Start Lab 01:52:30

Detect and Investigate Threats with Security Command Center

Lab 1 hour 15 minutes No cost Intermediate

GSP1125

Overview

Event Threat Detection is an integrated service of Security Command Center (SCC) that monitors Google Cloud logs for patterns signaling suspicious activities.

Container Threat Detection is another integrated service of SCC. This service can continuously monitor GKE working nodes. When it detects suspicious events, it analyzes them to confirm whether they can be treated as incidents or not.

In this lab, you receive hands-on practice with SCC's threat detection features and learn how to investigate and triage common vulnerabilities associated with events, virtual machines, and containers. You learn how to surface and manage your findings with SCC's Event Threat Detection and Container Threat Detection.

What you'll do

In this lab, you learn how to:

- Initiate and mitigate a threat with Event Threat Detection
- Configure a cloud environment to detect threats
- Manage SCC findings with Event Threat Detection
- Build an environment for detecting container threats
- Exploit a web server and detect issues with Container Threat Detection

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 the Security Command Center interface
- Familiarity with containers and Google Kubernetes Engine is recommended, but not required

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.

As a Cloud Security Engineer at Cymbal Bank, your task is to explore and implement robust security measures, leveraging Security Command Center's Event and Container Threat Detection capabilities for its Google Cloud resources. By integrating these services, you will ensure real-time monitoring, swift anomaly identification, and proactive vulnerability management for our event-driven architectures and containerized applications.

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**.

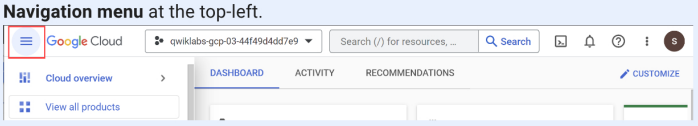
    > **Important:** You must use the credentials the lab provides you. Do not use your Google Cloud account credentials.

    > **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.

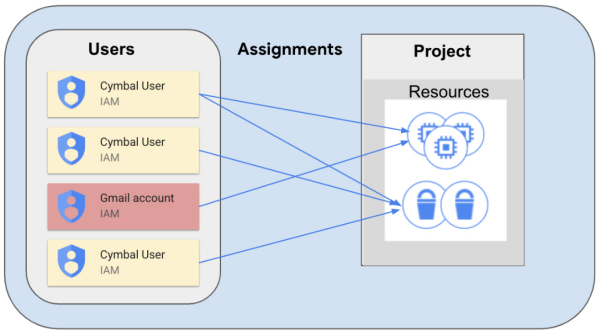
> **Note:** To view a menu with a list of Google Cloud products and services, click the **Navigation menu** at the top-left.
>
> 
>

Enable the Security Command Center API

1. Click on the **Navigation menu** in the top left corner of the Google Cloud console.
2. Select **APIs & Services** from the drop down and click on **Enable APIs & Services**.
3. Click **+ Enable APIs & Services**
4. Search for `Security Command Center API` in the search box.
5. Click on **Security Command Center API**, then click **Enable**

Task 1. Initiate and mitigate a threat with Event Threat Detection

Your first task as a Cloud Security Engineer for Cymbal Bank is to initiate and mitigate non-compliant accounts threats with Event Threat Detection.



The Event Threat Detection service of SCC detects many threats by monitoring suspicious activities reported in Google Cloud logs. One of these activities might be delegating sensitive roles to an external user, such as someone who has a miscellaneous `gmail.com` account that isn't tied to your corporate domain.

This might happen in situations when an intruder has managed to access a GCP organization and now they are interested in establishing persistence. To do this, the hacker would grant sensitive roles to their `@gmail.com` account.

This delegation simulates establishing persistence. If a hacker accidentally gets temporary access to your system, they will need to establish persistence and to get access to a more stable account.

1. In the Google Cloud Console, open the navigation menu and select **IAM & Admin > IAM**.
2. Press the **Grant Access** button.
3. In the "New principals" field, enter the demo email address `demouser1@gmail.com`
4. For the Role field, select **BigQuery > BigQuery Admin** and click **Save**.
5. Open the navigation menu and select **Security > Security Command Center > Findings**

6. Change the Time Range dropdown to the **Last 6 hours.**

You should see three Findings, two of which are related to the access you just granted:

- *Non org IAM member*
- *Persistence: IAM anomalous grant*

7. Click on the Finding **Non org IAM member** and scroll down to check the "Source display name" in the description of this Finding.
8. Ensure that the display name is set to Security Health Analytics—this is the SCC service that detected a misconfiguration in your Google Cloud Project.
9. Close the window with the Finding.
10. Click on the other Finding **Persistence: IAM anomalous grant** and scroll down to check the "Source display name" in the description of this Finding.
11. Ensure that the display name is set to "Event Threat Detection"—this is the SCC service that detected a misconfiguration in your Google Cloud Project.
12. Scroll to the top of the window and select the tab **Source Properties**.
13. In this tab expand the **Properties > sensitiveRoleGrant** field.
14. There you can find the most important characteristics of this finding:

- **principalEmail:** who performed the suspicious action
- **bindingDetails:** information about the role and the member to whom this role has been granted
- **members:** to whom the permission has been granted

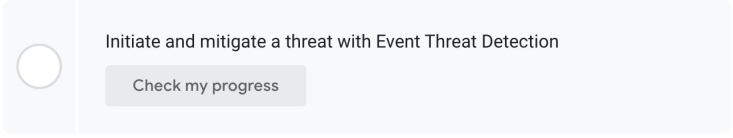
15. Close the Finding window.
16. From the navigation menu, select **IAM & Admin > IAM**.
17. Click the checkbox next to the `demouser1@gmail.com` principal and click the button **Remove Access**.
18. Click **Confirm**.
19. Now open the navigation menu and select **Security > Security Command Center > Findings**.

Note that the Findings "Non org IAM member" has disappeared from the list of findings. This is because the Security Health Analytics service has checked the updated configuration of IAM policies and deactivated this Finding.

> **Note:** If you still see this Finding in the list, please refresh the browser's tab.

The Finding "Persistence: IAM anomalous grant" has not changed its status. It was initiated by the ETD service, and cannot be deactivated automatically. We have already investigated this Finding and we can be sure that the user from gmail.com domain does not have access to our project.

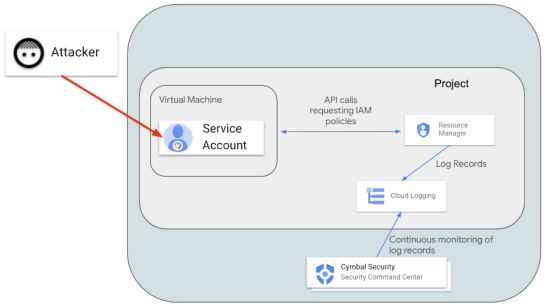
Click **Check my progress** to verify the objective.



> **Note:** If you are receiving less than 20 points for this task in the "Checkpoints" right-hand column, click the "Check my progress" button a couple of times.

Task 2. Configure a cloud environment to detect threats

Now that you've investigated and checked for non-compliant accounts, you'll configure Cymbal's environment to detect service account threats through logging.



Many logs in Google Cloud are enabled by default, but for detecting specific threats you will need to enable additional data access logs. In this exercise we will investigate the Service Account Self-Investigation threat.

In this scenario, a malicious actor exploits vulnerable software on a virtual machine and obtains access to the Default Service Account (which was used to create the instance). The actor wants to understand what they can do in the Google Cloud environment. To check their permissions, the actor will call the projects.getIamPolicy method. SCC should detect and report this suspicious activity recorded in the logs.

For SCC to detect this activity, we need to enable Resource Manager Admin Read logs.

1. In the Google Cloud Console open the navigation menu and select **IAM & Admin > Audit Logs.**

> **Note:** You can safely ignore the message: "You don't have permission to view inherited audit logs configuration data for one or more parent resources."

2. In the list of services find **Cloud Resource Manager API** and click the checkbox next to it.

> **Note:** If you cannot find it, scroll down to the parameter "Rows per page" and set its value to 200.

3. On the right side of the tab, find the configuration frame: **Cloud Resource Manager API - Permission Types**.

4. Select the **Admin Read** check box and click **Save.**

Now Resource Manager Data Read audit logs are collected and Event Threat Detection can analyze them.

For reproducing the scenario, you will need to create a new virtual machine with a default Service Account and `cloud-platform` access scope.

5. Open the navigation menu and select **Compute Engine > VM instances**.

6. Then click the **Create Instance** button.

7. Select region as **`Region`** and set zone as **`Zone`**.

8. In the "Access scopes" section, select the **Allow full access to all Cloud APIs** value.

9. Leave all other parameters set to their default value.
10. Click **Create** to launch the new VM instance.
11. Once the instance is created, click on the **SSH** button.
12. Accept the authorization prompts when the new SSH window opens.
13. In the SSH session, enter the following command:

```
gcloud projects get-iam-policy $(gcloud config get project)
```

You should see the list of IAM permissions granted to users in the Google Cloud project.

14. Open the navigation menu and select **Security > Security Command Center > Findings.**
15. Set the value of the time range selector to **Last hour**.

You should see **5** Security Findings related to the instance you just created:

- *Discovery: Service Account Self-Investigation*
- *Full API access*
- *Default service account used*
- *Compute secure boot disabled*
- *Public IP address*

The Finding "Discovery: Service Account Self-Investigation" was initiated by Event Threat Detection (ETD), which classifies findings with the *THREAT* Finding Class.

Other findings have been initiated by the Security Health Analytics component, which classifies Findings as *MISCONFIGURATION*.

