ThreatQuotient

Abnormal Security CDF User Guide

Version 1.0.0

October 10, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Not Actively Supported

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 **Not Actively Supported**.

Integrations, apps, and add-ons designated as **Not Actively Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Actively Supported integrations/apps/add-ons.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	Not Actively Supported

Introduction

The Abnormal Security CDF enables analysts to automatically ingest their Abnormal Security Cases & Threats into ThreatQ.

The integration provides the following feeds:

- **Abnormal Security - Cases** - ingests cases from Abnormal Security and creates incidents in ThreatQ
- **Abnormal Security - Threats** - ingests threats from Abnormal Security and creates incidents in ThreatQ

The integration ingests the following system objects:

- Incidents
- Events
- Identities
- Indicators

Prerequisites

An Abnormal Security License and API Key are required to use this integration. You can generate an API key from: https://portal.abnormalsecurity.com/home/settings/integrations.

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:

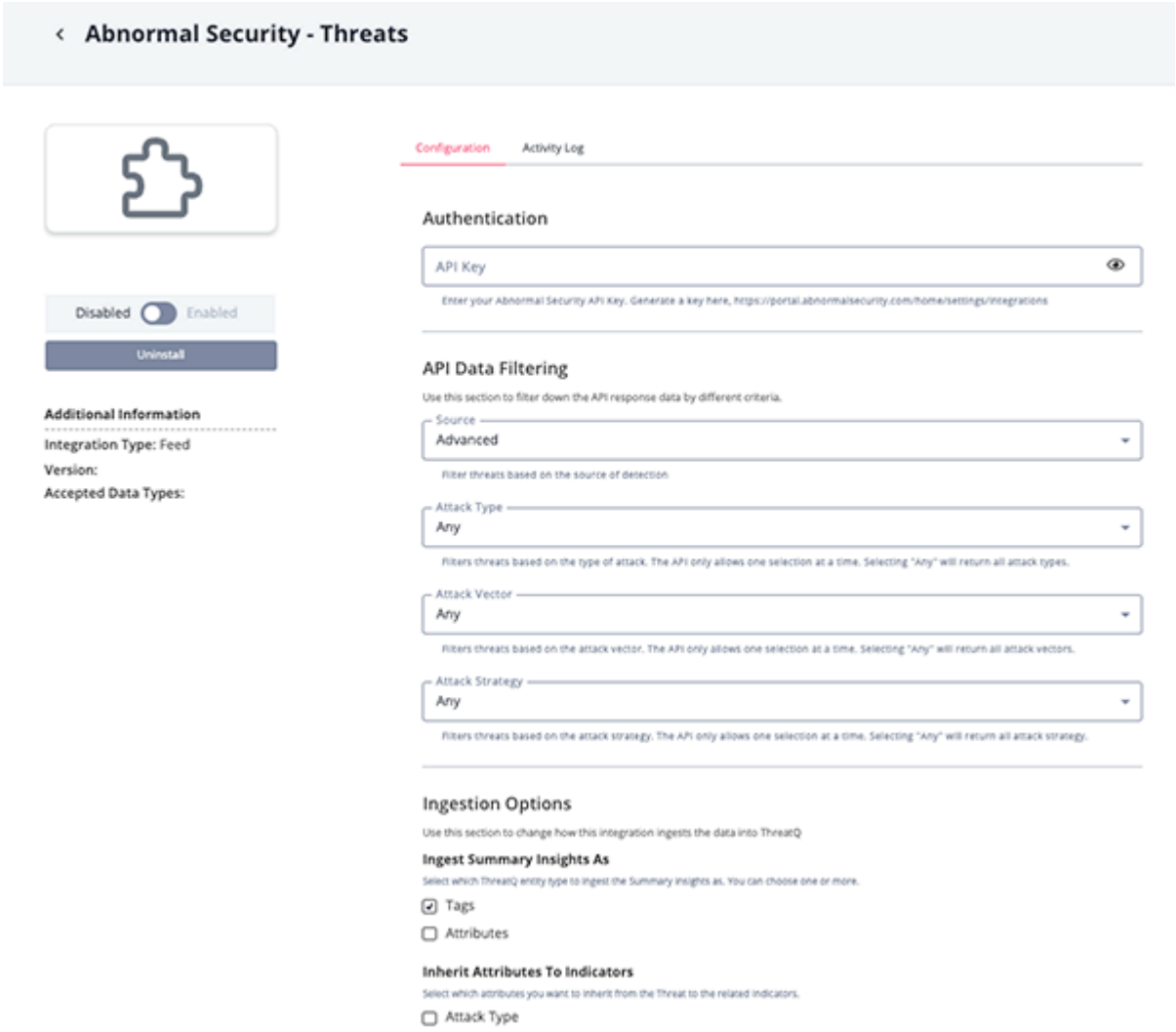
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
	AUTHENTICATION
API Key	Enter your Abnormal Security API Key.
	API DATA FILTERING *(Abnormal Security Threats feed only)*
Source	Filter threats based on the source of detection. Options include **Advanced** (default) and **All**.
Attack Type	Filter threats based on the type of attack. The API only allows one selection at a time. Selecting **Any** will return all attack types. Options include: ◦ Any (default) ◦ Internal-to-Internal Attacks (Email Account Takeover) ◦ Spam ◦ Reconnaissance ◦ Scam ◦ Social Engineering (BEC) ◦ Phishing: Credential ◦ Invoice/Payment Fraud (BEC) ◦ Malware ◦ Extortion ◦ Phishing: Sensitive Data

