ThreatQuotient

A Securonix Company

TruKno CDF

Version 1.0.0

August 03, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-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	1.0.0
Compatible with ThreatQ Versions	>= 6.5.0
Support Tier	ThreatQ Supported

Introduction

The **TruKno CDF** integration imports breach intelligence from TruKno into ThreatQ, enabling organizations to centralize breach reports and the associated threat context within a single platform. During ingestion, the integration retrieves breach summaries, collects the full details for each breach, and creates ThreatQ reports enriched with related indicators, vulnerabilities (including CVEs), MITRE ATT&CK attack patterns, adversaries, malware, tools, and additional contextual attributes. This enables analysts to correlate breach intelligence with existing ThreatQ data and accelerate investigation and response activities.

The integration provides the following feed:

- **TruKno Breaches** - Imports TruKno breach reports and their associated threat intelligence.

The integration ingests the following ThreatQ objects:

- Adversaries
    - Adversary Attributes
- Attack Patterns
- Indicators
- Malware
- Reports
    - Report Attributes
- Tools
    - Tool Attributes
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- TruKno enterprise API access.
- Either a TruKno API key or a valid TruKno username and password with permission to access the TruKno 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 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(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:

PARAMETER	DESCRIPTION
Authentication Type	Select the authentication method used to access the TruKno API. ◦ **Username & Password** (default) ◦ **API Key**
Email	Enter your TruKno email address. This field is required when `Username & Password` authentication is selected for the **Authentication Type** parameter.
Password	Enter your TruKno password. This field is required when `Username & Password` authentication is selected for the **Authentication Type** parameter.
API Key	Enter your TruKno API key. This field is required when `API Key` authentication is selected for the **Authentication Type** parameter.
Search Keyword (Optional)	Optional - enter a keyword to limit results to breach reports containing the specified term.

PARAMETER	DESCRIPTION
Category Filter	Select one or more breach categories to ingest. Selecting **All** ignores all other selections. Options include: ◦ All *(default)* ◦ Application Security ◦ Artificial Intelligence (AI) ◦ Blockchain ◦ Breach Testing & Simulation ◦ Cloud Security ◦ Consumer Security ◦ Cyber Attacks Insurance ◦ Cyber Crimes ◦ Cyber Training & Simulation ◦ DDoS Attacks ◦ Data Privacy & Security ◦ Data Security ◦ Digital Risk Management ◦ Email & Messaging Security ◦ Email Security ◦ Encryption ◦ Endpoint Security ◦ Fraud & Transaction Security ◦ Fraud Security ◦ Hardware Security ◦ IoT Security ◦ Identity & Access ◦ Insider Threats ◦ Internet Bots ◦ Intrusion Detection & Prevention

PARAMETER	DESCRIPTION
	◦ MSSP ◦ Miscellaneous ◦ Mobile Security ◦ Network Design ◦ Network Design & Monitoring ◦ Network Security ◦ Network Security & Performance ◦ Network Visibility & Monitoring ◦ Network and Infrastructure Technology ◦ OT / ICS Security ◦ Other ◦ Phishing Attacks ◦ Physical Security ◦ Prevalent Networks ◦ Risk & Compliance ◦ SOC ◦ Security Awareness & Training ◦ Security Consulting & Services ◦ Security Operations ◦ Security Operations & Incident Response ◦ Supply Chain Attacks ◦ Threat Intelligence ◦ User Privacy ◦ Voice & Video Security ◦ Voice / Video Collaboration ◦ Vulnerability & Risk Management ◦ Web Security ◦ Wi-Fi Security

PARAMETER	DESCRIPTION
	◦ Wireless Security
Malware Type Filter	Select one or more malware types to ingest. Selecting **All** ignores all other selections. Options include: ◦ All *(default)* ◦ Adware ◦ Backdoor ◦ Banking Trojan ◦ Botnet ◦ Campaign ◦ Code Implant ◦ Compression ◦ CryptoMiner ◦ Dark Web ◦ Darkweb Forum ◦ Digital Skimmer ◦ Downloader ◦ Framework ◦ Info Stealer ◦ Mobile Ransomware ◦ Mobile Spyware ◦ Phishing Campaign ◦ POS Malware ◦ Ransomware ◦ RAT ◦ Rootkit ◦ Service Manager Tool ◦ Spyware ◦ TrickBot

