Start Lab 01:30:00

Getting Started with Security Command Center

Lab 1 hour No cost Introductory

GSP1124

Google Cloud Self-Paced Labs

Overview

Security Command Center (SCC) is a security monitoring platform that helps users:

- Discover security-related misconfigurations of Google Cloud resources.
- Report on active threats in Google Cloud environments.
- Fix vulnerabilities across Google Cloud assets.

In this lab, you take your first steps with Security Command Center by exploring the service's interface, configurations, and vulnerability findings.

What you'll do

In this lab, you learn how to:

- Explore SCC interface elements.
- Configure SCC settings at the project level.
- Analyze and fix SCC vulnerability findings.

Prerequisites

It is recommended the learner has familiarity with the following before starting this lab:

- Fundamental understanding of cloud computing concepts.
- Familiarity with the Google Cloud Console.
- Familiarity with severity classifications for findings is recommended, but not required.

Setup and requirements

Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

To complete this lab, you need:

- Access to a standard internet browser (Chrome browser recommended).

> **Note:** Use an Incognito or private browser window to run this lab. This prevents any conflicts between your personal account and the Student account, which may cause extra charges incurred to your personal account.

- Time to complete the lab---remember, once you start, you cannot pause a lab.

> **Note:** If you already have your own personal Google Cloud account or project, do not use it for this lab to avoid extra charges to your account.

How to start your lab and sign in to the Google Cloud console

1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is the **Lab Details** panel with the following:
    - The **Open Google Cloud console** button
    - Time remaining
    - The temporary credentials that you must use for this lab
    - Other information, if needed, to step through this lab
2. Click **Open Google Cloud console** (or right-click and select **Open Link in Incognito Window** if you are running the Chrome browser).

    The lab spins up resources, and then opens another tab that shows the **Sign in** page.

    Tip: Arrange the tabs in separate windows, side-by-side.

    > **Note:** If you see the **Choose an account** dialog, click **Use Another Account**.

3. If necessary, copy the **Username** below and paste it into the **Sign in** dialog.

    ```
    "Username"
    ```

    You can also find the **Username** in the **Lab Details** panel.

4. Click **Next**.
5. Copy the **Password** below and paste it into the **Welcome** dialog.

    ```
    "Password"
    ```

You can also find the **Password** in the **Lab Details** panel.

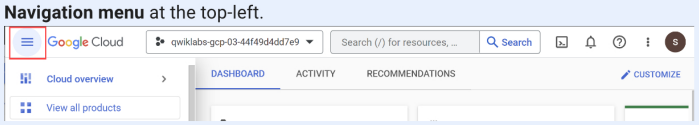
6. Click **Next**.

> **Important:** You must use the credentials the lab provides you. Do not use your Google Cloud account credentials.

> **Note:** Using your own Google Cloud account for this lab may incur extra charges.

7. Click through the subsequent pages:
    - Accept the terms and conditions.
    - Do not add recovery options or two-factor authentication (because this is a temporary account).
    - Do not sign up for free trials.

After a few moments, the Google Cloud console opens in this tab.

> **Note:** To view a menu with a list of Google Cloud products and services, click the **Navigation menu** at the top-left.


Activate Cloud Shell

Cloud Shell is a virtual machine that is loaded with development tools. It offers a persistent 5GB home directory and runs on the Google Cloud. Cloud Shell provides command-line access to your Google Cloud resources.

1. Click **Activate Cloud Shell** at the top of the Google Cloud console.

When you are connected, you are already authenticated, and the project is set to your **Project_ID**, `PROJECT_ID`. The output contains a line that declares the **Project_ID** for this session:

```
Your Cloud Platform project in this session is set to "PROJECT_ID"
```

`gcloud` is the command-line tool for Google Cloud. It comes pre-installed on Cloud Shell and supports tab-completion.