PARAMETER	DESCRIPTION
	◦ Other
Attack Vector	Filter threats based on the attack vector. The API only allows one selection at a time. Selecting **Any** will return all attack vectors. Options include: ◦ Any (default) ◦ Link ◦ Attachment ◦ Text ◦ Others ◦ Attachment with zipped files
Attack Strategy	Filter threats based on the attack strategy. The API only allows one selection at a time. Selecting **Any** will return all attack strategy. Options include: ◦ Any (default) ◦ Name Impersonation ◦ Internal Compromised Email Account ◦ External Compromised Email Account ◦ Spoofed Email ◦ Unknown Sender ◦ COVID 19 Related Attack
	INGESTION OPTIONS
Ingest Summary Insights As	Select which ThreatQ entity type to ingest the Summary Insights. Options include **Tags** (default) and **Attributes**.
Inherit Attributes to Indicators	Select which attributes you want to inherit to the related Indicators.



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

Abnormal Security - Cases

The Abnormal Security - Cases feed periodically pulls threats from Abnormal Security and creates incidents in ThreatQ.

`GET https://api.abnormalplatform.com/v1/threats`

Sample Response:

```
{
  "threats": [
    {
      "threatId": "184712ab-6d8b-47b3-89d3-a314efef79e2"
    }
  ],
  "pageNumber": 1,
  "nextPageNumber": 2
}
```

The mapping for this feed is defined within the following supplemental feed mappings:

- Abnormal Security - Get Case Details
- Abnormal Security - Get Case Analysis
- Abnormal Security - Get Threat Details

Abnormal Security - Threats

The Abnormal Security - Threats feed periodically pulls threats from Abnormal Security and creates incidents in ThreatQ.

```
GET https://api.abnormalplatform.com/v1/threats
```

Sample Response:

```
{
  "threats": [
    {
      "threatId": "184712ab-6d8b-47b3-89d3-a314efef79e2"
    }
  ],
  "pageNumber": 1,
  "nextPageNumber": 2
}
```

The mapping for this feed is defined within the following supplemental feed mappings:

- Abnormal Security - Get Threat Details
- Abnormal Security - Get Threat Relationship

Abnormal Security - Get Case Details (Supplemental)

The Abnormal Security - Get Case Details supplemental feed fetches the full case details for a given case ID.

```
GET https://api.abnormalplatform.com/v1/cases/{case_id}
```

