

# ThreatQuotient

A Securonix Company



## Cyware CSAP CDF

**Version 1.1.0**

April 27, 2026

### **ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### **Support**

Email: [tq-support@securonix.com](mailto:tq-support@securonix.com)

Web: <https://ts.securonix.com>

Phone: 703.574.9893

# Contents

<b>Warning and Disclaimer</b> .....	<b>3</b>
<b>Support</b> .....	<b>4</b>
<b>Integration Details</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
<b>Prerequisites</b> .....	<b>7</b>
<b>Installation</b> .....	<b>8</b>
<b>Configuration</b> .....	<b>9</b>
<b>ThreatQ Mapping</b> .....	<b>13</b>
Cyware CSAP Alerts .....	13
Cyware CSAP Indicator Type Mapping .....	16
Cyware CSAP - Get Alert (Supplemental) .....	17
<b>Average Feed Run</b> .....	<b>21</b>
<b>Known Issues / Limitations</b> .....	<b>22</b>
<b>Change Log</b> .....	<b>23</b>

## 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](mailto: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** 1.1.0

**Compatible with ThreatQ Versions**  $\geq 5.25.0$

**Support Tier** ThreatQ Supported

---

# Introduction

The Cyware CSAP CDF integration enables the automatic and periodic ingestion of alerts from Cyware CSAP. These alerts come into ThreatQ as Report objects, along with context such as tags, related malware, related threat actors, related indicators, attribution, and more.

Cyware CSAP is a platform for sharing threat information and collaborating on security incidents. It gathers alerts from various sources, analyzes them, and helps security teams prioritize and respond to threats more quickly. This improves situational awareness and allows teams to work together effectively to defend against cyberattacks.

The integration provides the following feed:

- **Cyware CSAP Alerts** - ingests alerts from Cyware CSAP.

The integration ingests the following system objects:

- Adversaries
- Attack Patterns
- Files (Attachments)
- Indicators
  - Indicator Attributes
- Malware
- Reports
  - Report Attributes
- Tags
- Vulnerabilities

## Prerequisites

The following is required in order to install and run the integration:

- Cyware CSAP API Credentials.
- Your ThreatQ instance's egress IP address must be whitelisted in Cyware CSAP.

# 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.


6. 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
<b>Cyware CSAP Host</b>	Enter your Cyware CSAP Hostname.
<b>Access ID</b>	Enter your Cyware CSAP API Access ID to authenticate using HMAC authentication.
<b>Secret Key</b>	Enter your Cyware CSAP API Secret Key to authenticate using HMAC authentication.
<b>Category ID Filter</b>	Optional - Enter a line-separated list of Category IDs to filter alerts. Ensure that the Category ID is used rather than the Category Name. For example, a valid ID would be: 4bfd32c0.
<b>Context Selection</b>	<p>Select the contextual fields to ingest with each Report (Alert) ingested into ThreatQ. This allows you to tailor the level of detail captured based on your organization's requirements. Options include:</p> <ul style="list-style-type: none"> <li>◦ Credibility (<i>default</i>)</li> <li>◦ Confidence (<i>default</i>)</li> </ul>


PARAMETER	DESCRIPTION
<ul style="list-style-type: none"> <li>◦ Vulnerability Type <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ Urgency <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Physical Threat Method <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ Severity <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Category <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ Priority <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Alert Group <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ Risk <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Tags <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ Tactic <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Info Source <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ Malware Family <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Report Source <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ Adversaries <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Target Industry <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ MITRE Techniques <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Cyber Threat Method <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ CVEs <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Threat Method <i>(default)</i></li> </ul>	<ul style="list-style-type: none"> <li>◦ [Attributes Parsed from Tags] <i>(default)</i></li> </ul>
<ul style="list-style-type: none"> <li>◦ Detection Method <i>(default)</i></li> </ul>	

 Note that not all fields may be available for every Alert.

