Google Cloud
Security

Google Security Operations Build Partner Content Guide

H1 2026

Rev. 1.0

Google Cloud
Security

Google Cloud
Security

WELCOME

In this guide, you'll learn how to build integrations between Google Security Operations (**Google SecOps**) and your chosen product platform to unlock better-together value for our joint customers.

For your awareness, Google Security Operations was formerly known as Chronicle, including SIEM and SOAR functionality. With that you may note "Chronicle" (SIEM) and "Siemplify" (SOAR) are referenced often in our API documentation.

RESOURCES

This guide is intended to be your primary resource when developing integrations and content with Google SecOps. However, we recommend the following assets:

- **Community**: Become familiar with and contribute to our Google Cloud Security Community blogs and forums to learn more about our offerings and gain advice from the broader Google SecOps user community.
- **Free Training:** Take a tour of Google SecOps Fundamentals for a nice overview and a SecOps Deep Dive into topics such as Google SecOps's architecture, developing detection rules, ingesting data and building SOAR integrations. *Disclaimer: our innovation is rapid and not all recent features are covered in this training at all times.*
- **Technical Documentation:** All Google SecOps technical documentation can be accessed here.
- **Partner Advantage:** We strongly encourage all partners to join Partner Advantage to take advantage of the broader programs and incentives made available for all Google Cloud partners. For partners that participate in the program, you have access to Partner Support Desk, among other unique resources, for all of your Partner Advantage needs.

Google Cloud
Security

REQUEST A GOOGLE SECOPS DEVELOPMENT LICENSE

Build partners of our Partner Advantage program are offered access to a Google Security Operations development license. Before proceeding, please make sure your company has completed sign-up for Partner Advantage. You can verify your company's participation in the program through our Partner Network Hub search, however, please note that recent status updates may not be immediately reflected in the directory.

Follow the below steps to request your Google Security Operations development license:

1. **Identify your Google SecOps SME and ensure your SME has the correct permissions.** The SME will need to have the following IAM roles: Chronicle API Admin, Chronicle Service Admin, Chronicle SOAR Admin.
2. **Have your SME create a Google Cloud project** to bind with your Google SecOps development license instance. Please refer to the below resources for guidance on creating a new Google Cloud Project.
    a. Creating and managing projects
    b. Quickstart using organization resources
3. **Enable the Chronicle API** in your newly created Google Cloud project by following the instructions outlined here. *Note: This step must be done before the Google SecOps development license is provisioned.*
4. **Complete the inbound request form** to formally request the development license. The form will request three key details:
    a. **The newly created Google Cloud project number** where you have enabled the Chronicle API.
    b. **The Org name or ID** used to create your Google Cloud project.
    c. **The name and email of a stakeholder** in your organization who will be responsible for the test instance setup. Note: This stakeholder must have the correct permissions *at the project level* in order to successfully set-up the Google Security Operations test instance.
5. **Receive your "Your Google Security Operations instance is ready" email** from Google SecOps to the contacts provided in the previous form. Follow the instructions provided to activate your Google SecOps development license making sure to select 'US Region' during the process.

For continued support in creating your project and enabling your Google SecOps development license, please reference the below technical documentation.

- Onboarding or migrating a Google SecOps instance
- Configure a Google Cloud identity provider
- Configure a third-party IdP

- Reference and contribute to our Google Cloud Security Community forums

GITHUB: CONTENT HUB CONTRIBUTION CHANNEL

To distribute third-party developed content to customers via the Google Security Operations' Content Hub, contributors must submit a pull request through our supported GitHub repository.

The Content Hub GitHub repository supports only Response Integrations and Playbooks today. Support will be expanded to include additional content types, such as rules and parsers, in the future.

Each submission undergoes a validation process that includes a series of automated validation checks followed by a final approval from the Google Security Operations team. Upon approval of your pull request, the content will be published and made available to all Google SecOps customers **within 24 hours.**

Documentation detailing the development standards and contribution guidelines is provided on the GitHub repository site.

