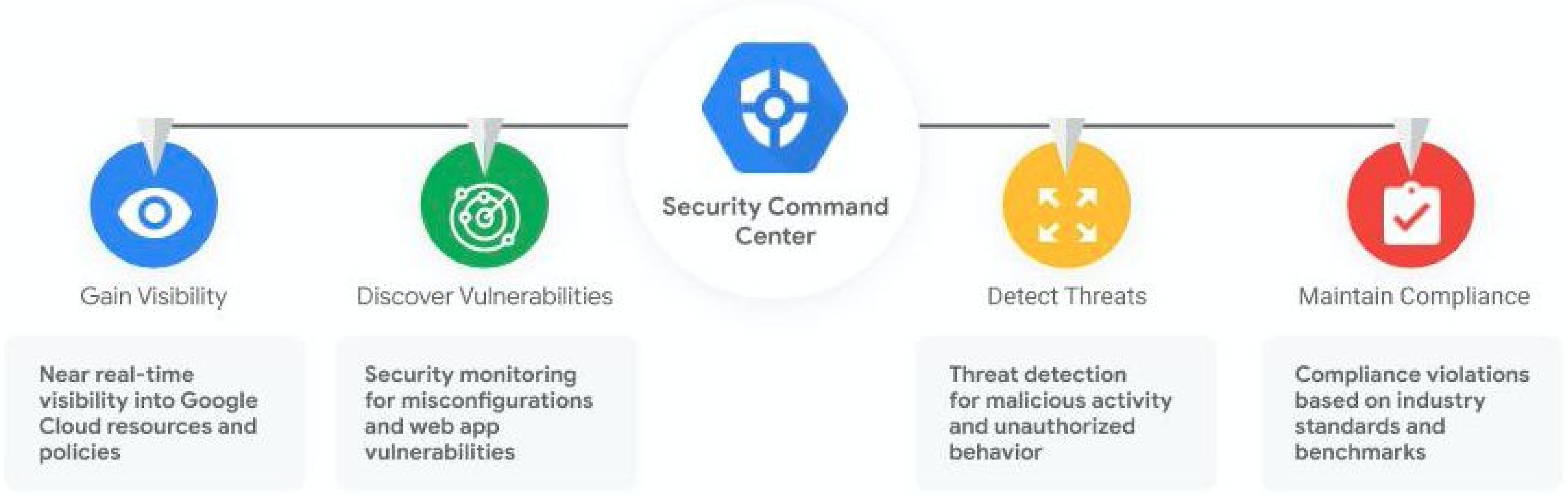
Security Command Center Evaluation Guide

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.


Security Command Center
Gain Visibility
Near real-time visibility into Google Cloud resources and policies
Discover Vulnerabilities
Security monitoring for misconfigurations and web app vulnerabilities
Detect Threats
Threat detection for malicious activity and unauthorized behavior
Maintain Compliance
Compliance violations based on industry standards and benchmarks

