ThreatQuotient

Exabeam CDF

Version 1.0.0

September 24, 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

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	>= 5.25.0
Support Tier	ThreatQ Supported

Introduction

The Exabeam CDF provides users with visibility into their Exabeam instance by ingesting Incidents into ThreatQ. In addition to the high level incident information, the integration also ingests the related indicators and attack patterns for each incident.

Exabeam is a cloud-native SIEM solution that provides teams with modern search capabilities, powerful correlation, as well as reporting, dashboarding, and case management.

The integration provides the following feeds:

- **Exabeam Events** - retrieves all events that are not closed.
- **Exabeam - Get Case (Supplemental) -** retrieves event context from Exabeam.

The integration ingests the following system object types:

- Attack Patterns
- Events
- Indicators
    - IP Address

Prerequisites

The following is required to utilize the integration:

- An Exabeam Client ID and Client Secret.

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 yaml file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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 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:

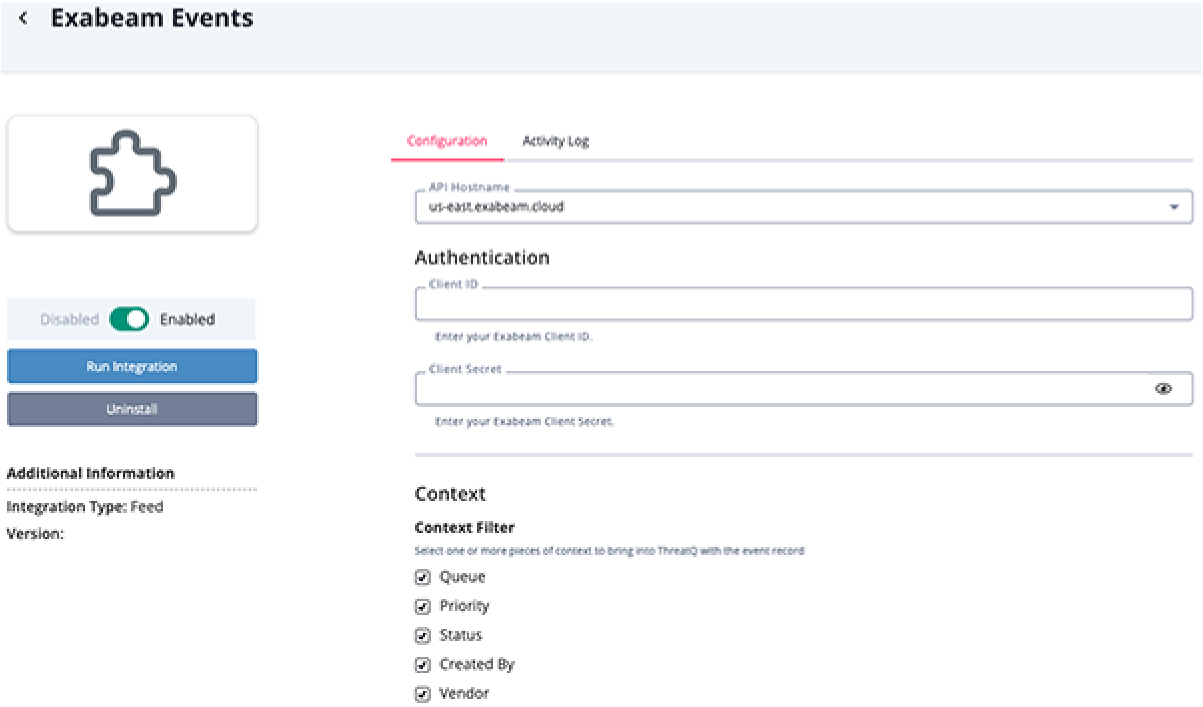
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
Exabeam Hostname/IP	Select the API hostname. Options include: ◦ us-west.exabeam.cloud ◦ us-east.exabeam.cloud(default) ◦ sg.exabeam.cloud ◦ jp.exabeam.cloud ◦ eu.exabeam.cloud ◦ au.exabeam.cloud ◦ ca.exabeam.cloud ◦ ch.exabeam.cloud
Client ID	Your Exabeam Client ID.
Client Secret	Your Exabeam Client Secret.
Context Filter	Select one or more pieces of context to bring into ThreatQ with the event record. Options include: ◦ Queue (default) ◦ Priority (default) ◦ Status (default) ◦ Created By (default) ◦ Vendor (default) ◦ Product (default) ◦ Risk Score (default) ◦ Last Modified (default) ◦ Assignee (default) ◦ Grouped By (default) ◦ Has Attachments (default) ◦ Is Deleted (default) ◦ Stage (default)

PARAMETER	DESCRIPTION
	◦ Approx Log Time (default) ◦ Use Case (default) ◦ Destination Hosts (default) ◦ Source Hosts (default)
Supporting Context	Select which pieces of context to relate to the events. Options include: ◦ IP Address (default) ◦ Attack patterns (default)



API Hostname: us-east.exabeam.cloud

Authentication

Client ID

Enter your Exabeam Client ID.

Client Secret

Enter your Exabeam Client Secret.

Context

Context Filter

Select one or more pieces of context to bring into ThreatQ with the event record

☑ Queue
☑ Priority
☑ Status
☑ Created By
☑ Vendor

Additional Information

Integration Type: Feed

Version:

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

Exabeam Events

The Exabeam Events feed fetches all the events from Exabeam that are not closed.