2. (Optional) You can list the active account name with this command:

```
gcloud auth list
```

3. Click **Authorize**.

Output:

```
ACTIVE: *
ACCOUNT: "ACCOUNT"

To set the active account, run:
    $ gcloud config set account `ACCOUNT`
```

4. (Optional) You can list the project ID with this command:

```
gcloud config list project
```

Output:

```
[core]
project = "PROJECT_ID"
```

Note: For full documentation of `gcloud`, in Google Cloud, refer to the gcloud CLI overview guide.

Scenario

Cymbal Bank is an American retail bank with over 2,000 branches in all 50 states. It offers comprehensive debit and credit services that are built on top of a robust payments platform. Cymbal Bank is a digitally transforming legacy financial services institution.

Cymbal Bank was founded in 1920 under the name Troxler. Cymbal Group acquired the company in 1975 after it had been investing heavily in Cymbal Group's proprietary ATMs. As the bank grew into a national leader, they put strategic emphasis on modernizing the customer experience both in-person at their branches and digitally through an app they released in 2014. Cymbal Bank employs 42,000 people nationwide and, in 2019, reported $24 billion in revenue.

Cymbal Bank is interested in integrating a centralized security monitoring platform to help monitor threats and remediate vulnerabilities across their Google Cloud resources in their corporate banking applications. As a Cloud Security Engineer, you are tasked with learning about Security Command Center's cutting-edge features so you can deliver a presentation to the CTO on the services' benefits.

Task 1. Explore SCC interface elements

In this task, you will tour the Security Command Center (SCC) interface and learn about the service's chief features.

1. Open the navigation menu and select **Security > Security Command Center > Risk Overview**.

Note: If you see the message that you need to "Create an Organization", simply refresh the browser.

2. Scroll down and investigate the information panels that refer to "New threats over time" and "Vulnerabilities per resource type".

- **Threats** notify Google Cloud users about current suspicious activities happening in their Google Cloud environments, such as a service account investigating its own permissions

permissions.
- **Vulnerabilities** provide information on misconfigurations or vulnerabilities of resources, such as an open TCP port or an outdated library running on a Virtual Machine.

Threats and vulnerabilities are two different types of *finding classes*, which SCC uses to categorize and report security issues in your environment. Check out this documentation to learn more about finding classes.

A *finding* is a record generated by SCC, which provides details on vulnerability or threat data in the Security Command Center dashboard.

3. In the "New threats over time" card, select the **FINDINGS BY RESOURCE TYPE** tab.

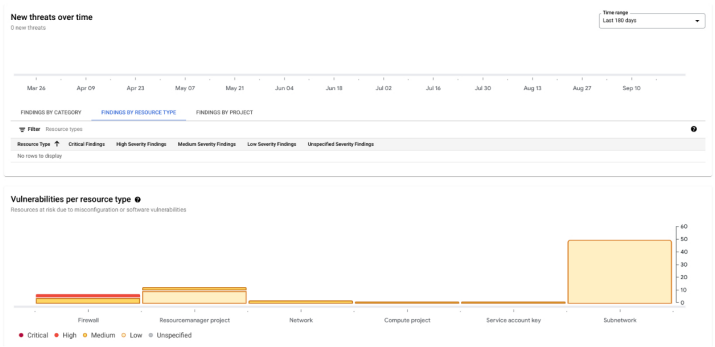
This card enumerates currently active threats that have happened in your project during the period of time determined by the "Time range" drop down on the right side of this information panel.

> **Note:** The number of threats will be zero because you are in a sandbox Google Cloud project that has never been attacked before. You will protect yourself from threats in the next lab *Detect and Investigate Threats with Security Command Center*.

By default, the time range drop down shows all threats that appeared during the last 7 days, but you can view all threats that happened during the last 180 days.

4. Scroll down to the **Vulnerabilities per resource type** card.

5. From the time range selector, select **Last 180 days**. Your output should be similar to the following:



You should see around 76 active vulnerabilities listed.

A majority of these findings are generated because we are using the default VPC network, which is insecure by design. For example, it contains firewall rules that allow SSH and RDP access from any IP address.

6. Now scroll down to the **Active vulnerabilities** card below.

7. Select the **FINDINGS BY CATEGORY** tab.

This will show your environment's vulnerabilities organized by different categories of vulnerabilities and their *severity*. This is a property of the finding that helps to estimate the risk that the issue poses to the Google Cloud environment.