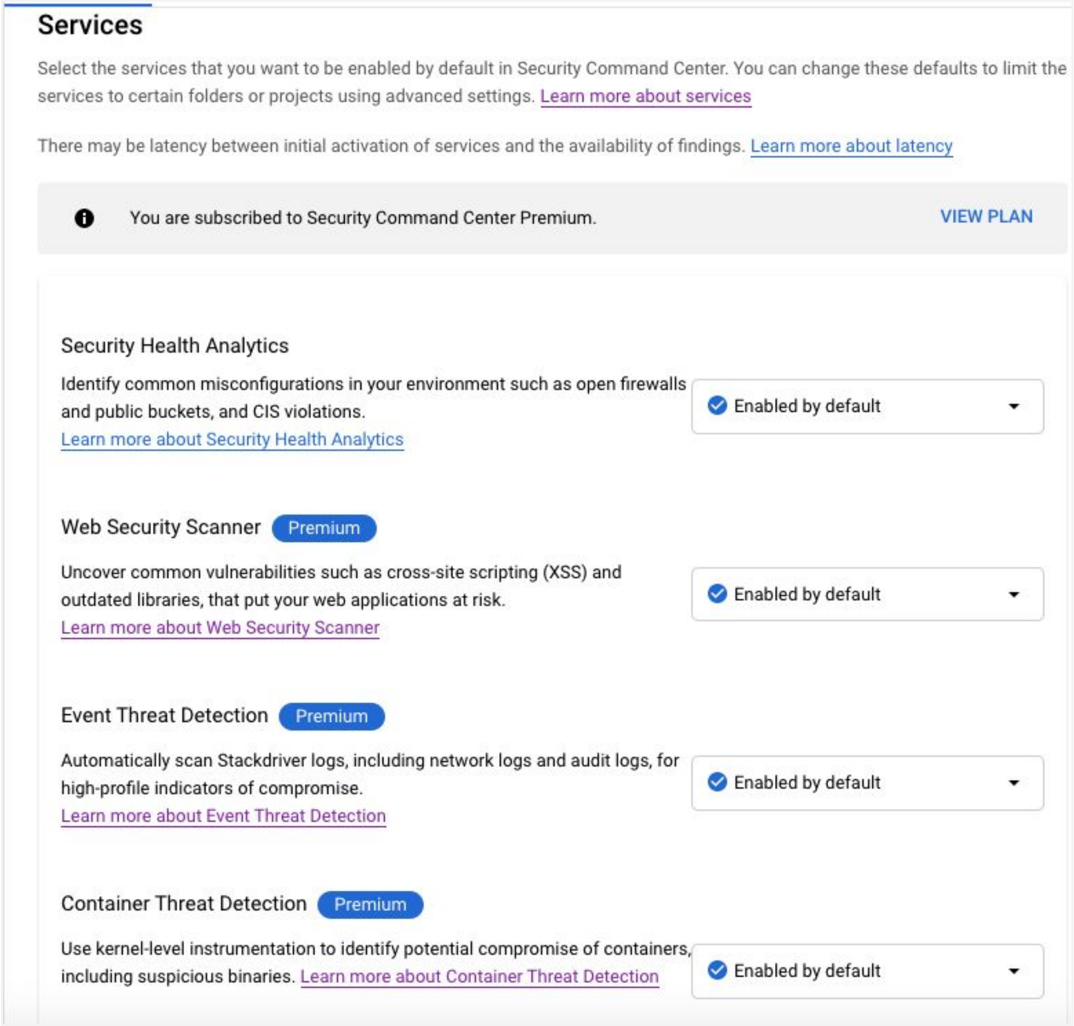
Purpose

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.

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



Services

Select the services that you want to be enabled by default in Security Command Center. You can change these defaults to limit the services to certain folders or projects using advanced settings. Learn more about services

There may be latency between initial activation of services and the availability of findings. Learn more about latency

You are subscribed to Security Command Center Premium.

Security Health Analytics

Identify common misconfigurations in your environment such as open firewalls and public buckets, and CIS violations.
Learn more about Security Health Analytics

Enabled by default

Web Security Scanner Premium

Uncover common vulnerabilities such as cross-site scripting (XSS) and outdated libraries, that put your web applications at risk.
Learn more about Web Security Scanner

Enabled by default

Event Threat Detection Premium

Automatically scan Stackdriver logs, including network logs and audit logs, for high-profile indicators of compromise.
Learn more about Event Threat Detection

