ThreatQuotient

A Securonix Company



Exabeam CDF

Version 2.0.0

November 16, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Exabeam Alerts Parameters 9
Exambeam Cases Parameters 11
ThreatQ Mapping **13**
Exabeam Cases 13
Exabeam - Get Case (Supplemental) 15
Exabeam Alerts 18
Average Feed Run **20**
Exabeam Cases 20
Exabeam Alerts 20
Known Issues / Limitations **21**
Change Log **22**

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.

Copyright © 2026 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: 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	>= 5.25.0
Support Tier	ThreatQ Supported

Introduction

The Exabeam CDF connects Exabeam Threat Center with ThreatQ, bringing alert and case data into your threat intelligence workflows. It retrieves matching alerts and open cases, then collects their details to provide additional context for investigation.

You can configure the feed to include relevant context, related IP address indicators, and MITRE ATT&CK patterns. When enabled, the optional Copilot Threat Summary can be added to an alert's event description. The feed ingests events, IP address indicators, and attack patterns into ThreatQ.

The integration provides the following feeds:

- **Exabeam Alerts** - retrieves matching alerts and then fetches each alert's details. The optional Copilot Threat Summary is intended for the event description.
- **Exabeam Cases** - retrieves open cases and then fetches each case's details.
    - **Exabeam - Get Token (Supplemental)** - obtains an OAuth access token used to authenticate API requests.
    - **Exabeam - Get Case (Supplemental)** - retrieves event context from Exabeam.
    - **Exabeam - Get Alert (Supplemental)** - retrieves full details for an alert returned by Exabeam Alerts.
    - **Exabeam - Get Threat Summary (Supplemental)** - requests the Copilot Threat Summary for an alert when the option is enabled.

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
6. Select the individual feeds to install, when prompted and click **Install**.

   > 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(s) 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:

Exabeam Alerts Parameters

PARAMETER	DESCRIPTION
API Hostname	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.

PARAMETER	DESCRIPTION
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.
Ingest Threat Summary	Select whether to request the Copilot Threat Summary for each alert.
Context Filter	Select one or more pieces of context to bring into ThreatQ with the event record. Options include: ◦ Status *(default)* ◦ Priority *(default)* ◦ Vendor *(default)* ◦ Product *(default)* ◦ Risk Score *(default)* ◦ 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)*

Exambeam Cases Parameters

PARAMETER	DESCRIPTION
API Hostname	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.
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.
Context Filter	Select one or more pieces of context to bring into ThreatQ with the event record. Options include: ◦ Case ID *(default)* ◦ Case Number *(default)* ◦ Stage *(default)* ◦ Assignee *(default)* ◦ Queue *(default)* ◦ Created By *(default)* ◦ Has Attachments *(default)*

PARAMETER	DESCRIPTION
	◦ Is Deleted *(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

Exabeam Cases

The Exabeam Cases feed searches Exabeam cases and ingests them as ThreatQ **Case** events. It includes case workflow fields such as case ID, case number, stage, assignee, and queue.

Sample Response:

```
{
  "alertId": "8c1f7292-b173-4d01-93a1-c927a0f4c2c8",
  "caseId": "2ee86830-7bc0-41d3-971a-48860d644800",
  "caseNumber": 483,
  "alertName": "Suspicious Cloud Resource Access",
  "alertDescription": "<p>Suspicious access to a protected cloud
resource.</p>",
  "creationTimestamp": "2025-04-04T01:10:12.000000Z",
  "ingestTimestamp": "2025-04-04T01:11:00.000000Z",
  "queue": "Tier 1 Analyst",
  "creationBy": "analyst@example.com",
  "assignee": "analyst@example.com",
  "stage": "NEW",
  "hasAttachments": true,
  "isDeleted": false
}
```

ThreatQ provides the following default mapping for **Exabeam Cases**:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
.alertName	Event Title	Case	N/A	.creationTimestamp	N/A	Identifies the case event.
.alertDescription or .alertDescriptionRt	Event Description	N/A	N/A	.creationTimestamp	N/A	Description from case response.
.ingestTimestamp	Event Happened At	N/A	N/A	.creationTimestamp	N/A	
.caseId	Event Attribute	Case ID	N/A	.creationTimestamp	N/A	Case identifier; configurable.
.caseNumber	Event Attribute	Case Number	N/A	.creationTimestamp	N/A	Workflow number; configurable.
.stage	Event Attribute	Stage	N/A	.creationTimestamp	N/A	Case workflow state.
.assignee	Event Attribute	Assignee	N/A	.creationTimestamp	N/A	Case owner; configurable.
.queue	Event Attribute	Queue	N/A	.creationTimestamp	N/A	Case queue; configurable.
.creationBy	Event Attribute	Created By	N/A	.creationTimestamp	N/A	Case creator; configurable.
.hasAttachments	Event Attribute	Has Attachments	N/A	.creationTimestamp	N/A	Case attachment state.
.isDeleted	Event Attribute	Is Deleted	N/A	.creationTimestamp	N/A	Case deletion state.