The level of severity cannot be changed—each type of finding has a severity level that is predetermined by SCC. Below is a list of the different types of severities and common examples:

- **Critical** - for example, a Reverse Shell session launched from inside of a GKE Pod.
- **High** - for example, an SSH port opened to the entire Internet (0.0.0.0/0);
- **Medium** - for example, one of primitive IAM roles (Owner/Editor/Viewer) has been granted to a user or a service account;
- **Low** - for example, no VPC Flow logs are collected
- **Unspecified** - can appear in SCC, but are not common.

Note that here we only gave examples of findings with different severities. Detailed criteria for setting findings severity are described on the page security classifications

criteria for setting finding's severity are described on the page severity classifications for findings.

Note: Take notice that the findings about open RDP and SSH ports have high severity levels.

8. Now select the **FINDINGS BY RESOURCE TYPE** tab. This will show vulnerabilities categorized by the different types of Google Cloud resources available.

Note: This project has a default VPC Network, so most findings here are related to network components such as firewall, network or subnetwork.

9. Finally, select the **FINDINGS BY PROJECT** tab. This tab is more informative when you use SCC on the level of a folder or organization root node.

Note: In our lab we have access only to one project, so this tab contains only the name of the current project.

10. In the left-hand menu, under the Security Command Center header, open each of the following tabs and read their description below:

- **Threats:** gives you a quick overview of findings that are classified as threats in SCC. Some examples could be:
    - Successful attempt of an SSH BruteForce attack (link).
    - Cryptomining software running on compute resources (link).
    - Reverse shell session was launched from inside a GKE container (link).
- **Vulnerabilities:** this tab gives you a quick overview of all misconfigurations or flaws in software which might exist in the current scope (whether that be inside your project, folder, or organization). This gives you more fine-grained access to the vulnerabilities, allowing you to drill down into each one. Some examples of vulnerabilities are:
    - MySQL port open to the whole Internet (link).
    - An Owner/Editor/Viewer role has been assigned to a user or a Service Account (link).
    - A web-page or a web-application vulnerable to XSS-attacks (link).
- **Compliance:** shows information about compatibility of your Project with the most important compliance standards such as CIS, PCI DSS, NIST 800-53 and others.
- **Findings:** this tab allows you to explore all findings available in the SCC database. We will investigate findings and how to work with them in task 3.
- **Sources:** the software modules that analyze configuration of Google Cloud resources and monitor current activities by reading log files and checking currently running processes. We can say that Sources are the actual "detectors" of SCC, which analyze configuration of resources and publish information to SCC.

11. Now, click the back button in your browser.

What triggered the significant amount of findings in this project?

- ◯ The project contains default VPC network.
- ◯ All Google Cloud projects are insecure.
- ◯ They were custom generated for this lab.
- ◯ The project contains default service accounts.

Submit

Task 2. Configure SCC settings at project level

In this task, you will learn how to configure SCC settings at the project level.

1. Click **SETTINGS** from the top right corner of the overview page.

2. Ensure you are on the **SERVICES** tab.

This tab will allow you to set up parameters of SCC's integrated services, which are also called sources ("the brains of SCC", as we learned about in the previous task). In this lab the terms services and sources are interchangeable.

Services detect threats and vulnerabilities and provide information to SCC. Most of them are available only in the Premium edition of SCC, which is what you have in this lab.

The following are built-in services that you can configure:

- **Security Health Analytics (SHA):** finds and reports misconfigurations of resources (disabled logs, extra IAM permissions, publicly exposed services). This is what we have currently enabled in our project and what detected the 76 vulnerabilities in our project.
- **Web Security Scanner (WSS):** scans publicly available web applications exposed via external IP addresses and checks for OWASP top 10 vulnerabilities. You will have a chance to work with this in a later lab.
- **Container Threat Detection (CTD):** can detect the most common container runtime attacks in a Container Optimized OS (will also be shown in a later lab).
- **Event Threat Detection (ETD):** log-based threat analysis that continuously monitors Google Cloud and Google Workspace logs to scan for potential threats.
- **Virtual Machine Threat Detection:** analyzes memory of VM instances on the level of a Hypervisor and can detect suspicious activities happening in VM memory. Examples are unexpected kernel modules or running crypto-mining software.
- **Rapid Vulnerability Detection (RVD):** a zero-configuration network and web application scanner that actively scans public endpoints to detect vulnerabilities that have a high likelihood of being exploited.