Enabled by default

Container Threat Detection Premium

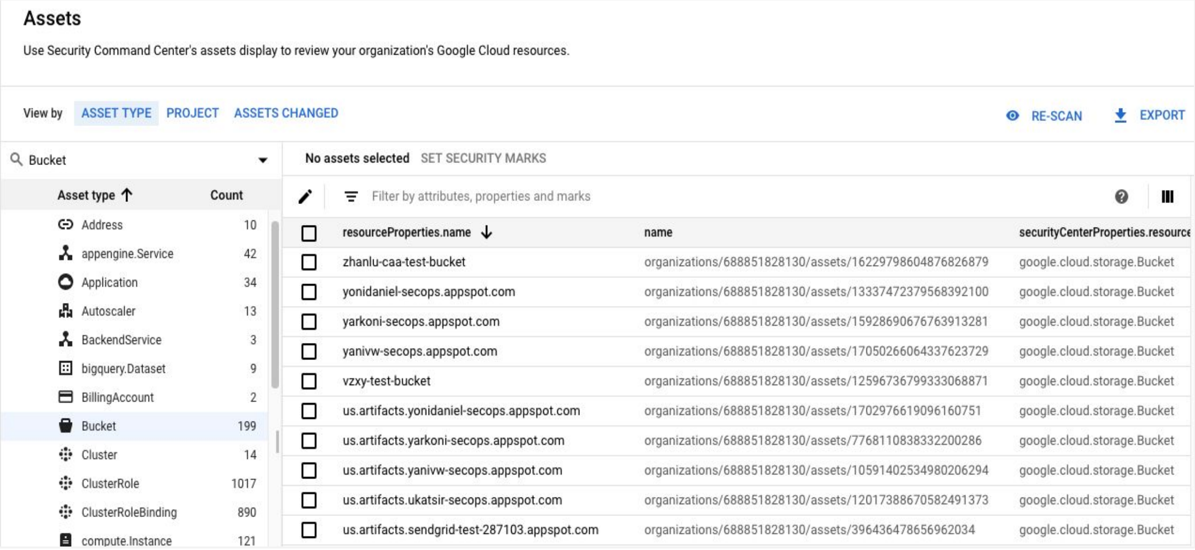
Use kernel-level instrumentation to identify potential compromise of containers, including suspicious binaries. Learn more about Container Threat Detection

Enabled by default

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.



Assets

Use Security Command Center's assets display to review your organization's Google Cloud resources.

Asset type ↑	Count
Address	10
appengine.Service	42
Application	34
Autoscaler	13
BackendService	3
bigquery.Dataset	9
BillingAccount	2
Bucket	199
Cluster	14
ClusterRole	1017
ClusterRoleBinding	890
compute.Instance	121

□	resourceProperties.name ↓	name	securityCenterProperties.resource
□	zhanlu-caa-test-bucket	organizations/688851828130/assets/16229798604876826879	google.cloud.storage.Bucket
□	yonidaniel-secops.appspot.com	organizations/688851828130/assets/13337472379568392100	google.cloud.storage.Bucket
□	yarkoni-secops.appspot.com	organizations/688851828130/assets/15928690676763913281	google.cloud.storage.Bucket
□	yanivw-secops.appspot.com	organizations/688851828130/assets/17050266064337623729	google.cloud.storage.Bucket
□	vzxy-test-bucket	organizations/688851828130/assets/12596736799333068871	google.cloud.storage.Bucket
□	us.artifacts.yonidaniel-secops.appspot.com	organizations/688851828130/assets/1702976619096160751	google.cloud.storage.Bucket
□	us.artifacts.yarkoni-secops.appspot.com	organizations/688851828130/assets/7768110838332200286	google.cloud.storage.Bucket
□	us.artifacts.yanivw-secops.appspot.com	organizations/688851828130/assets/10591402534980206294	google.cloud.storage.Bucket
□	us.artifacts.ukatsir-secops.appspot.com	organizations/688851828130/assets/12017388670582491373	google.cloud.storage.Bucket
□	us.artifacts.sendgrid-test-287103.appspot.com	organizations/688851828130/assets/396436478656962034	google.cloud.storage.Bucket

