

Course 2_Lab 2: Using Google Security Command Center reports to remediate findings

MY WORK:

Task 1: Identify the vulnerabilities with Security Command Center (SCC)

Google Cloud Skills Boost

Apply your skills in Google Cloud c

← Main menu

02 Strategies for Cloud Security Risk Management

Course · 21 hours 45 minutes 83% complete

Center

Use reports to remediate findings

Test your knowledge: Security Command Center

Understand Google Cloud's Risk Protection Program

The value of shared fate in cloud risk protection programs

Digital sovereignty and sovereign clouds

Test your knowledge: Risk protection programs

Organizational policies in the cloud

Organization Policy

Beginner: Google Cloud Cybersecurity Certificate > Course > Strategies for Cloud Security Risk Management >

Quick tip: Review the prerequisites before you run the lab

End Lab 01:08:46

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more.](#)

Open Google Cloud console

Google Cloud username
student-04-bb3e6c203c3ci

Google Cloud password
XsNB2cDu1EpF

Google Cloud project ID
qwiklabs-gcp-01-1f90a2f1

4. In the **Google Cloud compliance standards** section, click **View details** in the **CIS Google Cloud Platform Foundation 2.0** tile. The CIS Google Cloud Platform Foundation 2.0 report opens.

5. Click on the **Findings** column to sort the findings and display the active findings at the top of the list.

Which of the following rules in the report have active findings for the Cloud Storage bucket? Select all that apply.

☒ Cloud Storage buckets should not be anonymously or publicly accessible

☐ Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22

☐ VMs should not be assigned public IP addresses

☒ Bucket policy only should be Enabled

Submit

Task 2. Remediate the security vulnerabilities

Security Command Ce...

Risk Overview

Threats

Vulnerabilities

Compliance

Assets

Findings

Sources

Posture Management

Detections and Controls

Google SecOps

reCAPTCHA

Model Armor

Web Security Scanner

Cyber Insurance Hub

Binary Authorization

Advisory Notifications

Access Approval

Managed Microsoft AD

Data Protection

Sensitive Data Protecti...

Data Loss Prevention

Certificate Authority Se...

Key Management

Certificate Manager

Secret Manager

Zero Trust

Console & APIs Access...

Chrome Enterprise Pre...

Marketplace

Release Notes

View the breakdown of your controls by compliance status. Adjust the time period to view the state of your controls over time.

Filter Enter property name or value

Control	Status	Rule	Severity	Findings	Resources scanned
1.4	Non-compliant	User-managed service accounts should not have user-managed keys	High	1	1
1.5	Non-compliant	ServiceAccount should not have Admin privileges	High	1	1
2.1	Non-compliant	Cloud Audit Logging should be configured properly across all services and all users from a project	High	1	1
2.2	Non-compliant	Links should be configured for all Log entries	High	1	1
2.4	Non-compliant		High	1	
2.5	Non-compliant		High	1	
2.6	Non-compliant		High	1	
2.7	Non-compliant		High	1	
2.8	Non-compliant		High	1	
2.9	Non-compliant		High	1	
2.10	Non-compliant		High	1	
2.12	Non-compliant		High	1	
3.1	Non-compliant		High	1	
3.6	Non-compliant		High	1	
3.7	Non-compliant		High	1	
4.4	Non-compliant		High	1	
1.1	Compliant		Low	0	
1.2	Compliant		Low	0	
1.6	Compliant		Low	0	
1.7	Compliant		Low	0	

Join the community

The Security Command Center community is a dedicated space for users to connect, ask questions, learn, and grow together.

Detect attacks on the environment

Help document

Learn how Security Command Center Premium helps you detect and stop attacks.

Improve cloud security posture

Help document

Learn about improving your security posture on Google Cloud with Security Command Center.

Configuring Security Command Center

Help document

Learn how to configure Security Command Center services and features, such as mute rules and Cloud Logging export.

Mute Findings in Security Command Center

Help document

Learn how to control the volume of findings that you receive by muting findings.

Event Threat Detection overview

Help document

Learn how Event Threat Detection can help you detect threats in your Google Cloud environment in real time.

Virtual Machine Threat Detection overview

Help document

Learn how VM Threat Detection can help you identify threats like cryptomining abuse in Compute Engine instances.

Container Threat Detection overview

Help document

Learn how Container Threat Detection helps you identify potential threats to containers on Google Cloud.

Web Security Scanner overview

Help document

Learn how Web Security Scanner can help you identify vulnerabilities in your web applications.