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": []
}
```


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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
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
.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

Exabeam Alerts

The Alerts feed searches Exabeam alerts and ingests them as ThreatQ **Alert** events. It can include the optional Copilot Threat Summary in the description.

Sample Response:


```
{
  "alertCreationTimestamp": "2025-04-04T01:09:48.934673Z",
  "alertId": "6d9e4771-4a68-449f-9aeb-4c799bcf5b3c",
  "approxLogTime": "2025-04-04T01:09:48.934673Z",
  "creationTimestamp": "2025-04-04T01:09:48.934673Z",
  "alertDescription": "
```

```
Multiple failed logins followed by access to a restricted resource.
```

```
", "mitres": [ { "tacticKey": "TA0006", "tactic": "Credential
Access", "techniqueKey": "T1110", "technique": "Brute Force" } ],
"alertName": "Repeated Authentication Failures", "priority": "HIGH",
"riskScore": 85, "status": "UNREAD", "tags": [ "authentication",
"high-risk" ], "useCases": [ "Credential Abuse" ], "products":
[ "Correlation Rule" ], "vendors": [ "Exabeam" ], "srcHosts":
[ "endpoint-42.example.com" ], "srcIps": [ "198.51.100.42" ],
"destHosts": [ "identity.example.com" ], "destIps":
[ "203.0.113.10" ], "users": [ "user@example.com" ],
"ingestTimestamp": "2025-04-04T01:10:05.000000Z", "srcEndpoints":
[ "endpoint-42" ], "destEndpoints": [ "identity-service" ], "rules":
[ "Repeated Authentication Failures" ], "detections_info": [] }
```


Threat Summary response:


```
{
  "summary": "A user account accessed a restricted resource; the
alert includes details about the associated activity."
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
.alertName	Event Title	Alert	N/A	.creationTimestamp	N/A	Identifies the alert event.
.copilotSummary	Event Description	N/A	N/A	.creationTimestamp	N/A	Optional; controlled by **Ingest Threat Summary**.
.alertDescription or .alertDescriptionRt	Event Description	N/A	N/A	.creationTimestamp	N/A	Used when summary is unavailable.
.ingestTimestamp	Event Happened At	N/A	N/A	.creationTimestamp	N/A	
.status	Event Attribute	Status	N/A	.creationTimestamp	N/A	Alert read state; updatable.
.priority	Event Attribute	Priority	N/A	.creationTimestamp	N/A	Updatable; configurable.
.vendors[]	Event Attribute	Vendor	N/A	.creationTimestamp	N/A	Configurable.
.products[]	Event Attribute	Product	N/A	.creationTimestamp	N/A	Configurable.
.riskScore	Event Attribute	Risk Score	N/A	.creationTimestamp	N/A	Updatable; configurable.
.approxLogTime	Event Attribute	Approx Log Time	N/A	.creationTimestamp	N/A	Updatable; configurable.
.useCases[]	Event Attribute	Use Case	N/A	.creationTimestamp	N/A	Configurable.
.srcHosts[], .destHosts[]	Event Attribute	Source Hosts, Destination Hosts	N/A	N/A	N/A	Configurable.
.tags[]	Event Tag	N/A	N/A	N/A	N/A	
.srcIps[], .destIps[]	Related Indicator	IP Address	N/A	.creationTimestamp	N/A	Configurable.
.mitres[].tacticKey, .mitres[].tactic	Related Attack Pattern	N/A	N/A	N/A	N/A	Configurable; creates or relates tactics.
.mitres[].techniqueKey, .mitres[].technique	Related Attack Pattern	N/A	N/A	N/A	N/A	Configurable; creates or relates techniques.

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.

Exabeam Cases

METRIC	RESULT
Run Time	1 minute
Events	2
Event Attributes	16

Exabeam Alerts

METRIC	RESULT
Run Time	1 minute
Events	10
Event Attributes	136
Indicators	2
Attack Patterns	14

Known Issues / Limitations

- Exabeam does not provide Copilot Threat Summaries for manually created cases.

Change Log

- **Version 2.0.0**
  - Replaced the Events feed with separate Alerts and Cases feeds. Added optional ingestion of Copilot Threat Summaries for alerts.
- **Version 1.0.0**
  - Initial release