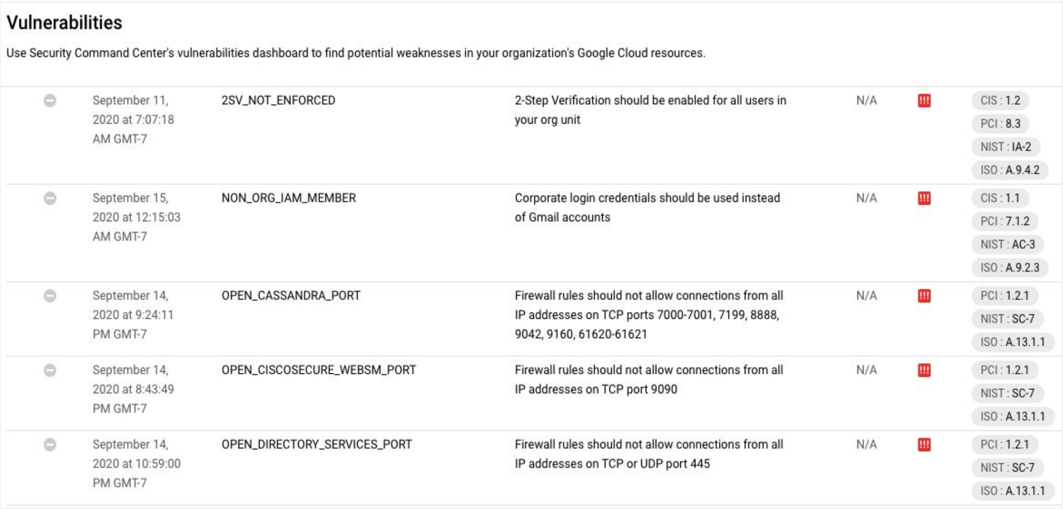
Step 2: Discover vulnerabilities

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



Vulnerabilities

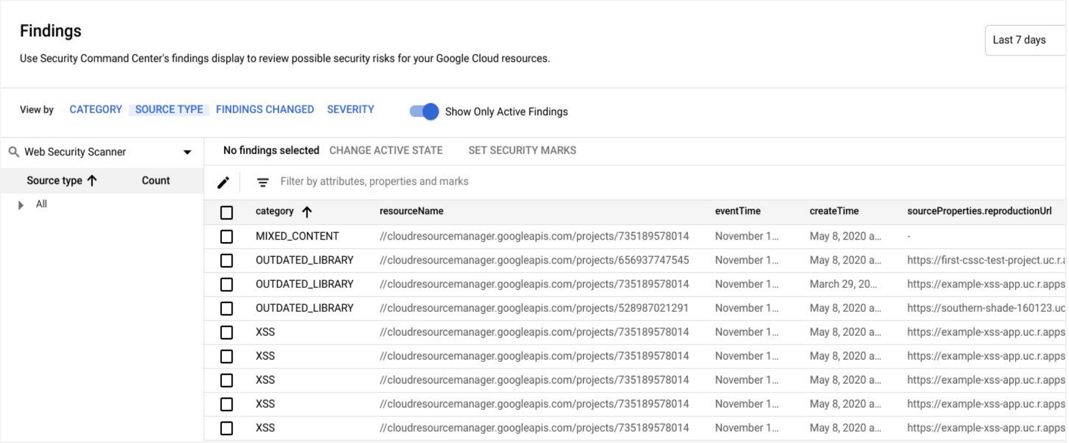
Use Security Command Center's vulnerabilities dashboard to find potential weaknesses in your organization's Google Cloud resources.

⊖	September 11, 2020 at 7:07:18 AM GMT-7	2SV_NOT_ENFORCED	2-Step Verification should be enabled for all users in your org unit	N/A	!!!	CIS : 1.2 PCI : 8.3 NIST : IA-2 ISO : A.9.4.2
⊖	September 15, 2020 at 12:15:03 AM GMT-7	NON_ORG_IAM_MEMBER	Corporate login credentials should be used instead of Gmail accounts	N/A	!!!	CIS : 1.1 PCI : 7.1.2 NIST : AC-3 ISO : A.9.2.3
⊖	September 14, 2020 at 9:24:11 PM GMT-7	OPEN_CASSANDRA_PORT	Firewall rules should not allow connections from all IP addresses on TCP ports 7000-7001, 7199, 8888, 9042, 9160, 61620-61621	N/A	!!!	PCI : 1.2.1 NIST : SC-7 ISO : A.13.1.1
⊖	September 14, 2020 at 8:43:49 PM GMT-7	OPEN_CISCOSECURE_WEBSM_PORT	Firewall rules should not allow connections from all IP addresses on TCP port 9090	N/A	!!!	PCI : 1.2.1 NIST : SC-7 ISO : A.13.1.1
⊖	September 14, 2020 at 10:59:00 PM GMT-7	OPEN_DIRECTORY_SERVICES_PORT	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 445	N/A	!!!	PCI : 1.2.1 NIST : SC-7 ISO : A.13.1.1

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



Findings

Use Security Command Center's findings display to review possible security risks for your Google Cloud resources.