<p><b>Inherit Selected Context to Indicators</b></p>	<p>Select which contextual fields from the alert should be inherited by related or extracted indicators. This option enables you to apply relevant alert-level context to indicators, supporting use cases such as scoring, correlation, and filtering. Options include:</p>
	<ul style="list-style-type: none"> <li>◦ Info Source</li> <li>◦ Report Source</li> <li>◦ Target Industry <i>(default)</i></li> <li>◦ Severity <i>(default)</i></li> <li>◦ Priority</li> <li>◦ Risk <i>(default)</i></li> </ul>

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> <li>◦ Cyber Threat Method <i>(default)</i></li> <li>◦ Threat Method <i>(default)</i></li> <li>◦ Detection Method</li> <li>◦ Confidence <i>(default)</i></li> <li>◦ Urgency</li> <li>◦ Malware Family <i>(default)</i></li> <li>◦ Adversaries <i>(default)</i></li> <li>◦ MITRE Techniques</li> <li>◦ CVEs <i>(default)</i></li> <li>◦ [Attributes Parsed from Tags] <i>(default)</i></li> </ul>
<p><b>Ingest CVEs As</b></p>	<p>Select how to ingest CVEs as in the ThreatQ platform. Options include:</p> <ul style="list-style-type: none"> <li>◦ Indicators (CVE)</li> <li>◦ Vulnerabilities (default)</li> </ul>
<p><b>Fetch &amp; Ingest Attachments</b></p>	<p>Enable this parameter to retrieve and ingest attachments associated with each Cyware CSAP Alert. When disabled, attachments will be referenced within the Alert description; however, the associated links may expire after a short period. This parameter is disabled by default.</p>
<p><b>Disable Proxies</b></p>	<p>Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.</p>
<p><b>Enable SSL Certificate Verification</b></p>	<p>Enable this parameter if the feed should validate the host-provided SSL certificate.</p>

< **Cyware CSAP Alerts**



Disabled

Enabled

Uninstall

**Additional Information**

Integration Type: Feed

Version:

Configuration
Activity Log

### Connection & Authentication

Enter your Cyware CSAP Hostname to connect to.

Enter your Cyware CSAP API Access ID to authenticate using HMAC authentication.

Enter your Cyware CSAP API Secret Key to authenticate using HMAC authentication.

### API Filtering

Enter a line-separated list of Category IDs to filter alerts by. You must use the Category ID, not the Category Name. For example, an ID looks like: 4bfb32c0

### Ingestion Options

#### Context Selection

Select which pieces of context to ingest with each Report (Alert) that gets ingested into ThreatIQ. This will allow you to customize what gets shown in ThreatIQ to provide more or less context, based on your organizational needs. Not all fields will be available for every Alert.

- Credibility
- Vulnerability Type
- Physical Threat Method
- Category

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

## Cyware CSAP Alerts

The Cyware CSAP Alerts feed ingests alerts from Cyware CSAP. Cyware CSAP provides report content as well as tags with each of the alerts. ThreatQ will parse these tags, looking for relevant threat actors, malware, attack patterns, vulnerabilities, and more. Parsing this context will allow you to better manage the threat intelligence, resulting in faster times to detection and response.

GET [https://{tenant}.cyware.com/api/csap/v1/list\\_alert/](https://{tenant}.cyware.com/api/csap/v1/list_alert/)

