
            "updateDate": 1659456970000,
            "elementType": "alert",
            "elementId": "92133628",
            "domain": {
                "id": "a7c2c8f7-efed-4148-9eda-e2b7b08c8248",
                "name": "threatquotient",
                "status": 0,
                "type": 11,
                "updateDate": 1658952948000,
                "creationDate": 1658952948000,
                "subscribed": 0,
                "daysLeft": 30,
                "showLanding": true,
                "reseller": null,
                "groupId": null,
```

```
                "alertsLastReseted": null
            },
            "title": "This is a demo annotiation",
            "status": null,
            "task": false
        }
    ],
    "alertLabel": "[threatquotient:my.alert.threatquotient.Suspiciously_Large_POST_Requests:92133628]"
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.tags`	Event Tags	N/A	`.createDate`	N/A	N/A
`.commentsList.title`, `.commentsList.msg`	Event Attribute	Annotation	`.createDate`	`This is a demo annotiation: This is the annotation's description`	`.commentsList.title` and `.commentsList.msg` are concatenated

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	2 minutes
Events	21
Event Attributes	168

Change Log

- **Version 1.0.0**
  - Initial release