3. Click on the link **MANAGE SETTINGS** for **Security Health Analytics**.

4. Click on the tab **MODULES**.

Modules are pre-defined, or custom units of detection logic. As you can see, SCC offers many different types of modules that can help you detect different misconfigurations of resources. SCC makes it easy to enable and disable different types of modules to support your security posture and the resources you are interested in monitoring.

5. In the filter, type in **VPC_FLOW_LOGS_SETTINGS_NOT_RECOMMENDED.**

6. Select **Enable** from the Status dropdown.

Security Health Analytics will now check whether the `enableFlowLogs` property of VPC subnetworks is missing or set to false.

> **Note:** There is a delay until SCC will start scanning resources using the newly enabled module.

Now that you are familiar with Security Command Center's different services and how to configure them, you will identify and fix a vulnerability with SCC.

Task 3. Analyze and fix SCC vulnerability findings

In this task, you will learn how to manage and mitigate vulnerability findings.

1. Open the navigation menu and select **Security > Security Command Center > Risk Overview**.
2. From the left-hand menu, select the **FINDINGS** tab.
3. Set the time range selector in the top-right corner to **All time**.

Roughly how many findings in total can you see in the list?

- ◯ 50
- ◯ 40
- ◯ 60
- ◯ 70

Submit

4. In the top-left corner of the screen, find the **Query preview** window, which contains a filter for sorting through all available findings.

By default in the **FINDINGS** tab you can see unmuted findings with the state **ACTIVE**.

The two properties *state* and *mute* of every finding define visibility of findings in many filters used for SCC.

- The Mute value can be set on findings by the security analyst or it can be set automatically if the analyst does not want to see irrelevant and noisy findings in the SCC interface.
- The State property indicates whether a finding requires attention and has not been addressed yet, or if it's been fixed or otherwise addressed and is no longer active.

A recommended way to manage the lifecycle of findings and hide them is to use the "mute" property. Changing the "state" property is typically handled by software sources.

5. In the "Quick filters" card select the category **Default network**.
6. Note that the query string in the "Query preview" has changed (it now has `AND category="DEFAULT_NETWORK"` attached to it.)
7. Select the checkbox next to "Default network" and select **CHANGE ACTIVE STATE**.
8. Set the state to **Inactive** state for this finding.

Now the finding has been deactivated and hidden from the screen because by default you can see only active and not muted findings.

9. Reset the **FINDINGS** tab view by clicking **Risk Overview**, then **Findings** under the SCC header.

Roughly how many findings in total can you see in the list?

- ◯ 70
- ◯ 60
- ◯ 50

40

Submit

10. Now press the **EDIT QUERY** button.
11. Change the query string in the Query Editor to `category="DEFAULT_NETWORK"`.
12. When you finish editing, press the **APPLY** button.
13. Ensure you see only one "Default network" finding.

If you look at the left-hand menu under "Quick filters", you will see that the "Show inactive" checkbox is selected. SCC gives you the flexibility to search for active and inactive findings. Now, you will revert the state of this finding.

14. Select the checkbox next to "Default network" and select **CHANGE ACTIVE STATE**.
15. Set the **Active** state for this finding.

Findings can be activated and deactivated manually, but they never can be deleted by a user. They are deleted automatically only when a finding has not been refreshed by scanners during 13 months.

When a security scanner checks the same finding and does not detect the misconfiguration which kicked off the finding, it marks it as "INACTIVE". If the vulnerability still presents in the system, the finding will stay in the same "ACTIVE" state.