Google Cloud
Security

LOG INGESTION INTO GOOGLE SECOPS

There are two ways you as a partner can enable log ingestion of your solution into Google Security Operations:

1. Send UDM Normalized Logs
2. Send Unstructured Logs

Send Normalized Logs to Google SecOps

Having your products' data ingested into Google SecOps is the foundation of our security intelligence, detection, investigation and context-aware response capabilities. We strongly encourage partners to send logs in our Unified Data Model (UDM) format using the Google SecOps Ingestion API. Having logs in UDM format is required to enable security workflows such as correlation, enrichment, threat detection, and contextual investigations in the Google SecOps platform. Below are the primary options for sending normalized data to Google SecOps:

Chronicle Ingestion API Integration
The Google Security Operations Ingestion API enables you to forward events parsed to UDM directly to your Google Security Operations instance, eliminating the need for additional hardware or software (for example, forwarders) in your environment. You can use the current Ingestion API or the ingestion methods in the Chronicle API. To future-proof new integrations, we recommend using the Chronicle API ingestion methods, currently in preview (beta) status.

Webhook Integration
Send your products' data pre-parsed logs to Google SecOps via an HTTPS webhook feed. To use Webhook, you must have access to a Google SecOps development license in a Google Cloud Project.

Troubleshooting: Mapping your telemetry to the Unified Data Model (UDM)

When considering how to parse your telemetry, refer to our technical documentation. There is a select set of key fields we encourage you to map referenced here. It is important to note UDM has two primary data model concepts - entities and events.

1) UDM Event: Stores data for an action that occurred in the environment.
2) UDM Entity: Contextual representation of elements such as assets, users, and resources.

We recommend reviewing this additional support documentation below:

- Overview of Unified Data Model
- UDM Field List
- Format Log data as UDM
- Sending UDM Events via Ingestion API
- UDM Usage GuideParser Syntax Reference
- Overview of Log Parsing

Sending Unstructured Data (Raw Logs) into Google SecOps

Partners may alternatively send logs in their original format to Google SecOps via the Ingestion API or Webhooks.

Unlike normalized data, Raw Log ingestion requires Google SecOps support of your “Log-Type” to recognize and label the feed. Once you have finalized your Raw Log integration, please complete this form to request Google SecOps’s support for your log type.

Troubleshooting: Create a Custom Parser for Raw Logs into Google SecOps

Understanding “Default Parsers”

The Google SecOps team has built and published "**Default Parsers**" for many applications based on customer use. Default Parsers automatically normalize defined data sources into our Unified Data Model (UDM). Default Parsers are accessible to all customers from the Google SecOps console.

As a partner, you may request to have Google revise an existing Default Parser for your product by completing this form. Today we consider support for new Default Parsers based on customer usage and do not support inbound requests for new Default Parsers.

Creating a Partner-Managed Parser

We strongly encourage partners to contribute and maintain the “**Default Parser**” rather than developing a separate parser. In this model, you can contribute updates to the “Default Parser” as your product changes. Google will distribute the parser as content updates to SecOps customers, ensuring that they receive regular updates and do not have to install a custom parser.

Creating a “Custom Parser”

If your product is not included in the Default Parser list, partners can also develop a **“Custom Parser”** as outlined in documentation here. We recommend hosting your customer parser in your organization’s GitHub repository for Google SecOps to redirect to through our technical documentation. In this model, customers will be responsible for installing updates to the custom parser, as they will not be distributed through Google SecOps.

Google Cloud
Security

GOOGLE SECOPS DASHBOARDS

Google SecOps provides dashboards based on the Yara-L search language for creating visualizations of data from your product. Dashboards also provide a way to join the data from your product with other data sources such as Cases, Detections, Entities, and IOCs.

For more details about the dashboards in SecOps and the permissions required to create dashboards, refer to the dashboards overview.

Creating a Dashboard

Follow the instructions to create a dashboard in your Google SecOps development instance using Yara-L searches and the available chart types.

Exporting a Dashboard

Once you have created a dashboard, you can export the dashboard configuration to include in your GitHub repository. SecOps users can use the import dashboard feature to use the dashboard with the data in their SecOps instance.

PULL GOOGLE SECOPS DATA INTO YOUR APPLICATION

For a subset of partners, you may also want to consider pulling data such as insights, events, and detections into your own application.

Chronicle API

The Chronicle APIs enable customers to programmatically access their security data directly through API calls to the Google Security Operations platform. This is the same security data presented in the Google Security Operations UI through a customer account.

