

ThreatQuotient

A Securonix Company



ThreatBook CDF

Version 1.0.0

October 13, 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	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	8
Installation	9
Configuration	10
ThreatBook IPs & ThreatBook IOCs	10
ThreatBook Hashes & ThreatBook URLs	11
ThreatBook Reports	12
ThreatQ Mapping	15
ThreatBook IPs	15
ThreatBook IOCs	17
ThreatBook Hashes	19
ThreatBook URLs	21
ThreatBook Reports	23
Average Feed Run	26
ThreatBook IPs	26
ThreatBook IOCs	26
ThreatBook Hashes	26
ThreatBook URLs	27
ThreatBook Reports	27
Known Issues / Limitations	29
Change Log	30

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: 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 ThreatBook CDF integration automatically ingests ThreatBook threat intelligence feeds and reports into ThreatQ to support intelligence analysis, enrichment, and operational workflows. ThreatBook provides STIX-based IOC and reputation intelligence, as well as contextual reports that can include attribution, affected targets, CVEs, IOCs, MITRE ATT&CK techniques, and detection rules.

The integration provides the following feeds:

- **ThreatBook IPs** - ingests ThreatBook IP reputation intelligence as IP Address indicators with verdict, threat type, and STIX metadata.
- **ThreatBook IOCs** - ingests ThreatBook IOC intelligence as supported indicator types, including domains, IP addresses, URLs, and hashes, with associated verdict and threat context.
- **ThreatBook Hashes** - ingests malicious file hashes as hash indicators with associated verdict, threat type, and threat name attributes.
- **ThreatBook URLs** - ingests malicious URL intelligence as URL indicators with associated verdict and STIX metadata.
- **ThreatBook Reports** - ingests ThreatBook threat intelligence reports with associated IOCs, CVEs, MITRE ATT&CK techniques, detection rules, and contextual threat data.

The integration ingests the following object types:

- Adversaries
- Attack Patterns
- Campaigns
- Courses of Action
- Events
- Identities
- Indicators
- Incidents
- Infrastructure
- Intrusion Sets
- Malware
- Notes

- Reports
- Signatures
- Tools
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A ThreatBook API Key
 - Obtain a ThreatBook API key with access to the ThreatBook feed and report APIs used by this integration.
 - Add the ThreatQ instance egress IP address to the ThreatBook **IP Access** allowlist.
 - To generate an API key, sign in to the ThreatBook portal and go to **Integration > API**.
 - Hosted ThreatQ customers must contact ThreatQuotient/Securonix Support to obtain their instance egress IP address.
 - The integration uses a bearer token in the `Authorization` header to authenticate STIX feed requests and passes the API key as the `apikey` query parameter for report requests.

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(s).

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:

ThreatBook IPs & ThreatBook IOCs

PARAMETER	DESCRIPTION
API Key	Required. Enter the ThreatBook API key used to authenticate the integration.
Save Intrusion Sets As	Select the ThreatQ object type used to ingest Threat Actor data provided as STIX Intrusion Sets. ThreatQuotient recommends selecting Adversaries to consolidate related threat actor information into a single profile. ◦ Adversaries (default) ◦ Intrusion Sets
Ingest STIX Patterns as Signatures	Select this option to create ThreatQ Signatures that preserve the original STIX pattern when the integration parses STIX 2.0 Indicator objects. The integration always extracts atomic IOCs from supported STIX patterns and ingests them as individual ThreatQ Indicators. Default: <u>False</u> .

PARAMETER	DESCRIPTION
Process & Parse Labels	Select this option to parse STIX 2.x object labels that contain contextual information in key-value format. The integration attempts to ingest parsed values as dedicated ThreatQ Attributes or tags. When disabled, the integration preserves STIX object labels as generic ThreatQ Attributes.
Convert MITRE Kill Chain Phases to Tactics	Select this option to normalize MITRE ATT&CK kill chain phases as Tactic attributes and map their values to standard MITRE ATT&CK tactic names. When disabled, the integration ingests kill chain phases using the Kill Chain: mitre-attack attribute. Default: True.
Ignored Attributes	Select parser-generated attributes to exclude from ingestion. ◦ External Reference ◦ Modified At ◦ Revoked ◦ Valid From ◦ Valid Until

ThreatBook Hashes & ThreatBook URLs

PARAMETER	DESCRIPTION
API Key	Required. Enter the ThreatBook API key used to authenticate the integration.
Save Intrusion Sets As	Select the ThreatQ object type used to ingest Threat Actor data provided as STIX Intrusion Sets. ThreatQuotient recommends selecting Adversaries to consolidate related threat actor information into a single profile. Options include Adversaries (default) and Intrusion Sets.

