ThreatQuotient

A Securonix Company

ACSC Alerts & Advisories CDF

Version 1.0.0

September 14, 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	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) publishes alerts and advisories covering current cybersecurity threats, critical software vulnerabilities, and malicious campaigns. These publications provide actionable guidance for government organizations, critical infrastructure operators, small and medium-sized businesses, and the broader Australian community.

The ACSC Alerts & Advisories CDF integration retrieves public content from the ACSC Alerts and Advisories portal and ingests each matching publication into ThreatQ as a Report. Each Report includes the publication date, intended audiences, article title, and article content, allowing analysts to review and operationalize ACSC guidance directly within ThreatQ.

The integration provides the following feed:

- **ACSC Alerts & Advisories** - retrieves published ACSC alerts and advisories.

The integration ingests reports and report attributes into ThreatQ.

Prerequisites

The integration requires the following:

- Network access from ThreatQ to `https://www.cyber.gov.au`.

No API key or user account is required by the feed definition. The integration accesses public ACSC alert and advisory content.

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 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 **OSINT** 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
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.

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

ACSC Alerts & Advisories

The ACSC Alerts & Advisories feed retrieves ACSC alerts and advisories published within the configured since and until date range. Each matching publication is ingested into ThreatQ as a Report, with the complete article content formatted for review in the Report description.

```
POST https://www.cyber.gov.au/views/ajax
```

Sample Response:

```
[
  {
    "command": "insert",
    "method": "replaceWith",
    "data": "<div class=\"views-row\"><a href=\"/about-us/view-all-content/alerts-
and-advisories/reported-widespread-credential-exposure-affecting-fortinet-firewalls-
and-vpn-gateways\"><header><div>22 Jun 2026</div><div><strong>Critical</strong></
div></header><h3>Reported widespread credential exposure affecting Fortinet Firewalls
and VPN Gateways</h3><div class=\"focus-audience\"><span>Government</span></div><div
class=\"focus-audience\"><span>Organisations & Critical Infrastructure</span></
div><p>Fortinet have released a blog post and additional guidance regarding this
activity.</p></a></div>"
  }
]
```

For each parsed listing entry, the feed makes a supplemental request to fetch the full article content:

```
GET https://www.cyber.gov.au{{ uri }}
```

This supplemental request returns HTML data that is parsed by the integration.

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<Parsed from HTML>	Report.Title	Report	data.published_at	Reported widespread credential exposure affecting Fortinet Firewalls and VPN Gateways	The title is sanitized and limited to 255 characters.
<Parsed from HTML>	Report.Description	N/A	data.published_at	N/A	N/A
<Parsed from HTML>	Report.Attribute	Published At	data.published_at	June 22, 2026	
<Parsed from HTML>	Report.Attribute	Audience	data.published_at	Government	Multiple Audience attributes may be created for one Report.
<Parsed from HTML>	Report.Attribute	Severity	data.published_at	High	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.

METRIC	RESULT
Run Time	2 minutes
Reports	10
Report Attributes	42

Known Issues / Limitations

- The feed retrieves only the 24 most recent posts from the ACSC Alerts and Advisories portal, typically covering approximately six months of content. Of those posts, only content published within the configured start and end dates is ingested. Posts outside the 24 most recent results cannot be ingested, even when they fall within the configured date range.
- If you need to ingest historical context (within the latest 24 posts), run the feed manually by setting the **since** date back.

Change Log

- **Version 1.0.0**
  - Initial release