The capability to access security data through API calls lets you develop new applications or modify existing applications to retrieve and process all of a customer's security data stored in Google Security Operations. Explore the below reference documentation based on data types:

- Receiving insights & events
- Receiving detections

SecOps MCP Server

- For AI integration with Google SecOps, we provide the Google SecOps MCP Server. This is a managed MCP server that you can use with your AI applications to interface with the Google SecOps instance.

Additional Recommended Resources for Support

- Examples of other partner Integrations with Google SecOps
- Google SecOps CLI User Guide for feed and parser management
- Google Cloud Security Community blogs and forums

RESPONSE INTEGRATIONS

Within Google Security Operations, a partner can contribute a **Response Integration**.

A **Response integration** - is a collection of scripts bound to a specific product that are leveraged by the SOC analysts during the triaging of cases.

Response Integrations consist of:

- Actions
- Connectors
- Jobs
- Ontology Mapping

Action - a script that is used to perform a task. For example, enrich information about IOCs in a Case.

Connector - a script that is executed periodically (like a cron job) to ingest alerts/incidents/events from integrations. A connector is responsible for the creation of Alerts and Cases in Google SecOps.

Jobs - a script that is executed periodically, but unlike connector, the main goal for a job is to synchronize data from an external product with Google SecOps. For example, if there is a ticket in ServiceNow that is tied to a Case in SecOps, then any comment that was added to the ServiceNow ticket, this information should be synced to Google SecOps Case.

Ontology Mapping - a mapping file for how IOCs and Assets should be extracted from an Alert and mapped to a Case..

Relevant Documentation:

- My First Integration
- Using the Integrated Development Environment (IDE)
- Create Custom Action
- My first action
- My first connector
- Map and Model Alerts
- CI/CD with GitSync

LAUNCH YOUR GOOGLE SECOPS CONTENT

Publishing your content on Google Cloud properties

Once you have completed your partner content, Google Cloud will host a redirect listing to your content via our Partner-Developed Content technical documentations page.

To request support in listing your content, please complete this form.

Note: *To include your content in Google-hosted technical documentation, you must provide a URL hosted on your company website that directs users to details regarding your Google SecOps content. The URL must be publicly accessible. We are not able to accept general company marketing web pages.*

Announcing your content in partnership with Google Cloud

We strongly encourage all partners to promote the launch of their Google SecOps content. We provide "Build" partners of our Partner Advantage program the opportunity to launch a press release, develop a blog post, and create a landing page for Google SecOps content on their own properties with our support.

For those interested in creating Google Cloud supported content (e.g. press release, blog post, landing page, etc.), please submit your content for review by Google Cloud here. Please be aware of our **10-day SLA** for feedback and approval for publication. See our Guidelines and Templates doc for more info and FAQs.

In addition, Google Cloud SecOps each cycle features new technical milestones in our official Google Cloud Security Community. We publish a recurring "Integration Spotlight" blog post that aggregates the latest validated integrations, providing a centralized platform for customers to discover your solutions. By participating in the partner amplification process, your integration becomes eligible for inclusion in these posts, where we highlight the technical synergy between our platforms and direct the community to your specific partner-hosted content. This collaborative approach ensures that your integration is not only promoted through your own channels but is also woven into the broader Google SecOps ecosystem narrative.

Below outlines various resources to guide you in your content development:

- Google Security Operations Landing Page for messaging guidance
- Partner Co-Branding Guidelines for Google Cloud Security *[Note: This document is only made accessible to Partner Advantage partners]*

Note: *The above benefits are only provided to Build partners of our Partner Advantage program. Before proceeding, please make sure your company has completed sign-up for Partner Advantage. You can verify your company's participation in the program through our Partner Network Hub search.*

QUESTIONS AND ADDITIONAL SUPPORT RESOURCING

Google Cloud Security Community

We strongly encourage all partners to refer to and contribute to our Google Cloud Security Community forums for any questions that may arise. Our product and engineering teams actively monitor and contribute to our forums.

Additional support

If additional support is of interest, below is a select group of services partners who are able to provide hands-on support in developing and, in some cases, maintaining your integrations and content with Google Security Operations:

- Analytica42; contact sales@analytica42.com
- Citreno; contact info@citreno.com
- Crest Data; contact sales@crestdata.ai
- Metron Security; contact connect@metronlabs.com