Security Command Center Evaluation Guide

Security Command Center Overview

Security Command Center is a native security and risk management platform for Google Cloud. Security Command Center continuously monitors your Google Cloud environment and enables you to gain visibility into your cloud assets, discover vulnerabilities in your resources, detect threats targeting your assets, and help maintain compliance based on industry standards and benchmarks.

Purpose

This guide walks through the key steps on how to setup and evaluate the core capabilities of Security Command Center Premium in your Google Cloud environment. For a complete set of product how-to-guides and API reference, please visit Security Command Center documentation.

Google Cloud

For more information, visit cloud.google.com/security-command-center
Step 0: Setup the Security Command Center
Premium

- To setup Security Command Center, you need the following Identity and Access Management (IAM) roles:
  - Organization Admin: roles/resourcemanager.organizationAdmin
  - Security Center Admin: roles/securitycenter.admin
  - Security Admin: roles/iam.securityAdmin
  - Create Service Accounts: roles/iam.serviceAccountCreator

- Select the Security Command Center Premium tier.
- Go to SETTINGS and make sure you keep the built-in services you want in Premium enabled.
- When you finish setup, Security Command Center starts an initial asset scan, after which you can use the dashboard to review, explore security findings, and take necessary action. You have the option to exclude resources by navigating to the Advanced settings menu and changing resource settings.

Watch this video for an overview of the Security Command Center

---

Google Cloud
For more information, visit cloud.google.com/security-command-center
Step 1: Gain visibility through asset view

Discover and view your assets in near-real time across your Google Cloud resources and policies.

- Navigate to **ASSETS**. Assets are your Google Cloud resources, like Compute Engine instances or Cloud Storage buckets, and policies.
- Discover your asset inventory across your organization. Review historical discovery scans to identify new, modified, or deleted assets.
- To receive real-time notifications about resource and policy changes, create and subscribe to a **feed**.
- You can test asset discovery by creating a VM instance or a GCS bucket and check if these resources show up in the Assets dashboard of Security Command Center.
Step 2: Discover vulnerabilities

Identify security misconfigurations and web application vulnerabilities in your Google Cloud assets and take action.

a. **Security Health Analytics** built-in service discovers misconfigurations & vulnerabilities
   - Navigate to **VULNERABILITIES** tab to display a list of findings for the project that you selected.
   - To view these findings, use the **FINDINGS** tab. Click on **View by: Source Type**, and then select **Security Health Analytics**.
   - Take action and remediate these vulnerability findings by following this [guide](#).

Watch this [video on getting started with Security Health Analytics](#)

b. **Web Security Scanner** built-in service discovers common web application vulnerabilities
   - Navigate to **VULNERABILITIES** tab to display a list of findings for the project that you selected.
   - To view these findings, use the **FINDINGS** tab. Click on **View by: Source Type**, and then select **Web Security Scanner**
   - Web Security Scanner’s **managed scan** feature automatically configures and schedules scans for each of your in-scope projects.
   - Take action and remediate these vulnerability findings by following this [guide](#)
   - You can test Web Security Scanner by following this [guide](#)

Watch this [video on getting started with Web Security Scanner](#)
Step 3: Detect Threats

Uncover threats targeting your Google Cloud assets and take action to remediate.

a. Event Threat Detection built-in service uncovers threats using logs & threat intelligence
   - Enable logs required to find threats in your organization: VPC flow logs, Cloud DNS logs, and Firewall Rules logs.
   - Navigate to THREATS tab to find potential security issues associated with your organization's Google Cloud resources.
   - To view these findings, use the FINDINGS tab. Click on View by: Source Type, and then select Event Threat Detection.
   - Review the findings and affected resources to remediate and take action.
   - You can test Event Threat Detection by following this guide.

Watch this video on getting started with Event Threat Detection

b. Container Threat Detection built-in service uses kernel-level instrumentation to identify Container runtime threats
   - Navigate to THREATS tab to find potential security issues associated with your organization's Google Cloud resources.
   - To view these findings, use the FINDINGS tab. Click on View by: Source Type, and then select Container Threat Detection.
   - You can test Container Threat Detection by following this guide.

Watch this video on getting started with Container Threat Detection

For more information, visit cloud.google.com/security-command-center
Step 4: Maintain and get compliance reports

Review and export compliance reports to help ensure all your resources are meeting their compliance requirements.

- Navigate to **COMPLIANCE** tab to review your organization’s compliance posture with regards to industry standards and benchmarks like CIS, PCI DSS, NIST 800-53 and ISO/IEC 27001.
- Review the dashboard to check your organization’s compliance score against the industry benchmarks and any violations.
- View all violations by severity and take action by following the recommendations to fix the violations.
- Get reports by clicking on **EXPORT** to export reports in a CSV format.

---

Google Cloud

For more information, visit [cloud.google.com/security-command-center](http://cloud.google.com/security-command-center)
Step 5: Integrate with your SecOps ecosystem

a. Consolidate findings into the Security Command Center
   - Go to SETTINGS and navigate to Integrated Services tab and select or add supported integrations.
   - Enable the integrated services for findings to be appear in Security Command Center’s findings view

<table>
<thead>
<tr>
<th>SERVICES</th>
<th>INTEGRATED SERVICES</th>
<th>SINKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prisma Cloud SCC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source ID</td>
<td>organizations/688851#28130/thirdPartyFindingProviders/redlock-gcp/redlock-scc</td>
<td>Enabled</td>
</tr>
<tr>
<td>Service account</td>
<td><a href="mailto:prisma-gcpplame@andychang.scc-totes-demo.iam.gserviceaccount.com">prisma-gcpplame@andychang.scc-totes-demo.iam.gserviceaccount.com</a></td>
<td></td>
</tr>
</tbody>
</table>

| StackRox Cloud SCC Connector | | |
| Source ID | organizations/688851#28130/thirdPartyFindingProviders/stackroxlauncher-project/1/stackroxccloud-scc | Enabled |
| Service account | scc-notifications@ac-new-scc-notifications-demo.iam.gserviceaccount.com | |

b. Export your security findings to remediation and ticketing systems
   - Enable the Security Command Center API notifications feature.
   - Send findings to existing 3rd party solutions like a Security Orchestration Automation & Response (SOAR), Security Information & Event Management (SIEM) platforms or ticketing systems
   - Use Cloud Functions library to take automated actions.

Google Cloud
For more information, visit cloud.google.com/security-command-center