PARAMETER	DESCRIPTION
Ingest STIX Patterns as Signatures	Select this option to create ThreatQ Signatures that preserve the original STIX pattern when the integration parses STIX 2.0 Indicator objects. The integration extracts atomic IOCs from supported STIX patterns and ingests them as individual ThreatQ Indicators. Default: <code>False</code> .
Process & Parse Labels	Select this option to parse STIX 2.x object labels that contain contextual information in key-value format. The integration attempts to ingest parsed values as dedicated ThreatQ Attributes or tags. When disabled, the integration preserves STIX object labels as generic ThreatQ Attributes.
Convert MITRE Kill Chain Phases to Tactics	Select this option to normalize MITRE ATT&CK kill chain phases as Tactic attributes and map their values to standard MITRE ATT&CK tactic names. When disabled, the integration ingests kill chain phases using the <code>Kill Chain: mitre-attack</code> attribute. Default: <code>True</code> .
Ignored Attributes	Select parser-generated attributes to exclude from ingestion.

ThreatBook Reports



When querying ThreatBook reports, the integration sends the selected filters as API query parameters. Severity, threat type, category, target region, and target country values are sent as comma-separated lists. Enabled API flags are sent with a value of `true`.

PARAMETER	DESCRIPTION
API Key	Required. Enter the ThreatBook API key used to authenticate the integration.

PARAMETER	DESCRIPTION
Query	Optional. Enter keywords to search across indexed report fields, including report titles, summaries, tags, IOCs, CVE identifiers and names, target products, target organizations, and other relevant attributes.
Severity Selection	Select the report severity levels to ingest into ThreatQ. Options: Critical (default), High (default), and Low (default).
Threat Type Selection	Select the threat types of reports to ingest into ThreatQ. Options: APT , Ransomware , Supply Chain Attack , Phishing , Data Leakage , Data Breach , Crypto Mining , DDoS , and Others . All options are selected by default.
Category Selection	Select the report categories to ingest into ThreatQ. Options: Incident Analysis , Malware Analysis , Vulnerability Analysis , Summary Report , Security News , and Incident Response . All options are selected by default.
Target Region Filter	Enter a line-separated list of target regions used to filter reports. For example: financial-services, government, or technology.
Target Country Filter	Enter a line-separated list of target countries used to filter reports. For example: Italy, Mexico, or United States.
API Flags	Select one or more criteria to pass to the ThreatBook API. The integration ingests only reports that meet all selected criteria. ◦ Published by the ThreatBook ThreatLab Team ◦ Has Detection Rules ◦ Has CVEs ◦ Has IOCs

PARAMETER	DESCRIPTION
Inherit Context to IOCs	Select report context to inherit to associated IOCs. Inherited context can support Indicator Scoring Policies but may add noise if a report has lower-fidelity or incorrect attribution. Options: Threat Type (default), Severity (default), Target Industry , and Target Country .

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

ThreatBook IPs

GET <https://api.threatbook.io/v2/feeds/stix/ip-reputation>

Sample Response:

```
{
  "type": "bundle",
  "id": "bundle--90aae187bde94dfc22ca3a04082c3835",
  "spec_version": null,
  "objects": [
    {
      "created": "2016-04-10T23:16:22.000Z",
      "id": "indicator--c3989f32-bf98-b282-27b2-b2cad1b953bb",
      "indicator_types": ["malicious-activity"],
      "modified": "2026-04-03T12:32:25.000Z",
      "name": "mal_ip: 185.139.215.211",
      "pattern": "[ipv4-addr:value = '185.139.215.211']",
      "pattern_type": "stix",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2016-04-10T23:16:22.000Z",
      "valid_until": "2026-07-02T13:00:00.000Z",
      "x_threatbook_inbound_verdict": "malicious",
      "x_threatbook_labels": ["spam"]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.objects[].pattern</code>	Indicator.Value	IP Address	<code>.objects[].valid_from</code>	185.139.215.211	Parsed from the STIX pattern.
<code>.objects[].indicator_types[]</code>	Indicator.Attribute	Indicator Type	<code>.objects[].valid_from</code>	malicious-activity	Preserved as an attribute by default.
<code>.objects[].x_threatbook_labels[]</code>	Indicator.Attribute or Tag	Threat Type or Tag	<code>.objects[].valid_from</code>	spam	Converted to Threat Type: Spam. If label parsing is enabled, labels can be parsed into dedicated attributes or tags.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].x_threatbook_inbound_verdict	Indicator.Attribute	Verdict	.objects[].valid_from	malicious	Converted to Verdict: Malicious.
.objects[].modified	Indicator.Attribute	Modified At	.objects[].valid_from	2026-04-03T12:32:25.000Z	Updatable
.objects[].valid_from	Indicator.Attribute	Valid From	.objects[].valid_from	2016-04-10T23:16:22.000Z	Updatable
.objects[].valid_until	Indicator.Attribute	Valid Until	.objects[].valid_from	2026-07-02T13:00:00.000Z	Updatable
.objects[].revoked	Indicator.Attribute	Revoked	.objects[].valid_from	false	Updatable

ThreatBook IOCs

GET <https://api.threatbook.io/v2/feeds/stix/ioc>

Sample Response:

```
{
  "type": "bundle",
  "id": "bundle--b73d7403df90e3774681b1f9bf24a49f",
  "spec_version": null,
  "objects": [
    {
      "created": "2016-08-14T12:36:33.000Z",
      "id": "indicator--7bea616d-4685-25ab-d430-ac513e4e3c86",
      "indicator_types": ["malicious-activity"],
      "modified": "2026-07-02T13:21:41.000Z",
      "name": "sus_domain: defrost.cn",
      "pattern": "[domain-name:value = 'defrost.cn']",
      "pattern_type": "stix",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2016-08-14T12:36:33.000Z",
      "valid_until": "2026-07-02T14:00:00.000Z",
      "x_threatbook_labels": ["phishing"],
      "x_threatbook_outbound_verdict": "suspicious"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].pattern	Indicator.Value	Domain, IP Address, URL, Hash, or other parsed STIX observable type	.objects[].valid_from	defrost.cn	Parsed from the STIX pattern.
.objects[].indicator_types[]	Indicator.Attribute	Indicator Type	.objects[].valid_from	malicious-activity	Preserved as an attribute by default.
.objects[].x_threatbook_labels[]	Indicator.Attribute or Tag	Threat Type or Tag	.objects[].valid_from	phishing	Converted to Threat Type: Phishing. If label parsing is enabled, labels can be parsed into dedicated attributes or tags.
.objects[].x_threatbook_	Indicator.Attribute	Verdict	.objects[].valid_from	malicious	Converted to Verdict: Malicious when present.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
outbound_verdict					
.objects[].modified	Indicator.Attribute	Modified At	.objects[].valid_from	2026-07-02T13:21:41.000Z	Updatable
.objects[].valid_from	Indicator.Attribute	Valid From	.objects[].valid_from	2016-08-14T12:36:33.000Z	Updatable
.objects[].valid_until	Indicator.Attribute	Valid Until	.objects[].valid_from	2026-07-02T14:00:00.000Z	Updatable

ThreatBook Hashes

GET <https://api.threatbook.io/v2/feeds/stix/hash>

Sample Response:

```
{
  "type": "bundle",
  "id": "bundle--f472639b-06e3-4561-95fc-e2840055bed2",
  "spec_version": "2.1",
  "objects": [
    {
      "id": "indicator--0df590fb-913b-58e8-8b8f-45071f85b0ec",
      "type": "indicator",
      "name": "Malicious File",
      "x_threatbook_threat_classify": "Trojan",
      "x_threatbook_threat_name": "Phish",
      "x_threatbook_verdict": "malicious",
      "indicator_types": ["malicious-activity"],
      "valid_from": "2026-06-30T23:51:09.000Z",
      "pattern": "[file:hashes.'SHA-256' =
'9cf2d45d56d65399e5a0843231cfc4d3a06fda8554249876001ecc58be9a4004' ]",
      "pattern_type": "stix",
      "created": "2026-06-30T23:51:09.000Z",
      "modified": "2026-06-30T23:52:48.000Z",
      "spec_version": "2.1"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].pattern	Indicator.Value	MD5, SHA-1, SHA-256, SHA-384, or SHA-512	.objects[].valid_from	9cf2d45d56d65399e5a0843231cfc4d3a06fda8554249876001ecc58be9a4004	Parsed from the STIX file hash pattern.
.objects[].indicator_types[]	Indicator.Attribute	Indicator Type	.objects[].valid_from	malicious-activity	Preserved as an attribute by default.
.objects[].x_threatbook_verdict	Indicator.Attribute	Verdict	.objects[].valid_from	malicious	Converted to Verdict: Malicious.
.objects[].x_threatbook_threat_classify	Indicator.Attribute	Threat Type	.objects[].valid_from	Trojan	Converted to Threat Type: Trojan.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.objects[].x_threatbook_threat_name</code>	Indicator.Attribute	Threat Name	<code>.objects[].valid_from</code>	Phish	Converted to Threat Name: Phish.
<code>.objects[].modified</code>	Indicator.Attribute	Modified At	<code>.objects[].valid_from</code>	2026-06-30T23:52:48.000Z	Updatable
<code>.objects[].valid_from</code>	Indicator.Attribute	Valid From	<code>.objects[].valid_from</code>	2026-06-30T23:51:09.000Z	Updatable
<code>.objects[].valid_until</code>	Indicator.Attribute	Valid Until	<code>.objects[].valid_from</code>	2026-07-02T14:00:00.000Z	Updatable

ThreatBook URLs

GET <https://api.threatbook.io/v2/feeds/stix/url>

Sample Response:

```
{
  "type": "bundle",
  "id": "bundle--df862d08-c640-4e0f-acce-3d31e0f77632",
  "spec_version": "2.1",
  "objects": [
    {
      "id": "indicator--6295a42b-d1a0-5331-bef2-2d5dd7c95dc2",
      "type": "indicator",
      "name": "Malicious URL",
      "x_threatbook_verdict": "malicious",
      "indicator_types": ["malicious-activity"],
      "valid_from": "2026-06-29T22:54:42.000Z",
      "pattern": "[url:value = 'http://www.rapidfilestorage.com/updates/ya/wrtzr_ytab_b_1/win/version.txt?mFANbphHDbHlaBAoRgufBLnwKEIpTXohE']",
      "pattern_type": "stix",
      "created": "2026-06-29T22:54:42.000Z",
      "modified": "2026-06-29T22:54:42.000Z",
      "spec_version": "2.1"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.objects[.pattern]</code>	Indicator .Value	URL	<code>.objects[.valid_from]</code>	<code>http://www[.]rapidfilestorage[.]com/updates/ya/wrtzr_ytab_b_1/win/version.txt?mFANbphHDbHlaBAoRgufBLnwKEIpTXohE</code>	Parsed from the STIX URL pattern. URL normalization is disabled so query parameters are preserved.
<code>.objects[.indicator_types[.]]</code>	Indicator .Attribute	Indicator Type	<code>.objects[.valid_from]</code>	malicious-activity	Preserved as an attribute by default.
<code>.objects[.x_threatbook_verdict]</code>	Indicator .Attribute	Verdict	<code>.objects[.valid_from]</code>	malicious	Converted to Verdict: Malicious.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.objects[].modified</code>	Indicator .Attribute	Modified At	<code>.objects[].valid_from</code>	2026-06-29T22:54:42.000Z	Updatable
<code>.objects[].valid_from</code>	Indicator .Attribute	Valid From	<code>.objects[].valid_from</code>	2026-06-29T22:54:42.000Z	Updatable
<code>.objects[].valid_until</code>	Indicator .Attribute	Valid Until	<code>.objects[].valid_from</code>	2026-07-02T14:00:00.000Z	Updatable

ThreatBook Reports

The ThreatBook Reports feed queries the report list endpoint for the scheduled run window, then calls the supplemental ThreatBook - Get Report by ID feed for each returned report ID.