Sample Response:

```
{
  "caseId": "1234",
  "severity": "Potential Account Takeover",
  "affectedEmployee": "John Doe",
  "firstObserved": "2020-06-09T17:42:59Z",
  "threatIds": ["184712ab-6d8b-47b3-89d3-a314efef79e2"]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.caseId`	Incident.Attribute	Case ID	N/A	`1234`	N/A
`.severity`	Incident.Attribute	Severity	N/A	`Potential Account Takeover`	N/A
`.affectedEmployee`	Incident.Attribute	Affected Employee	N/A	`John Doe`	N/A
`.caseId`, `.severity`, `affectedEmployee`	Incident.Value	N/A	`.firstObserved`	`1234 - Potential Account Takeover - John Doe`	N/A
`.threatIds[]`	Incident.Attribute	Threat Count	N/A	`1`	List Length

Abnormal Security - Get Case Analysis (Supplemental)

The Abnormal Security - Get Case Analysis supplemental feed fetches the analysis for a given case.

`GET https://api.abnormalplatform.com/v1/cases/{case_id}/analysis`

Sample Response:


```
{
  "threatId": "184712ab-6d8b-47b3-89d3-a314efef79e2",
  "messages": [
    {
      "threatId": "184712ab-6d8b-47b3-89d3-a314efef79e2",
      "abxMessageId": 4551618356913732000,
      "abxPortalUrl": "https://portal.abnormalsecurity.com/home/threat-center/
remediation-history/4551618356913732076",
      "subject": "Phishing Email",
      "fromAddress": "support@secure-reply.org",
      "fromName": "Support",
      "senderDomain": "secure-reply.org",
      "toAddresses": "example@example.com, another@example.com",
      "recipientAddress": "example@example.com",
      "receivedTime": "2020-06-09T17:42:59Z",
      "sentTime": "2020-06-09T17:42:59Z",
      "internetMessageId": "<5edfca1c.1c69fb81.4b055.8fd5@mx.google.com>",
      "remediationStatus": "Auto Remediated",
      "attackType": "Extortion",
      "attackStrategy": "Name Impersonation",
      "returnPath": "support@secure-reply.org",
      "replyToEmails": ["reply-to@example.com"],
      "ccEmails": ["cc@example.com"],
      "senderIpAddress": "100.101.102.103",
      "impersonatedParty": "None / Others",
      "attackVector": "Text",
      "attachmentNames": ["attachment.pdf"],
      "attachmentCount": 0,
      "urls": ["https://www.google.com/"],
      "urlCount": 0,
      "summaryInsights": [
        "Bitcoin Topics",
        "Personal Information Theft",
        "Unusual Sender"
      ],
      "remediationTimestamp": "2020-06-09T17:42:59Z",
      "isRead": true,
      "attackedParty": "VIP",
      "autoRemediated": true,
      "postRemediated": false
    }
  ],
```