16. Reset the findings tab by clicking the **Clear All** button next to Quick Filters.
17. In the "Query preview" window, click **Edit Query**.
18. Now copy and paste the the following query:

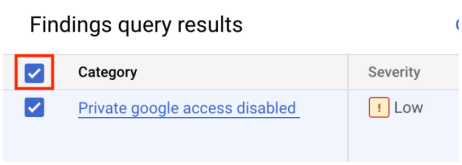
```
state="ACTIVE" AND NOT mute="MUTED" AND
resource.type="google.compute.Subnetwork"
```

19. When you finish editing, press the **APPLY** button.

Now you should see all findings related to subnetworks. Our default VPC network was created with `--subnet-mode=auto` parameter, so none of its subnets have Private Google Access enabled and all subnets do not write VPC Flow logs.

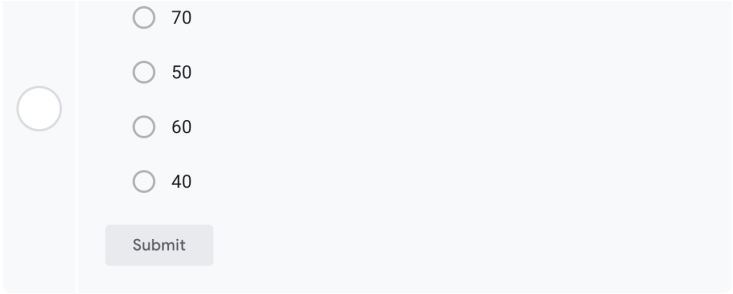
Imagine that we are working in a test environment, so we do not want to see SCC findings about Private Google Access in this network.

20. In the "Quick filter" window select the category **Private google access disabled**.
21. Now click on the **Category** checkbox so all "Private google access disabled" findings are selected:



22. Now click the **MUTE OPTIONS** button.
23. Then click **Mute**. This operation mutes existing findings.
24. Reset the findings query by clicking **Risk Overview**, then **Findings**.

Roughly how many findings in total can you see in the list?



Now that the "Private google access disabled" findings are muted, you will no longer see any of them in the Console. As you can see, muting is a powerful way to filter Security Command Center's results, and provides you the fine-grained control over your resources and findings you are interested in.

Another misconfiguration of the default network is that VPC Flow Logs are also disabled in the subnets of this network. Since we are working in a test environment, we won't need VPC Flow Logs enabled, so we are going to mute all existing and all future findings related to this category.

25. Click the button **MUTE OPTIONS > Create mute rule**.

Note: You will create SCC configuration which will mute existing and all new findings satisfying the criteria, defined in the "Finding query" field. Note that previously we muted existing "Private google access disabled" (PGA) findings.

That was a one-time operation and newly coming findings reporting about disabled PGA will still appear in SCC. If you create a mute rule, you will effectively mute all existing and all new findings.

26. In the new window enter a new Mute rule ID: **muting-pga-findings**.

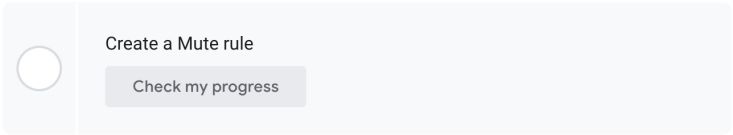
27. For the mute rule description, enter **Mute rule for VPC Flow Logs.**

28. In the "finding query" enter the following filter:

```
category="FLOW_LOGS_DISABLED"
```

29. Now press the **SAVE** button.

You should see a notification in the bottom part of the Console that a mute rule was created.



30. Now refresh the main SCC Dashboard by selecting **Findings** from the left-hand menu.

31. Ensure that you no longer see any "Private google access disabled" or "Flow logs disabled" findings.

Note: If you still see any of these findings displayed, please refresh the browser's tab.

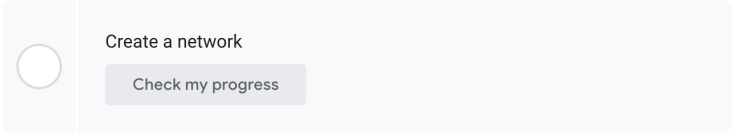
Now we will create one more network with automatically configured subnets.

