chrome enterprise

Integrate Google Security Operations with Chrome Enterprise in Chrome Enterprise Core

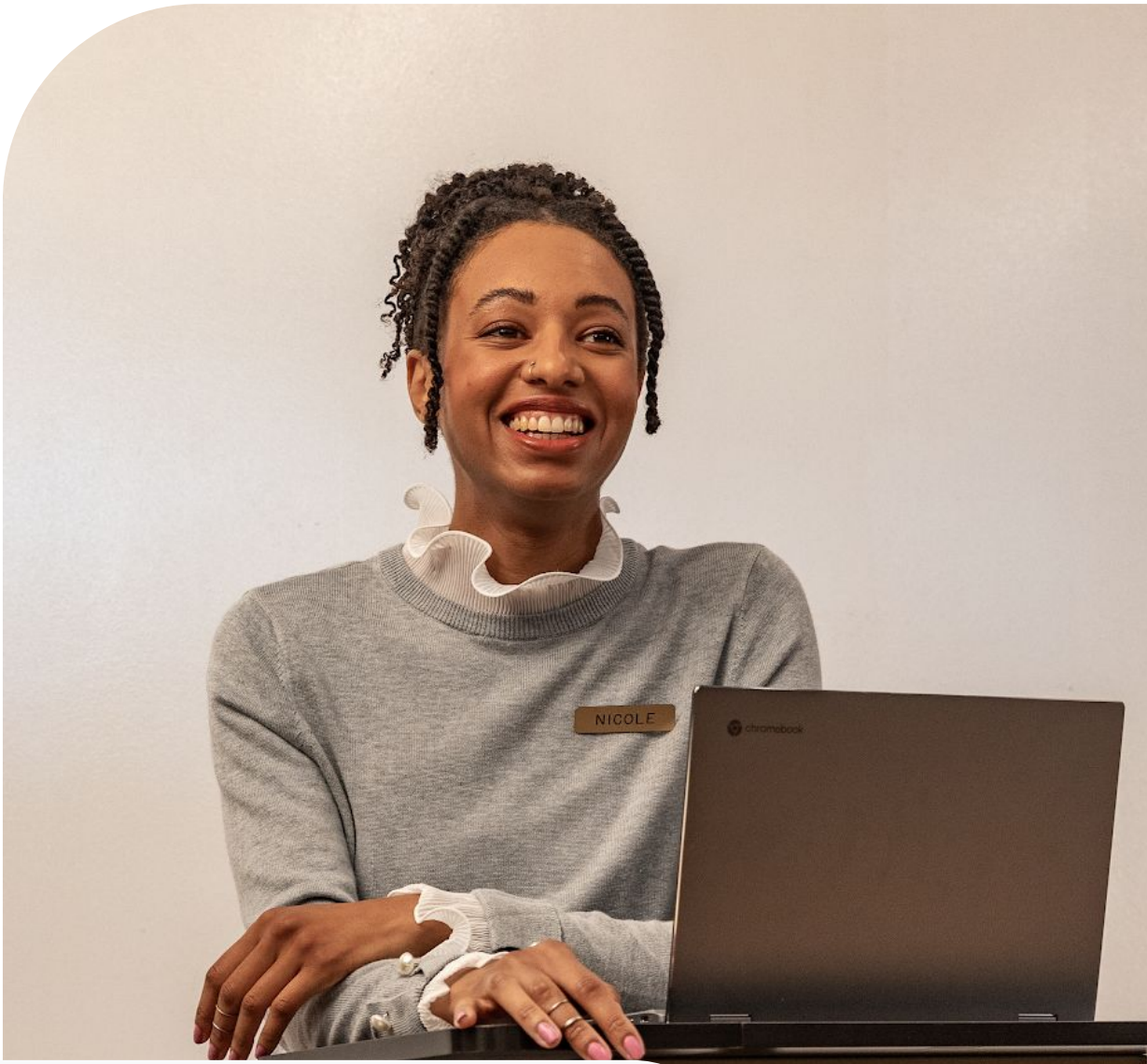
Table of Contents

Resources

This document will guide you through the process of setting up the reporting integration between Chrome Enterprise Core and Google Security Operations. Note that this feature requires devices to be enrolled into Chrome Enterprise Core to send security events to Google Security Operations.

Here are some useful links:

- Setting up Chrome Enterprise Core
- Best practices for using Chrome Enterprise Core
- Help Center Article for Reporting Connectors



Generate the API key for Google Security Operations in the Google Cloud Platform console

Please contact Google Security Operations Support or your Google Security Operations customer point of contact to request your Google Security Operations ingestion API key.

Troubleshooting issues in Chrome Browser Cloud Management

The following data is sent from Chrome browser to Google Security Operations once the integration is set up. The data is also logged in the Google Admin console under Reporting>Audit and investigation>Chrome log events. For more information, please review this Help Center article.

Here is a brief overview of just a few of the events captured:

Event value	Description
Malware transfer	The content uploaded or downloaded by the user is considered to be malicious, dangerous, or unwanted
Password changed	The user resets their password for the first-signed-in user account
Password reuse	The user has entered a password into a URL that's outside of the list of allowed enterprise login URLs
Unsafe site visit	The URL visited by the user is considered to be deceptive or malicious

For a complete list of all of the events that can be sent, please review this help center article.

Set up the Google Security Operations configuration in the Google Admin console

1. Log into the Google Admin console at admin.google.com.
2. Navigate to Chrome browser>Settings. Add a filter for “event reporting”.
3. Under Events reporting, select Enable Event Reporting. Under the additional settings, you can also specify which events you want to send to Google Security Operations.
4. Now that the events are turned on, click on the blue hyperlink that says “reporting Connector provider configurations” to take you to the connector provider configurations, or it can be found under Chrome browser>Connectors.
5. Click the New Provider Configuration button and select Google Security Operations as the provider.
6. Enter the configuration name that you want this connector to display as in the Google Admin console.
7. Enter the API key value you received from Google Security Operations support or your customer engineer.
8. Enter your regional endpoint for the host name. You can find the regional endpoints at cloud.google.com/chronicle or via this link.
9. You can pick and choose what events you want Google Security Operations to receive here.
10. Press the Add Configuration to save.
11. Select the Organizational Unit that the reporting events are turned on in and select the Chrome Google Security Operations connector that was created in the previous step, and hit Save.

View Chrome events in Google Security Operations

Alerts from managed browsers will start being sent to Google Security Operations once the policy is applied in Chrome Browser Cloud Management. Ingested events include fields like accessed domain, downloaded file hash, and username. Each of these can be found within Google Security Operations using the following methods:

- **Search & Investigative Views:** Username, hash, domain, and IP values can be directly entered into Google Security Operation's search bar, and results will be materialized in Google Security Operation's respective investigative views
- **Google Security Operations Detect:** Customers can create or enhance existing threat detection rules using Chrome alert data
- **Raw Log Scan:** Customers can use Google Security Operation's Raw Log Scan capability to search over raw data

For more information about what events are sent to Google Security Operations, please review this Help Center article and Google Security Operations documentation

- Note that password events will only be sent if the feature is turned on. For more information about Password Alert, please review this blog.
- Chrome Data Protection events are available only for customers who have purchased Chrome Enterprise Premium. For more information about Chrome Enterprise Premium and how to set it up, go to Protect Chrome users with Chrome Enterprise Premium Threat and Data Protection.