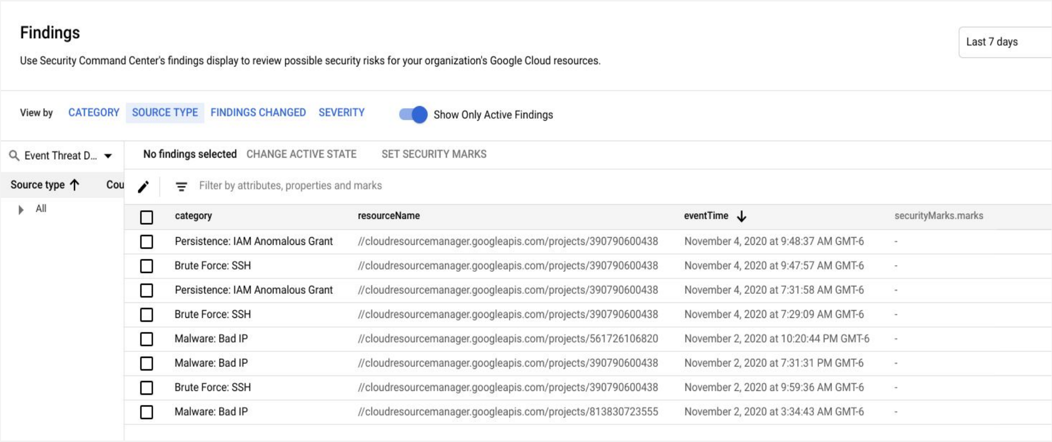
□	category ↑	resourceName	eventTime	createTime	sourceProperties.reproductionUrl
□	MIXED_CONTENT	//cloudresourcemanager.googleapis.com/projects/735189578014	November 1...	May 8, 2020 a...	-
□	OUTDATED_LIBRARY	//cloudresourcemanager.googleapis.com/projects/656937747545	November 1...	May 8, 2020 a...	https://first-cssc-test-project.uc.r.a
□	OUTDATED_LIBRARY	//cloudresourcemanager.googleapis.com/projects/735189578014	November 1...	March 29, 20...	https://example-xss-app.uc.r.apps
□	OUTDATED_LIBRARY	//cloudresourcemanager.googleapis.com/projects/528987021291	November 1...	May 8, 2020 a...	https://southern-shade-160123.uc
□	XSS	//cloudresourcemanager.googleapis.com/projects/735189578014	November 1...	May 8, 2020 a...	https://example-xss-app.uc.r.apps
□	XSS	//cloudresourcemanager.googleapis.com/projects/735189578014	November 1...	May 8, 2020 a...	https://example-xss-app.uc.r.apps
□	XSS	//cloudresourcemanager.googleapis.com/projects/735189578014	November 1...	May 8, 2020 a...	https://example-xss-app.uc.r.apps
□	XSS	//cloudresourcemanager.googleapis.com/projects/735189578014	November 1...	May 8, 2020 a...	https://example-xss-app.uc.r.apps
□	XSS	//cloudresourcemanager.googleapis.com/projects/735189578014	November 1...	May 8, 2020 a...	https://example-xss-app.uc.r.apps

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.