PARAMETER	DESCRIPTION
	◦ Trojan ◦ UEFI Bootkit ◦ UEFI Rootkit ◦ Web Hook ◦ Web Shell ◦ Web Skimmer ◦ Worm
Industry Filter	Select one or more industries to ingest. Selecting **All** ignores all other selections. Options include: ◦ All *(default)* ◦ Education ◦ Electronics & Semiconductors ◦ Energy & Utility ◦ Finance ◦ Government ◦ Healthcare ◦ Industrial ◦ Media & Entertainment ◦ Professional Services ◦ Real Estate ◦ Retail & E-Commerce ◦ Software & IT ◦ Telecom & MSP ◦ Transportation ◦ Travel ◦ Other

PARAMETER	DESCRIPTION
Context Filter	Select the contextual information to import into ThreatQ. Only the selected fields are ingested. Options include: ◦ Affected Industry *(default)* ◦ Affected Technology *(default)* ◦ Category *(default)* ◦ Source *(default)* ◦ Author ◦ Service ◦ Related CVEs *(default)* ◦ Related Indicators *(default)* ◦ Related Malware *(default)* ◦ Related Tools *(default)* ◦ Related MITRE Techniques *(default)* ◦ Related Threat Actors *(default)*
Ingest CVEs As	Select how related CVEs are represented in ThreatQ. Options include: ◦ **Vulnerabilities** *(default)* ◦ **Indicators (CVEs)**
Inherit Relationships to Related IOCs	Optional - inherit report relationships to related indicators. Options Include: ◦ Related Threat Actors ◦ Related Malware

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

TruKno Breaches

The TruKno Breaches feed retrieves paginated breach summaries from the TruKno API v2. For each breach returned, the feed uses the breach ID to retrieve the complete breach details, including report metadata, indicators of compromise (IOCs), CVEs, MITRE ATT&CK techniques, threat actors, malware, tools, services, and other related threat intelligence.

```
GET https://api.trukno.com/v2/breaches/list
```