### Sample Response:

```
{
  "count": 2,
  "data": [
    {
      "short_id": "80d38c75",
      "title": "ZeroFox Intelligence Brief - Article 23 and Risks to Foreign Nationals in Hong Kong",
      "status": "PUBLISHED",
      "published_time": 1711469354
    },
    {
      "short_id": "64cd1c71",
      "title": "Top Malware Reported in the Last 24 Hours",
      "status": "PUBLISHED",
      "published_time": 1711466108
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Report.value	N/A	.published_time	N/A	N/A
.content, .card_info, .recommendation, .attachments[], .optional_fields.description, .optional_fields.additional_info, .optional_fields.response_action,	Report.Description	N/A	N/A	N/A	Fields are concatenated to form description HTML

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.custom_fields, .optional_fields.threat_information, .optional_fields.ttps, .optional_fields.impact					
.card_tag[].tag_name	Related Malware.Value	N/A	.published_time	Jasmin Ransomware	Parsed based on tag value
.tactic_technique_pairs_data.attack_technique.title	Related Adversary.Name	N/A	.published_time	APT28	Parsed based on tag value
.card_tag[].tag_name	Related Attack Pattern.Value	N/A	.published_time	T1041 - XXXXX	Parsed based on tag value
.card_tag[].tag_name	Related Indicator.Value	CVE	.published_time	CVE-2024-12345	Parsed based on tag value; If Ingest CVEs As user field is set to Indicators
.card_tag[].tag_name	Related Vulnerability.Value	N/A	.published_time	CVE-2024-12345	Parsed based on tag value; If Ingest CVEs As user field is set to Vulnerabilities
tactic_technique_pairs_data.attack_tactic.title	Report.Attribute	Tactic	.published_time	Initial Access	Parsed based on tag value
.card_tag[].tag_name	Report.Attribute	Target Industry	.published_time	Healthcare	Parsed based on tag value
.targeted_sector[]	Report.Tag	N/A	.published_time	Cyber Threats	If no other entity is parsed from the tag
.indicators.{type}.blacklisted[]	Related Indicator.value	Mapped from .indicators.{type}	.published_time	N/A	Default Indicator Status is applied
.indicators.{type}.whitelisted[]	Related Indicator.value	Mapped from .indicators.{type}	.published_time	N/A	Whitelisted Status is applied
.info_source[].source_name	Report.Attribute	Source	.published_time	Flashpoint	N/A
.card_group[].group_name	Report.Attribute	Alert Group	.published_time	All CSAP Portal Users (MMost Users)	Only applied to Report
.cyber_threat_method[].cyber_threat_method_name	Report.Attribute	Cyber Threat Method	.published_time	Compromised User Accounts	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.physical_threat_method[].physical_threat_method_name	Report.Attribute	Physical Threat Method	.published_time	N/A	Only applied to Report
.threat_actor[].threat_actor_name	Related Adversary Name	N/A	.published_time	N/A	N/A
.reportsource[].reportsource_name	Report.Attribute	Source	.published_time	Government Organisation	N/A
.detectionmethod[].detectionmethod_name	Report.Attribute	Detection Method	.published_time	N/A	N/A
.vulnerability_type[]	Report.Attribute	Vulnerability Type	.published_time	N/A	Only applied to Report
.targeted_sector[]	Report.Attribute	Target Sector	.published_time	N/A	N/A
.content, .card_info	Report.Description	CVE	.published_time	N/A	CVEs parsed from description; If Ingest CVEs As user field is set to Indicators
.content, .card_info	Report.Description	N/A	.published_time	N/A	CVEs parsed from description; If Ingest CVEs As user field is set to Vulnerabilities
.credibility.credibility_name	Report.Attribute	Credibility	.published_time	Verified	Only applied to Report. Updated at ingestion
.card_category.category_name	Report.Attribute	Category	.published_time	Malware	Only applied to Report
.confidence.confidence_name	Report.Attribute	Confidence	.published_time	N/A	Updated at ingestion
.urgency.urgency_name	Report.Attribute	Urgency	.published_time	N/A	Updated at ingestion
.severity.severity_name	Report.Attribute	Severity	.published_time	N/A	Updated at ingestion
.priority.priority_name	Report.Attribute	Priority	.published_time	N/A	Updated at ingestion
.risk.risk_name	Report.Attribute	Risk	.published_time	N/A	N/A

## Cyware CSAP Indicator Type Mapping

ThreatQuotient provides the following Cyware CSAP Indicator Type to ThreatQ mapping:

<b>CYWARE CSAP INDICATOR</b>	<b>THREATQ INDICATOR TYPE</b>
md5	MD5
sha1	SHA-1
sha256	SHA-256
sha512	SHA-512
ipv4	IP Address
ip	IP Address
ipv6	IPv6 Address
fqdn	FQDN
host	FQDN
hostname	FQDN
domain	FQDN
url	URL

## Cyware CSAP - Get Alert (Supplemental)

The Get Alert supplemental feed fetches an attachment's content by its ID and its parent's report ID.