Findings

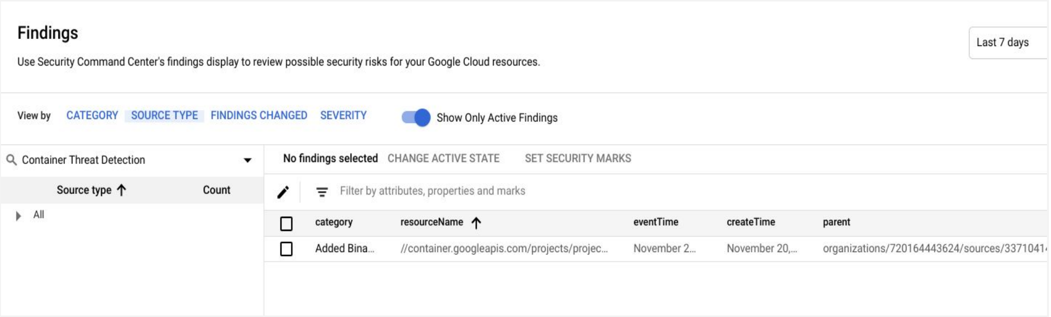
Use Security Command Center's findings display to review possible security risks for your organization's Google Cloud resources.

□	category	resourceName	eventTime	securityMarks.marks
□	Persistence: IAM Anomalous Grant	//cloudresourcemanager.googleapis.com/projects/390790600438	November 4, 2020 at 9:48:37 AM GMT-6	-
□	Brute Force: SSH	//cloudresourcemanager.googleapis.com/projects/390790600438	November 4, 2020 at 9:47:57 AM GMT-6	-
□	Persistence: IAM Anomalous Grant	//cloudresourcemanager.googleapis.com/projects/390790600438	November 4, 2020 at 7:31:58 AM GMT-6	-
□	Brute Force: SSH	//cloudresourcemanager.googleapis.com/projects/390790600438	November 4, 2020 at 7:29:09 AM GMT-6	-
□	Malware: Bad IP	//cloudresourcemanager.googleapis.com/projects/561726106820	November 2, 2020 at 10:20:44 PM GMT-6	-
□	Malware: Bad IP	//cloudresourcemanager.googleapis.com/projects/390790600438	November 2, 2020 at 7:31:31 PM GMT-6	-
□	Brute Force: SSH	//cloudresourcemanager.googleapis.com/projects/390790600438	November 2, 2020 at 9:59:36 AM GMT-6	-
□	Malware: Bad IP	//cloudresourcemanager.googleapis.com/projects/813830723555	November 2, 2020 at 3:34:43 AM GMT-6	-

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.



Findings

Use Security Command Center's findings display to review possible security risks for your Google Cloud resources.

□	category	resourceName	eventTime	createTime	parent
□	Added Bina...	//container.googleapis.com/projects/projec...	November 2...	November 20,...	organizations/720164443624/sources/3371041

Watch this video on getting started with Container Threat Detection

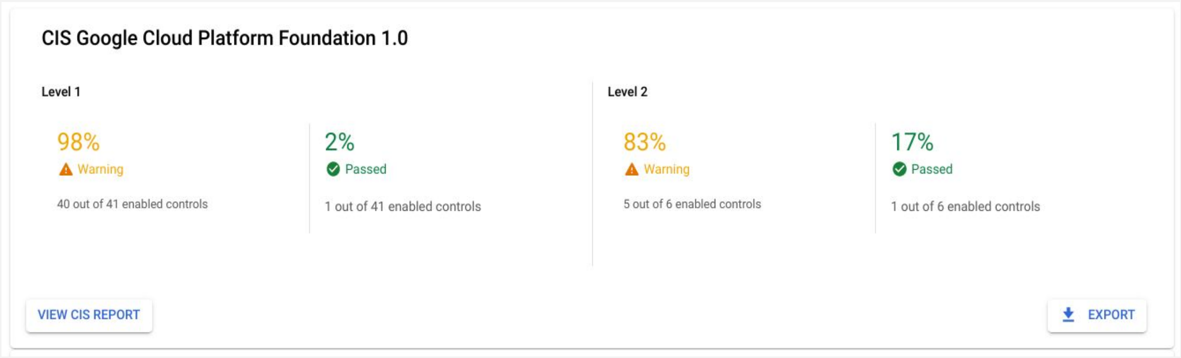
Google Cloud

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.