`POST https://{host}/threat-center/v1/search/cases`

Sample Response:

```
{
  "timeStartedMillis": 1726228934591,
  "timeCompletedMillis": 1726228936538,
  "rows": [
    {
      "groupedbyKey": "Src Ip",
      "groupedbyValue": "10.2.1.28",
      "ingestTimestamp": 1725232224731076,
      "caseId": "e5c8183d-6141-43ca-a9fc-53dcb3cced1e",
      "creationTimestamp": 1725231744876320,
      "alertId": "46582464-19d3-467e-bef3-ee6d324955c5"
    },
    {
      "groupedbyKey": "Rule",
      "groupedbyValue": "partnerlab2 - to identify new logsource",
      "ingestTimestamp": 1725223840161667,
      "caseId": "33095869-a95b-4fd2-8795-9bdbb4723d20",
      "creationTimestamp": 1725223342073796,
      "alertId": "edb49883-d294-45b3-b92f-cdec6108a3e6"
    },
}
```

Exabeam - Get Case (Supplemental)

The Exabeam - Get Case supplemental feed fetches details for a specific case id.

`GET https://{host}/threat-center/v1/cases/{{caseId}}`

Sample Response:

```
{
  "alertCreationTimestamp": "2024-09-01T01:36:25.780685",
  "alertId": "c3e5cfcc-ce50-40b3-81b3-dddf0d0d6259",
  "approxLogTime": "2024-09-01T01:27:00",
  "assignee": "Unassigned",
  "creationTimestamp": "2024-09-01T01:40:18.185756",
  "caseId": "3162c0ea-83b3-4757-866c-c64716a1c238",
  "creationBy": "system",
  "stage": "NEW",
  "alertDescriptionRt": "For alert_severity HIGH, greater than 2 events were observed in 30 minutes, actual value 4",
  "hasAttachments": false,
  "isDeleted": false,
  "lastModifiedBy": "dNyh4tLk0bJCBJpkqL8PkYHxSlKa2whAXw7kyXreAqVN1MDx",
  "lastModifiedTimestamp": "2024-09-13T12:03:18.35489232",
  "mitres": [
    {
      "tacticKey": "TA0007",
      "tactic": "Discovery",
      "techniqueKey": "T1619",
      "technique": "Cloud Storage Object Discovery"
    },
    {
      "tacticKey": "TA0002",
      "tactic": "Execution",
      "techniqueKey": "T1651",
      "technique": "Cloud Administration Command"
    }
  ],
  "alertName": "Wiz Alert High",
  "priority": "LOW",
  "riskScore": 75,
  "queue": "Tier 1 Analyst",
  "status": "READ",
  "tags": [],
  "useCases": [
    "Cloud Data Protection"
  ],
  "products": [
    "Correlation Rule"
  ],
  "vendors": [
    "Exabeam"
  ],
  "srcHosts": [],
  "srcIps": [],
  "destHosts": [],
  "destIps": [],
  "users": [],
  "groupedbyKey": "Rule",
  "groupedbyValue": "wiz alert high",
  "ingestTimestamp": "2024-09-01T01:39:22.497263",
  "srcEndpoints": [],
  "destEndpoints": []
}
```

Feed Mapping Table

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
`.alertName`	Event Title	Alert	N/A	`.creationTimestamp`	N/A	N/A
`.alertDescriptionRt`	Event Description	N/A	N/A	`.creationTimestamp`	N/A	N/A
`.ingestTimestamp`	Event Happened At	N/A	N/A	`.creationTimestamp`	N/A	N/A
`.queue`	Event Attribute	Queue	N/A	`.creationTimestamp`	N/A	User-configurable
`.priority`	Event Attribute	Priority	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`.status`	Event Attribute	Status	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`.creationBy`	Event Attribute	Created By	N/A	`.creationTimestamp`	N/A	User-configurable
`.vendors`	Event Attribute	Vendor	N/A	`.creationTimestamp`	N/A	User-configurable
`.products`	Event Attribute	Product	N/A	`.creationTimestamp`	N/A	User-configurable
`.riskScore`	Event Attribute	Risk Score	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`approxLogTime`	Event Attribute	Approx Log Time	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`.useCases`	Event Attribute	Use Case	N/A	`.creationTimestamp`	N/A	User-configurable
`.lastModifiedTimestamp`	Event Attribute	Last Modified	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`.assignee`	Event Attribute	Assignee	N/A	`.creationTimestamp`	N/A	User-configurable
`.groupedbyKey`	Event Attribute	Grouped By	N/A	`.creationTimestamp`	N/A	User-configurable
`.hasAttachments`	Event Attribute	Has Attachments	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`.isDeleted`	Event Attribute	Is Deleted	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`.stage`	Event Attribute	Stage	N/A	`.creationTimestamp`	N/A	Updatable; User-configurable
`.destHosts[]`	Event Attribute	Destination Hosts	N/A	`.creationTimestamp`	N/A	User-configurable
`.srcHosts[]`	Event Attribute	Source Hosts	N/A	`.creationTimestamp`	N/A	User-configurable
`.tags`	Event Tag	N/A	N/A	N/A	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
`.destIps[]`, `.srcIps[]`	Related Indicator	IP Address	N/A	`.creationTimestamp`	N/A	User-configurable
`.mitres.tacticKey`- `.mitres.tactic`	Related Attack Pattern	N/A	N/A	`.creationTimestamp`	N/A	User-configurable; Ingests if the `.mitres.tacticKey` does not exist in TQ, or else relates the objects
`.mitres.techniqueKey`- `.mitres.technique`	Related Attack Pattern	N/A	N/A	`.creationTimestamp`	N/A	User-configurable; Ingests if the `.mitres.techniqueKey` does not exist in TQ, or else relates the objects

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
Events	10
Event Attributes	136
Indicators	2
Attack Patterns	14

Change Log

- **Version 1.0.0**
  - Initial release