Google Cloud Security Command Center Premium

Compliance detail

UTC-4 Apr 24, 2025 May 1, 2025 May 8, 2025 May 15, 2025

Filter Enter property name or value

Control	Status	Rule	Severity	Findings	Resources scanned
1.1	Compliant			0	
1.2	Compliant			0	
1.4	Non-compliant			1	
1.5	Non-compliant			1	
1.6	Compliant			0	
1.7	Compliant			0	
1.8	Compliant			0	
1.9	Compliant			0	
1.10	Compliant			0	
1.11	Compliant			0	
1.12	Compliant			0	
1.13	Compliant			0	
1.14	Compliant			0	
1.15	Compliant			0	
1.16	Compliant			0	
1.17	Compliant			0	
1.18	Compliant			0	
2.1	Non-compliant			1	
2.2	Non-compliant			1	
2.3	Compliant			0	

Learn more about Security Command Center Premium

Join the community

The Security Command Center community is dedicated space for users to connect, ask questions, learn, and grow together.

Detect attacks on the environment

Help document

Learn how Security Command Center Premium helps you detect and stop cyber attacks.

Improve cloud security posture

Help document

Learn about improving your security posture on Google Cloud with Security Command Center.

Configuring Security Command Center

Help document

Learn how to configure Security Command Center services and features, such as mute rules and Cloud Logging exports.

Mute findings in Security Command Center

Help document

Learn how to control the volume of findings that you receive by muting findings.

Event Threat Detection overview

Help document

Learn how Event Threat Detection can help you detect threats in your Google Cloud environment in real time.

Virtual Machine Threat Detection

Vulnerabilities were remediated at this stage based on the requirements for the Google Lab.

Cloud Storage Bucket details

qwklabs-gcp-01-1f90a2fedbca

Public to internet: This bucket is publicly accessible because allUsers or allAuthenticatedUsers have one or more permissions. Remove these principals to stop public access.

Edit access Dismiss

Location: us-west1 (Oregon) Storage class: Standard Public access: Public to internet Protection: Soft Delete

Objects Configuration Permissions Protection Lifecycle Observability New Inventory Reports Operations

Public access

Public to internet

One or more bucket-level permissions grant access to everyone on the internet (allUsers) or anyone signed into a Google account (allAuthenticatedUsers). If this bucket should not be publicly accessible, remove these public permissions or prevent public access to this bucket. [Learn more](#)

Prevent public access

Access control

Fine-grained: Object-level ACLs enabled

Access to objects can be granted through object access control lists (ACLs). To enforce a single set of permissions on the bucket and its objects, switch to uniform bucket-level access control. [Learn more](#)

Switch to uniform

Permissions

View by principals View by roles

Grant access Remove access

Filter Enter property name or value

Type	Principal	Name	Role	Inheritance
	1094389810671@cloudbuild.gserviceaccount.com	Legacy Cloud Build Service Account	Cloud Build Service Account	qwklabs-gcp-01-1f90a2fedbca

Get started with Cloud Storage

Getting bucket information

Help document

Get information on the size and of your Cloud Storage buckets.

Uploading objects

Help document

Upload the objects containing your Cloud Storage buckets.

Downloading objects

Help document

Download the objects from your Storage buckets.

Use cases for Cloud Storage

Help document

Explore use cases, best practice industry solutions.

Terraform samples

Help document

See examples of using Terraform Cloud Storage resources.

Architecture guides for storage

Help document

Discover best practices and reference architectures for storage.

Prevent public access

Tutorial

Modify the public access settings for your bucket.

The top screenshot shows the 'Edit access control' dialog in the Google Cloud console. The dialog prompts the user to choose how to control object access in the bucket. The 'Uniform' option is selected, which ensures uniform access to all objects in the bucket by using only bucket-level permissions (IAM). The 'Fine-grained' option is also available, which grants access to individual objects by using object-level permissions (ACLs) in addition to bucket-level permissions. A warning message states: 'Uniform access control removes object ACLs from this bucket. This will revoke object access for users who rely solely on ACLs for access unless you add their permissions to the bucket's IAM policy.' The 'Add project role ACLs to the bucket IAM policy' option is also present.

The bottom screenshot shows the 'Permissions' tab in the Google Cloud console. The 'Public access' section indicates that 'Subject to object ACLs' is currently selected. The 'Access control' section shows 'Fine-grained: Object-level ACLs enabled'. A 'Switch to uniform' button is visible. The 'Permissions' section shows a list of roles and principals, including 'Cloud Build Service Account (1)', 'Cloud Build Service Agent (1)', 'Compute Engine Service Agent (1)', 'Storage Admin (1)', 'Storage Legacy Bucket Owner (2)', and 'Storage Legacy Bucket Reader (1)'. A message at the bottom indicates 'allUsers removed'.

Access control lists have been updated for buckets that required changes for this lab.

TO DO:

My Self-Assessment:

Add information to explain the steps above with pictures.