```
GET https://{tenant}.cyware.com/api/csap/v1/get_alert_detail/  
{alert.short_id}
```

### Sample Response:

```
{  
  "short_id": "0a586299",  
  "title": "Alpha Ransomware Emerges from NetWalker Ashes",  
  "content": "<html><body><p>Alpha, a new ransomware that first  
appeared in February 2023 has intensified its activities in recent  
weeks and strongly resembles the now defunct NetWalker ransomware  
that vanished in January 2021.</p></body></html>",  
  "status": "PUBLISHED",  
  "tlp": "CLEAR",  
  "card_group": [  
    {  
      "group_id": "70455e0f",  
      "group_name": "All CSAP Portal Users (MMost Users)",  
      "group_tlp": "RED",  
      "group_type": "CUSTOM"  
    }  
  ],  
  "card_category": {  
    "category_id": "910364bb",  
    "category_name": "Partner Advisory"  
  },  
  "card_info": "To view additional indicators provided by RiskIQ,  
click <a href=https://community.riskiq.com/article/507ee0d6>https://  
community.riskiq.com/article/507ee0d6</a> to set up an  
account.<br><br>",  
  "info_source": [  
    {  
      "source_id": "da07127f",  
      "source_name": "RiskIQ"  
    }  
  ],  
  "card_image": null,  
  "push_required": true,  
}
```

```

    "push_email_notification": true,
    "published_time": 1708459200,
    "optional_fields": {
      "threat_indicators":
"0bad18cb64b14a689965540126e0adbc952f090f1fb7b6447fe897a073860cdb
1c12ff296e7d9f90391e45f8a1d82d8140edf98d616a7da28741094d60d4779d
2d07f0425dc465b3a1267a672c1293f9a3d0cd23106b7be490807fea490978ea
46569bf23a2f00f6bac5de6101b8f771feb972d104633f84e13d9bc98b844520
480cf54686bd50157701d93cc729ecf70c14cd1acd2cb622b38fc25e23dfbc26
5f3bf9c07eedde053f19ce134caa7587f8fb6c466e33256e1253f3a9450b7110
6462b8825e02cf55dc905dd42f0b4777dfd5aa4ff777e3e8fe71d57b7d9934e7
6e204e39121109dafcb618b33191f8e977a433470a0c43af7f39724395f1343e
89bfcfbf74607ad6d532495de081a1353fc3cf4cd4a00df7b1ba06c10c2de3972
9c71500a9472814f7bf97a462fe9822cf93dc41e2e34cc068734586d5e5146ef
9d6ed8396ee79ae92a5e6cef718add321226def3461711cf585e0fd302c961ae
a8d350bbe8d9ccfb0c3e9c2dd9251c957d18ce13ae405ceb2f2d087c115db15
ab317c082c910cfe89214b31a0933eaab6c766158984f7aafb9943aef7ec6cbb
b2adf8ec7ab5193c7358f6acb30b003493466daee33ea416e3f703e744f73b7d
b7ca6d401b051712cb5b1a388a2135921a4420db8fe41842d51d2ec27380b479
c00fbf3fb992e7f237c396d69081246570cbd60d6c7a2262c01ae4d8e6f17ddd
c5f7492a3e763b4456afbb181248fdb8e652575cea286db7861e97ffcd1b72e4
df15266a9967320405b3771d0b7353dc5a4fb1cbf935010bc3c8c0e2fe17fb94
e43b1e06304f39dfcc5e59cf42f7a17f3818439f435ceba9445c56fe607d59ea
e573d2fec8731580ab620430f55081ceb7153d0344f2094e28785950fb17f499
e68dd7f20cd31309479ece3f1c8578c9f93c0a7154dcf21abce30e75b25da96b
f3858d29073ae90f90c9bb284913752533fe1a6437edd6536e4b1775fc8f6db4
f5d25777331ba55d80e064dea72240c1524ffcd3870555a8c34ff5377def3729"
    },
    "indicators": {
      "sha256": {
        "whitelisted": [],
        "blacklisted": [
"1c12ff296e7d9f90391e45f8a1d82d8140edf98d616a7da28741094d60d4779d" ,
"6462b8825e02cf55dc905dd42f0b4777dfd5aa4ff777e3e8fe71d57b7d9934e7"
        ]
      }
    },
    "credibility": null,
    "confidence": null,
    "announcement_type": null,

```