```
  "pageNumber": 1,
  "nextPageNumber": 2
}
```

ThreatQuotient provides the following default mapping for this feed:

> The following mapping is based on fields within each of the `messages`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attackType`, `.subject`, `.fromAddress`, `recipientAddress`, `abxMessageId`	Event.Title	N/A	`.receivedTime`	`ABX Threat (Extortion): Phishing Email; support@secure-reply.org -> example@example.com; ID: 4551618356913732000`	Fields are concatenated together
`.threatId`	Event.Attribute	Threat ID	`.receivedTime`	`184712ab-6d8b-47b3-89d3-a314efef79e2`	N/A
`.attackType`	Event.Attribute	Attack Type	`.receivedTime`	`Extortion`	N/A
`.fromAddress`	Indicator.Value	Email Address	`.receivedTime`	`support@secure-reply.org`	N/A
`.urls[]`	Indicator.Value	URL	`.receivedTime`	`https://www.google.com/`	N/A
`.senderIpAddress`	Indicator.Value	IP Address	`.receivedTime`	`100.101.102.103`	N/A
`.abxPortalUrl`	Event.Attribute	ABX Portal Link	`.receivedTime`	`https://portal.abnormalsecurity.com/home/threat-center/remediation-history/4551618356913732076`	N/A
`.subject`	Event.Attribute	Subject	`.receivedTime`	`Phishing Email`	N/A
`.recipientAddress`	Event.Identity	N/A	`.receivedTime`	`example@example.com`	N/A
`.sentTime`	Event.Attribute	Sent At	`.receivedTime`	`2020-06-09T17:42:59Z`	N/A
`.receivedTime`	Event.Attribute	Received At	`.receivedTime`	`2020-06-09T17:42:59Z`	N/A
`.remediationStatus`	Event.Attribute	Remediation Status	`.receivedTime`	`Auto Remediated`	N/A
`.attackStrategy`	Event.Attribute	Attack Strategy	`.receivedTime`	`Name Impersonation`	N/A
`.replyToEmails[]`	Event.Attribute	Reply To Address	`.receivedTime`	`reply-to@example.com`	N/A
`.impersonatedParty`	Event.Attribute	Impersonated Party	`.receivedTime`	`None / Others`	N/A
`.attackedParty`	Event.Attribute	Attacked Party	`.receivedTime`	`VIP`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attackVector`	Event.Attribute	Attack Vector	`.receivedTime`	`Text`	N/A
`.summaryInsights[]`	Event.Attribute/ Event.Tag	Summary Insight	`.receivedTime`	`Personal Information Theft`	Depends on `Ingest Summary Insights As` user config
`.isRead`	Event.Attribute	Is Read	`.receivedTime`	`true`	N/A
`.autoRemediated`	Event.Attribute	Auto Remediated	`.receivedTime`	`true`	N/A
`.remediationTimestamp`	Event.Attribute	Remediated At	`.receivedTime`	`2020-06-09T17:42:59Z`	N/A

Abnormal Security - Get Threat Details (Supplemental)

Abnormal Security - Get Threat Details supplemental feed that fetches the details for a given threat by its' ID.

`GET https://api.abnormalplatform.com/v1/threats/{threat_id}`

Sample Response:


```
{
  "threatId": "184712ab-6d8b-47b3-89d3-a314efef79e2",
  "messages": [
    {
      "threatId": "184712ab-6d8b-47b3-89d3-a314efef79e2",
      "abxMessageId": 4551618356913732000,
      "abxPortalUrl": "https://portal.abnormalsecurity.com/home/threat-center/
remediation-history/4551618356913732076",
      "subject": "Phishing Email",
      "fromAddress": "support@secure-reply.org",
      "fromName": "Support",
      "senderDomain": "secure-reply.org",
      "toAddresses": "example@example.com, another@example.com",
      "recipientAddress": "example@example.com",
      "receivedTime": "2020-06-09T17:42:59Z",
      "sentTime": "2020-06-09T17:42:59Z",
      "internetMessageId": "<5edfca1c.1c69fb81.4b055.8fd5@mx.google.com>",
      "remediationStatus": "Auto Remediated",
      "attackType": "Extortion",
      "attackStrategy": "Name Impersonation",
      "returnPath": "support@secure-reply.org",
      "replyToEmails": ["reply-to@example.com"],
      "ccEmails": ["cc@example.com"],
      "senderIpAddress": "100.101.102.103",
      "impersonatedParty": "None / Others",
      "attackVector": "Text",
      "attachmentNames": ["attachment.pdf"],
      "attachmentCount": 0,
      "urls": ["https://www.google.com/"],
      "urlCount": 0,
      "summaryInsights": [
        "Bitcoin Topics",
        "Personal Information Theft",
        "Unusual Sender"
      ],
      "remediationTimestamp": "2020-06-09T17:42:59Z",
      "isRead": true,
      "attackedParty": "VIP",
      "autoRemediated": true,
      "postRemediated": false
    }
```