32. Open a new Cloud Shell session (▶) and run the following command to create this network:

```
gcloud compute networks create scc-lab-net --subnet-mode=auto
```

33. Ensure you see a similar output:

```
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-03-c6821aef4c0f/global/networks/SCC-lab-net].
NAME: SCC-lab-net
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
```



34. Close the Cloud Shell window after you have verified the above message.

35. Refresh the SCC findings window and note that you can see newly created "Private google access disabled" finding, but there are no findings about VPC Flow Logs (this is because of the mute rule we created earlier).

36. Although we created mute rules for VPC Flow Logs, SCC still allows you to view them by using the query editor.

37. Click the **Edit Query** button and paste in the following:

```
category="FLOW_LOGS_DISABLED"
```

38. Now click **Apply**.

39. Check the findings query results table and note that in the column "Resource display name" you can see both networks: "defaults" and "SCC-lab-net".

Note: If you do not see the default network, please make sure that the parameter "Rows per page" is set to 100. You can see this parameter in the right bottom corner of the page. Also check that the “Time Range” parameter is set to the “All time” value.

40. In the "Query preview" window, click **Edit Query**.

41. Now copy and paste the the following query:

```
state="ACTIVE" AND NOT mute="MUTED"
```

42. When you finish editing, press the **APPLY** button.

43. Now we will investigate and fix two findings with high severity.

44. In the Quick Filters section, select **High** from the list of severity options.

You should see two findings: "Open RDP port" and "Open SSH port". They have been initiated because the "default" network contains two firewall rules enabling SSH and RDP traffic to all instances in this network from the whole Internet.

45. Click on the **Open RDP port** finding.

A new window will appear. In this window you will find a detailed description of the issue itself, list of affected resources and "Next steps", which help you remediate it.

46. Click on the link to go to the firewall rules page, which will open a new tab.

47. Click **default-allow-rdp** firewall rule.

48. Click **EDIT**.

49. Delete the source IP range **0.0.0.0/0**.

50. Add the following source IP range **35.235.240.0/20** and press **Enter**.

> **Note:** This range of IP addresses is used for connecting to VM instances securely via Identity Aware Proxy. More information is available on the page Using IAP for TCP forwarding.

51. Do not change any other parameters!

52. Click **SAVE**.

53. Once saved, close the browser tab where you edited the firewall rule.

54. Refresh the SCC finding browser tab.

55. You should now see only one finding with "High" severity - "Open SSH Port".

56. Click on the **Open SSH port** finding.

57. Click on the link to go to the firewall rules page, which will open in a new tab.

58. Click **default-allow-ssh** firewall rule.

59. Click **EDIT**.

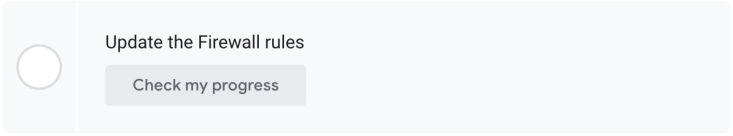
60. Delete the source IP range **0.0.0.0/0**.

61. Add the following source IP range **35.235.240.0/20** and press **Enter**.

62. Do not change any other parameters!

63. Click **SAVE**.

64. Once saved, close the browser tab where you edited the firewall rule.



65. Now close the window with an open finding description and refresh the browser window.

66. You should now see no findings with High severity.

You have now successfully used Security Command Center to identify and remediate critical security vulnerabilities in your Google Cloud environment.

Congratulations!

Throughout this lab, you learned how to explore SCC interface elements, configure SCC settings at the project level, and analyze and fix SCC vulnerability.

Next steps / Learn more

- Check out the lab titled Analyzing Findings with Security Command Center.

Google Cloud training and certification

...helps you make the most of Google Cloud technologies. Our classes include technical skills and best practices to help you get up to speed quickly and continue your learning journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. Certifications help you validate and prove your skill and expertise in Google Cloud technologies.

Manual Last Updated April 29, 2024

Lab Last Tested April 29, 2024