```

"risk": null,
"urgency": null,
"severity": null,
"priority": null,
"kill_chain_phase": null,
"exploit_likelihood": null,
"exploited_wild": null,
"systemsaffected": null,
"threat_actor": [],
"threat_method": [],
"detectionmethod": [],
"root_cause": [],
"card_intel_source": [
  {
    "source_id": "da07127f",
    "info_source_id": "da07127f",
    "card_count": 462,
    "info_source_name": "RiskIQ",
    "alert_count": 462,
    "created": "2022-08-02T18:55:42.009932Z",
    "modified": "2022-08-02T18:55:42.010177Z",
    "source_name": "RiskIQ",
    "is_editable": false,
    "is_active": true,
    "index": 0
  }
],
"cyber_threat_method": [],
"physical_threat_method": [],
"document_type": [],
"vendorsnproduct": [],
"reportsource": [],
"vulnerability_type": [],
"vulnerability_source": [],
"targeted_sector": [],
"card_tag": [
  {
    "tag_name": "Alpha",
    "tag_id": "9475209d-1313-49a0-9a19-9f5cca3dc2ac",
    "is_active": true,
    "tag_slug": "alpha"
  }
],

```

```

    {
      "tag_name": "T1056 - Input Capture",
      "tag_id": "5bb0b5e8-57b6-4bd9-b44a-7cd75715eb7e",
      "is_active": true,
      "tag_slug": "t1056-input-capture"
    },
    {
      "tag_name": "OSINT",
      "tag_id": "41b726a3-3298-4c46-a089-b796dadcbad2",
      "is_active": true,
      "tag_slug": "osint"
    },
    {
      "tag_name": "Ransomware",
      "tag_id": "caeeb35d-a009-498a-93f8-a36fcb390054",
      "is_active": true,
      "tag_slug": "ransomware"
    }
  ],
  "previous_base_card": null,
  "child_cards": null,
  "tactic_technique_pairs_data": [],
  "custom_fields": {},
  "tracking_id": "42729d71-ddb9-49b4-8931-72df2751bdac",
  "attachments": [],
  "event": null,
  "intel_id": null,
  "rfi_id": null
}

```

# 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	7 minutes
Adversaries	12
Indicators	172
Indicator Attributes	390
Malware	16
Reports	65
Report Attributes	205
Vulnerabilities	13

## Known Issues / Limitations

- Cyware CSAP has a rate limit on how many API calls you can make within an hour. If you are requesting historical data, you may hit this limit, which will cause a feed run error.

---

# Change Log

- **Version 1.1.0**

- Added support for filtering alerts by Category ID.
- Enhanced description content to include additional context such as Threat Information, TTPs, Impact, and Custom Fields.
- Added support for parsing additional MITRE ATT&CK techniques.
- Introduced configurable context selection for both alerts and related indicators.
- Added support for fetching and ingesting alert attachments.
- Enhanced parsing to extract additional indicators from tables within alert custom fields.
- Included direct links to the Cyware user portal in alert (Report) descriptions.
- Added support for incorporating external reference links into alert (Report) descriptions.
- Introduced the ability to enable or disable SSL verification.
- Added support for enabling or disabling proxy configurations.
- Implemented cleanup of placeholder attachments prior to each run to prevent accumulation.
- Ensured original media titles and filenames are preserved for accurate matching.
- Documented that placeholder attachments cannot be fulfilled across separate runs.
- Added the following new configuration parameters:
  - **Category ID Filter** - enter a line-separated list of Category IDs to filter alerts.
  - **Context Selection** - select the contextual fields to ingest with each Report (Alert) ingested into ThreatQ
  - **Inherit Selected Context to Indicators** - select which contextual fields from the alert should be inherited by related or extracted indicators.
  - **Fetch & Ingest Attachments** - enable this parameter to retrieve and ingest attachments associated with each Cyware CSAP Alert. When disabled, attachments will be referenced within the Alert description.
  - **Disable Proxies** - determine if the feed should honor proxy settings set in the ThreatQ UI.
  - **Enable SSL Certification Verification** - determine if the feed should validate the host-provided SSL certificate.

- Removed the **Inherit Relationships & Contexts to Indicators** configuration parameter. The new **Context Selection** and **Inherit Selected Context to Indicators** parameters have replaced this parameter.
- **Version 1.0.0**
  - Initial release