GET <https://api.threatbook.io/v2/reports/list>

Sample Response:

```
{
  "data": {
    "items": [
      {
        "id": "report-id",
        "title": "Example ThreatBook Report",
        "summary": "Report summary text",
        "published_time": "2026-06-30T12:00:00Z",
        "category": "Incident Analysis",
        "severity": "high",
        "source": "ThreatBook",
        "threat_type": "APT"
      }
    ],
    "cursor": "next-page-cursor"
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.title	Report.Value	N/A	.data.published_time	Example ThreatBook Report	Returned by the supplemental report detail endpoint.
.data.summary	Report.Description	N/A	N/A	Report summary text	Included in the generated HTML report description.
.data.reference_link[]	Report.Description	N/A	N/A	https://threatbook.io/example	Included in the generated HTML report description. The generic https://threatbook.cn value is dropped.
.data.category	Report.Attribute	Category	.data.published_time	Incident Analysis	N/A
.data.severity	Report.Attribute	Severity	.data.published_time	high	Can optionally be inherited by related IOCs.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.source	Report.Attribute	Source	.data.published_time	ThreatBook	N/A
.data.threat_type	Report.Attribute and Tag	Threat Type	.data.published_time	APT	Also added as a report tag and can optionally be inherited by related IOCs.
.data.targets.industries[]	Report.Attribute	Target Industry	.data.published_time	financial-services	Can optionally be inherited by related IOCs.
.data.targets.products[]	Report.Attribute	Target Product	.data.published_time	Microsoft Exchange	N/A
.data.targets.countries[]	Report.Attribute	Target Country	.data.published_time	United States	Can optionally be inherited by related IOCs.
.data.targets.organizations[]	Identity.Value	Identity Class	.data.published_time	Example Organization	Identity Class is set to organization.
.data.tags.threat_actors[]	Adversary.Name	N/A	.data.published_time	Example Actor	Related to the report.
.data.tags.virus_family[]	Malware.Value	N/A	.data.published_time	Example Malware	Related to the report.
.data.tags.attack_tools[]	Tool.Value	N/A	.data.published_time	Example Tool	Related to the report.
.data.ttps[] .technique_id / .data.ttps[].technique	AttackPattern.Value	N/A	.data.published_time	T1059 - Command and Scripting Interpreter	If the MITRE technique exists in ThreatQ, the CDF maps to the existing Attack Pattern value.
.data.iocs.ip[]	Indicator.Value	IP Address	.data.published_time	192.0.2.1	Related to the report. Selected report context can be inherited as IOC attributes.
.data.iocs.url[]	Indicator.Value	URL	.data.published_time	https://example.com/path	Related to the report. URL normalization is disabled.
.data.iocs.domain[]	Indicator.Value	Domain	.data.published_time	example.com	Related to the report.
.data.iocs.hash[]	Indicator.Value	MD5, SHA-1, SHA-256, SHA-384, or SHA-512	.data.published_time	9cf2d45d56d65399e5a0843231cfc4d3a06fda8554249876001ecc58be9a4004	Hash type is determined by hash length.
.data.malicious_files[]	Indicator.Value	Filename	.data.published_time	malware.exe	Related to the report.
.data.cves[] .cve_id	Vulnerability.Value or Indicator.Value	N/A or CVE	.data.published_time	CVE-2024-0001	The current CDF references user_fields.ingest_cves_as, but no corresponding user field is defined in the YAML. Validate CVE ingestion behavior in the target runtime.
.data.cves[] .vuln_name	Vulnerability.Attribute or	Vulnerability Name	.data.published_time	Example Vulnerability	Applied to the CVE object.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
	Indicator.Attribute				
.data.impact s[]	Report.Description	N/A	N/A	Data theft	Included in the generated HTML report description.
.data.mitiga tions[]	Report.Description	N/A	N/A	Patch affected systems	Included in the generated HTML report description.
.data.rules[]	Report.Description	N/A	N/A	YARA or Sigma rule content	Included in the generated HTML report description.

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.

ThreatBook IPs

METRIC	RESULT
Runtime	10 minutes
Indicators	5,178
Indicator Attributes	15,567

ThreatBook IOCs

METRIC	RESULT
Runtime	3 minutes
Indicators	775
Indicator Attributes	1,572

ThreatBook Hashes

METRIC	RESULT
Runtime	100 minutes

METRIC	RESULT
Indicators	45,534
Indicator Attributes	182,136

ThreatBook URLs

METRIC	RESULT
Runtime	60 minutes
Indicators	32,197
Indicator Attributes	64,394

ThreatBook Reports

METRIC	RESULT
Runtime	6 minutes
Adversaries	68
Attack Patterns	248
Identities	139
Identity Attributes	131
Indicators	142
Malware	41

METRIC	RESULT
Reports	290
Report Attributes	1,645
Tools	15

Known Issues / Limitations

General

- After a feed is enabled, the first run may take several minutes to appear as **In Progress** in the ThreatQ user interface. Activity log updates may also be delayed while the integration parses STIX data.
- The STIX parser maps only supported STIX object types and properties. Unsupported custom STIX fields may not be ingested unless the CDF specifically supports them.
- Enabling **Ingest STIX Patterns as Signatures** can increase the number of ingested objects because the integration stores both the original STIX pattern as a Signature and the extracted atomic Indicators.
- Enabling **Process & Parse Labels** can convert vendor-provided labels into dedicated ThreatQ attributes or tags. Inconsistent or high-volume labels may result in noisy attributes or tags.

ThreatBook Reports

- The Reports feed makes an additional ThreatBook API request for each report ID returned by the report list endpoint. Connector run time can increase significantly when the configured time range and filters return a large number of reports.
- Report IOCs can inherit selected report-level context. While this can support Indicator Scoring Policies, it may overstate IOC attribution when the source report contains broad or low-fidelity context.
- MITRE ATT&CK Attack Patterns must already exist in ThreatQ for the integration to map them to canonical MITRE Attack Pattern objects. If a matching technique ID is unavailable, the integration uses the vendor-provided technique ID and name.

Change Log

- **Version 1.0.0**
 - Initial release