CIS Google Cloud Platform Foundation 1.0

Level 1

98% ⚠ Warning

40 out of 41 enabled controls

2% ✓ Passed

1 out of 41 enabled controls

Level 2

83% ⚠ Warning

5 out of 6 enabled controls

17% ✓ Passed

1 out of 6 enabled controls

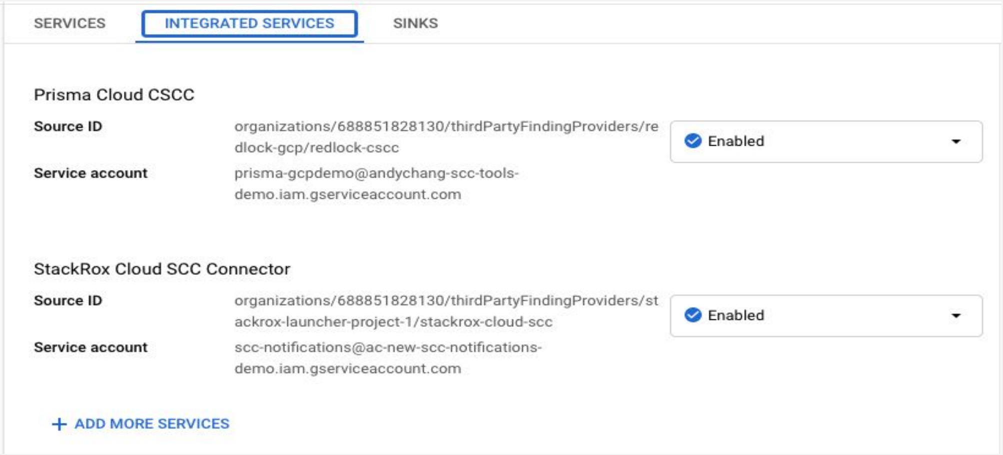
Google Cloud

For more information, visit **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



SERVICES | INTEGRATED SERVICES | SINKS

Prisma Cloud CSCC

Source ID organizations/688851828130/thirdPartyFindingProviders/redlock-gcp/redlock-cscc

Service account prisma-gcpdemo@andychang-scc-tools-demo.iam.gserviceaccount.com

✓ Enabled

StackRox Cloud SCC Connector

Source ID organizations/688851828130/thirdPartyFindingProviders/stackrox-launcher-project-1/stackrox-cloud-scc

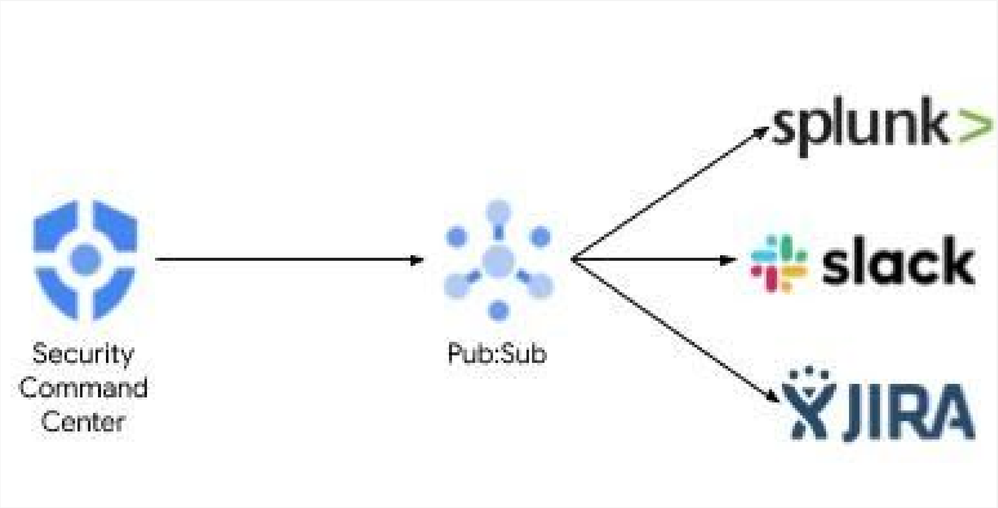
Service account scc-notifications@ac-new-scc-notifications-demo.iam.gserviceaccount.com

✓ Enabled

+ ADD MORE SERVICES

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**