```
  ],
  "pageNumber": 1,
  "nextPageNumber": 2
}
```

ThreatQuotient provides the following default mapping for this feed:

> The following mapping is based on fields within each of the `messages`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attackType`, `.subject`, `.fromAddress`, `recipientAddress`, `abxMessageId`	Event.Title	N/A	`.received Time`	`ABX Threat (Extortion): Phishing Email; support@secure-reply.org -> example@example.com; ID: 4551618356913732000`	Fields are concatenated together
`.threatId`	Event.Attribute	Threat ID	`.received Time`	`184712ab-6d8b-47b3-89d3-a314efef79e2`	N/A
`.attackType`	Event.Attribute	Attack Type	`.received Time`	`Extortion`	N/A
`.fromAddress`	Indicator.Value	Email Address	`.received Time`	`support@secure-reply.org`	N/A
`.urls[]`	Indicator.Value	URL	`.received Time`	`https://www.google.com/`	N/A
`.senderIpAddress`	Indicator.Value	IP Address	`.received Time`	`100.101.102.103`	N/A
`.abxPortalUrl`	Event.Attribute	ABX Portal Link	`.received Time`	`https://portal.abnormalsecurity.com/home/threat-center/remediation-history/4551618356913732076`	N/A
`.subject`	Event.Attribute	Subject	`.received Time`	`Phishing Email`	N/A
`.recipientAddress`	Event.Identity	N/A	`.received Time`	`example@example.com`	N/A
`.sentTime`	Event.Attribute	Sent At	`.received Time`	`2020-06-09T17:42:59Z`	N/A
`.receivedTime`	Event.Attribute	Received At	`.received Time`	`2020-06-09T17:42:59Z`	N/A
`.remediationStatus`	Event.Attribute	Remediation Status	`.received Time`	`Auto Remediated`	N/A
`.attackStrategy`	Event.Attribute	Attack Strategy	`.received Time`	`Name Impersonation`	N/A
`.replyToEmails[]`	Event.Attribute	Reply To Address	`.received Time`	`reply-to@example.com`	N/A
`.impersonatedParty`	Event.Attribute	Impersonated Party	`.received Time`	`None / Others`	N/A
`.attackedParty`	Event.Attribute	Attacked Party	`.received Time`	`VIP`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attackVector`	Event.Attribute	Attack Vector	`.receivedTime`	`Text`	N/A
`.summaryInsights[]`	Event.Attribute/ Event.Tag	Summary Insight	`.receivedTime`	`Personal Information Theft`	Depends on `Ingest Summary Insights As` user config
`.isRead`	Event.Attribute	Is Read	`.receivedTime`	`true`	N/A
`.autoRemediated`	Event.Attribute	Auto Remediated	`.receivedTime`	`true`	N/A
`.remediationTimestamp`	Event.Attribute	Remediated At	`.receivedTime`	`2020-06-09T17:42:59Z`	N/A

Abnormal Security - Get Threat Relationship (Supplemental)

The Abnormal Security - Get Threat Relationship supplemental feed that fetches relationships for a given threat

`GET https://api.abnormalplatform.com/v1/threats/{threat_id}/{relationship_type}`

Relationship Type: Links

Sample Response:

```
{
  "threats": [
    {
      "abxMessageId": 4551618356913732000,
      "domainLink": "lamronba.com",
      "linkType": "html href",
      "source": "body",
      "displayText": "This is not a spoof!",
      "linkUrl": "http://spoof.lamronba.com"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.linkUrl`	Indicator.Value	URL	N/A	N/A	N/A

Relationship Type: Attachment

Sample Response:

```
{
  "threats": [
    {
      "abxMessageId": 4551618356913732000,
      "attachmentName": "attachment1.jpg"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.attachmentName`	Indicator.Value	Filename	N/A	N/A	N/A

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.

Abnormal Security - Cases

METRIC	RESULT
Run Time	1 minute
Incident	1
Incident Attributes	5
Indicators	2
Events	2
Event Attributes	32
Identities	2

Abnormal Security - Threats

METRIC	RESULT
Run Time	1 minute
Indicators	2

METRIC	RESULT
Events	2
Event Attributes	32
Identities	2

Change Log

- **Version 1.0.0**
  - Initial release