Sample Response:


```
{
  "results": [
    {
      "_id": "6a3190955945e980453a9b6e",
      "category": ["Network Security", "Hardware Security"],
      "description": "A new Gafgyt botnet variant, C0XMO, that
spreads by exploiting CVE-2021-27137.",
      "source": "Fortinet",
      "title": "Inside the Cross-Platform Propagation of a New Gafgyt
Variant C0XMO",
      "url": "https://www.fortinet.com/blog/threat-research/inside-
cross-platform-propagation-of-new-gafgyt-variant-c0xmo",
      "ttpsCount": 19,
      "cvesCount": 5,
      "actorsCount": 0,
      "malwareCount": 1,
      "date": "2026-06-16T18:04:47.000Z",
      "affectedIndustries": ["Software  IT"],
      "affectedTechnologies": ["Linux (Endpoint OS)", "Linux (Server
OS)"],
      "detectionRulesCount": 0
    }
  ],
  "metadata": {
    "page": "1",
    "totalCount": 14,
    "totalPages": 2,
    "limit": 10,
```

```
    "start_date": "2026-06-15T00:00:00.000Z",
    "end_date": "2026-06-18T23:59:59.000Z"
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

> The list response is used to collect breach IDs. ThreatQ object mapping is performed from the supplemental GET `https://api.trukno.com/v2/breaches/{id}` breach detail response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Report.Value	N/A	.date	Inside the Cross-Platform Propagation of a New Gafgyt Variant C0XMO	N/A
.description, .url, .relatedTTPs[].procedure	Report.Description	N/A	N/A	A new Gafgyt botnet variant, C0XMO...	Formatted into HTML description.
.source	Report.Attribute	Source	.date	Fortinet	User-Configurable
.author	Report.Attribute	Author	.date	N/A	User-Configurable
.category[]	Report.Attribute	Category	.date	Network Security	User-Configurable
.affectedIndustries[]	Report.Attribute	Target Industry	.date	Software & IT	User-Configurable
.affectedTechnologies[]	Report.Attribute	Target Product	.date	Linux (Endpoint OS)	User-Configurable
.relatedServices[].name	Report.Attribute	Service	.date	N/A	User-Configurable
.iocs[].ioc	Indicator.Value	See IOC Type Mapping	.date	217.160.125.125	User-Configurable
.relatedCVEs[].name	Vulnerability.Value or Indicator.Value	Vulnerability or CVE	.date	CVE-2015-2051	User-Configurable
.relatedCVEs[].description	Vulnerability.Description or Indicator.Description	N/A	N/A	The D-Link DIR-645 Wired/ Wireless Router...	User-Configurable
.relatedCVEs[].tags[]	Vulnerability.Tag or Indicator.Tag	N/A	N/A	N/A	User-Configurable
.relatedCVEs[].vendors[]	Vulnerability.Attribute or Indicator.Attribute	Target Vendor	.date	dlink	User-Configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.relatedCVEs[].products[]	Vulnerability.Attribute or Indicator.Attribute	Target Product	.date	dir-645_firmware	User-Configurable
.relatedCVEs[].baseScore	Vulnerability.Attribute or Indicator.Attribute	CVSS Base Score	.date	9.8	User-Configurable
.relatedCVEs[].baseSeverity	Vulnerability.Attribute or Indicator.Attribute	CVSS Base Severity	.date	CRITICAL	User-Configurable
.relatedTTPs[]	Attack Pattern.Value	N/A	.date	T1110.001 - Password Guessing	User-Configurable
.relatedTTPs[].description	Attack Pattern.Description	N/A	N/A	Adversaries with no prior knowledge...	User-Configurable
.relatedMalware[]	Malware.Value	N/A	.date	C0XMO Botnet	User-Configurable
.relatedActors[].name	Adversary.Name	N/A	.date	N/A	User-Configurable
.relatedActors[].location	Adversary.Attribute	Country	.date	N/A	User-Configurable
.relatedTools[].malwareName	Tool.Value	N/A	.date	N/A	User-Configurable
.relatedTools[].malwareType	Tool.Attribute	Type	.date	N/A	User-Configurable

IOC Type Mapping

The following table describes how indicator types returned by the TruKno API are mapped to their corresponding ThreatQ indicator types during ingestion.

TRUKNO IOC TYPE	THREATQ INDICATOR TYPE
`hash-md5`	MD5
`hash-sha1`	SHA-1
`hash-sha256`	SHA-256
`hash-sha512`	SHA-512
`ip`	IP Address
`ipv6`	IPv6 Address
`domain`	FQDN
`hostname`	FQDN
`url`	URL
`email`	Email Address
`mutex`	Mutex

CVE Value Mapping

The following table describes how the **Ingest CVEs As** configuration determines the ThreatQ object type used when importing related CVEs from TruKno.

INGEST CVES AS VALUE	THREATQ OBJECT TYPE
`vulnerability`	Vulnerability
`indicators`	Indicator (CVE)

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
Adversaries	3
Adversary Attributes	2
Attack Patterns	187
Indicators	208
Malware	38
Reports	19
Report Attributes	86
Tools	6
Tool Attributes	6

Known Issues / Limitations

- **API Rate Limits:** The TruKno API enforces a limit of **200 requests per minute** per client. Large data retrieval operations may require additional time if the rate limit is reached.
- **Indicator Classification:** TruKno may include domains that are not inherently malicious as indicators of compromise (IOCs). To support analyst review, related indicators are ingested into ThreatQ with a default status of **Review**.

Change Log

- **Version 1.0.0**
  - Initial release