

ThreatQuotient



Google Chrome Updates Blog CDF

Version 1.0.0

July 08, 2025

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping..... 10

 Google Chrome Updates Blog..... 10

Average Feed Run..... 12

 Google Chrome Updates Blog..... 12

Known Issues / Limitations 13

Change Log 14

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 © 2025 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: support@threatq.com

Support Web: <https://support.threatq.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	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Google Chrome Updates Blog CDF enables analysts to automatically ingest Google Chrome update posts from the Google Blog. This allows analysts to stay up-to-date on security fixes for Google Chrome.

Blog: <https://chromereleases.googleblog.com/search/label/Stable%20updates>

Considering the pace of new articles, we recommend running this CDF every day.

The integration provides the following feed:

- **Google Chrome Updates Blog** - pulls blogs posts from the Google Chrome Update Blog as report objects.

The integration ingests the following system object types:

- Indicators
 - Indicator Attributes
- Reports
 - Report Attributes
- Vulnerabilities

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.

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.
Blogs	Select the blogs from which you want to pull posts: <ul style="list-style-type: none"> • Stable Updates (default) • Beta Updates • Dev Updates
Platform Filter	Select which platforms you want to track: <ul style="list-style-type: none"> • Desktop (default) • Android iOS • Chrome OS
Parsed IOC Types	Select the IOC types you want to automatically parse from the content: <ul style="list-style-type: none"> • CVE (default)
Ingest CVEs As	Select the entity type to ingest CVE IDs as: <ul style="list-style-type: none"> • Vulnerabilities (default)

PARAMETER

DESCRIPTION

- Indicators



This field is displayed if you select CVE in the Parsed IOC Types field.

< Google Chrome Updates Blog



Disabled ☒ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version: 1.0.0

Configuration

Activity Log

Connection

☒ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Ingestion Options

Blogs

Select which blogs you want to pull posts from.

☒ Stable Updates

☐ Beta Updates

☐ Dev Updates

Platform Filter

Select which platforms you want to keep track of.

☒ Desktop

☐ Android

☐ iOS

☐ Chrome OS

Parsed IOC Types

Select the IOC types you would like to automatically parse from the content.

☒ CVE

Ingest CVEs As

Vulnerabilities

Select the entity type to ingest CVE IDs as.

Set indicator status to...

Review

Run Frequency

Every 24 Hours

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Google Chrome Updates Blog

This feed periodically pulls blog posts from the Google Chrome Update Blog as Report Objects. The following endpoints are queried based on Blogs user configuration:

GET <https://chromereleases.googleblog.com/search/label/Stable%20updates>

GET <https://chromereleases.googleblog.com/search/label/Beta%20updates>

GET <https://chromereleases.googleblog.com/search/label/Dev%20updates>

Google provides their blog posts in HTML format. This integration parses the HTML and ingests the parsed posts as Reports.

Sample Response:

Stable Channel Update for Desktop

Monday, June 30, 2025

The Stable channel has been updated to 138.0.7204.96/.97 for Windows, 138.0.7204.92/.93 for Mac and 138.0.7204.92 for Linux which will roll out over the coming days/weeks.

Security Fixes and Rewards

This update includes 1 security fix.

Below, we highlight fixes that were contributed by external researchers.

Please see the Chrome Security Page for more information.

[NA][427663123] High CVE-2025-6554: Type Confusion in V8.

Reported by Clément Lecigne of Google's Threat Analysis Group on 2025-06-25.

This issue was mitigated on 2025-06-26 by a configuration change pushed out to Stable channel across all platforms.

Google is aware that an exploit for CVE-2025-6554 exists in the wild.

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
{HTML}	Report.Value	Report	{HTML}	Stable Channel Update for Desktop - Monday, June 30, 2025	Parsed from HTML.
{HTML}	Report.Description	N/A	{HTML}	The Stable channel has been updated to 138.0.7204.96/.97...	Parsed from HTML.
{HTML}	Report.Attribute	External Reference	{HTML}	N/A	Parsed from HTML.
{HTML}	Report.Attribute	Affected Platform	{HTML}	Desktop	Parsed from title.
{HTML}	Report.Attribute	Channel Type	{HTML}	Stable	Parsed from title.
{HTML}	Indicator/Vulnerability.Value	CVE/Vulnerability	{HTML}	CVE-2025-6554	Parsed from HTML. Ingested according to Ingest CVEs As.
N/A	Report/Indicator/Vulnerability.Attribute	Affected Product	{HTML}	Chrome	Static Attribute.
N/A	Report/Indicator/Vulnerability.Attribute	Affected Vendor	{HTML}	Chrome	Static Attribute.

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.

Google Chrome Updates Blog

METRIC	RESULT
Run Time	1 minute
Reports	3
Report Attributes	12
Indicators	14
Indicator Attributes	3

Known Issues / Limitations

- This feed uses "since" and "until" dates to make sure entries are not re-ingested if they have not been updated.
- This feed cannot be run historically as the only posts it has access to are the ones from the first page of results.

Change Log

- Version 1.0.0
 - Initial release