16. Click on the Finding **Discovery: service account self-investigation**.
17. Select the **Source Properties** tab at the top of the window.
18. Now expand the field **properties > serviceAccountGetsOwnIamPolicy**.
19. Inspect the following values:

- **principalEmail** - the email address of the Service Account that is investigating its own permissions
- **callerIp** - IP address from which the `projects.getIamPolicy` method was called. In our case it should be the external IP address of the virtual machine `instance-1`.

20. Exit out of the Finding window.

Outside of this scenario, this Finding can inform us that our virtual machine and the default Service Account have been compromised and we need to investigate and contain this incident.

Now that we've investigated this finding, let's mute it.

21. Click on the checkbox next to the **Discovery: Service Account Self-Investigation** Finding.
22. Click on the **MUTE OPTIONS** drop-down list.
23. Then select the **Mute** option.
24. Ensure that this Finding no longer appears in the SCC interface.

Click **Check my progress** to verify the objective.

Configure a cloud environment to detect threats

Check my progress

Task 3. Manage SCC findings with Event Threat Detection

As you see, for detecting some threats you need to enable additional logs, which are not enabled by default. For detecting some findings, you also need to create additional configurations, such as DNS policies.

This will allow you to detect malicious software running on compute resources and identify well-known malicious DNS addresses.

When a DNS request is made on a virtual machine, this query is not logged by default, and in turn SCC cannot detect connections to malicious internet resources.

In the previous task, we enabled logs for the Resource Manager service using an IAM configuration. For logging all DNS queries, you will need to create a DNS policy with enabled logging.

> **Note:** You can learn more about logging and monitoring metrics for Cloud DNS here.

1. To enable full DNS query logging, open the navigation menu and select **Network services > Cloud DNS.**
2. Select the "DNS Server Policies" tab and then click the **Create Policy** button.
3. Enter **dns-test-policy** for the name of the DNS policy.
4. Select the **On** radio-button for DNS logs.
5. In the "Alternate DNS servers" part, select **default** from the network dropdown and click **OK**.
6. Click the **Create** button.
7. Now return to the SSH session of our virtual machine and try connecting to the malicious URL by running the following command:

```
curl etd-malware-trigger.goog
```

You should receive a similar output:

```
<!DOCTYPE html>
<html lang="en-us">
<meta charset="utf-8">
<title>ETD Malware Trigger</title>
<p>This domain is used to trigger a malware finding in Google Event
Threat Detection. For more information, please visit <a
href="https://cloud.google.com/event-threat-
detection">https://cloud.google.com/event-threat-detection</a>
```

8. Return to the Google Cloud Console.
9. Open the navigation menu and select **Security > Security Command Center > Findings**.
10. You should now see a new threat appear "Malware: Bad Domain"

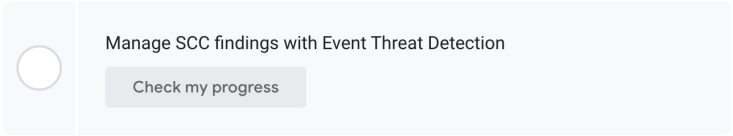
> **Note:** If you don't see the new threat, refresh your browser window.

11. Click on this Finding.
12. In the new window, click on the **SOURCE PROPERTIES** tab.
13. Expand the **properties** field and examine the following:

- **domains:** the list of domains for which the instance requested address resolution
- **instanceDetails:** the ID of the instance that connected to the "malicious" domain

14. Close the Finding Window.
15. Click on the checkbox near the Finding **Malware: Bad Domain**.
16. Now click on the **Mute Options** drop-down list.
17. Click **Mute**. This Finding will now be removed from the SCC interface.
18. From the navigation menu, select **Compute Engine > VM instances.**
19. Click on the checkbox next to the `instance-1` virtual machine and press **Delete.**
20. Confirm the delete action by clicking **Delete**.

Click **Check my progress** to verify the objective.



Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly

notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly

security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the

security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their

containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their

through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability

through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a

Task 4. Build an environment for detecting container threats

Cymbal Bank is focused on enhancing their corporate banking application's scalability through Google Kubernetes Engine (GKE). To ensure the utmost security for their containers, you will implement Container Threat Detection to actively monitoring the security status of each container, detecting potential threats in real-time, and promptly notifying your team of any incidents.

With this proactive approach and seamless integration with Google Cloud Security Command Center, you can confidently safeguard Cymbal's deployments and services to maintain a robust security posture.

Container Threat Detection (CTD) is a special service that tracks suspicious activities happening inside GKE-based workloads. Currently CTD supports detection of several threats, such as:

- **Added binary executed:** initiated when a new binary, which was not a part of a container, is launched.
- **Added library loaded:** similar to the previous finding, but monitors only newly launched libraries.
- **Reverse shell:** a process inside of the container redirects network streams to a