**Diagrama

Descripción generada automáticamenteUn dibujo de un animal con la boca abierta

Descripción generada automáticamente con confianza baja**

P4 Respond and recover from a data breach

[Subtítulo del documento]

26 de junio de 2024

adrián gonzález iglesias

máster sistemas multicloud

INSTITUTO TAJAMAR

**Índice**

Contenido

[**Índice** 1](#_Toc170293779)

[**Respond and recover from a data breach** 2](#_Toc170293780)

[**Activity overview** 3](#_Toc170293781)

[**Scenario** 3](#_Toc170293782)

[**Task 1. Analyze the data breach and gather information** 5](#_Toc170293783)

[**Task 2. Fix the Compute Engine vulnerabilities** 12](#_Toc170293784)

[Challenge: Delete the compromised VM 13](#_Toc170293785)

[**Task 3. Fix Cloud Storage bucket permissions** 15](#_Toc170293786)

[Challenge: Modify storage bucket access 15](#_Toc170293787)

[**Task 4. Limit firewall ports access** 17](#_Toc170293788)

[Challenge: Restrict SSH access 17](#_Toc170293789)

[**Task 5. Fix the firewall configuration** 18](#_Toc170293790)

[Challenge: Customize firewall rules 18](#_Toc170293791)

[Challenge: Enable logging 18](#_Toc170293792)

[**Task 6. Verify compliance** 20](#_Toc170293793)

[**Conclusion** 21](#_Toc170293794)

[**End your lab** 22](#_Toc170293795)

**Respond and recover from a data breach**

[Respond and recover from a data breach | Google Cloud Skills Boost](https://www.cloudskillsboost.google/paths/419/course_templates/970/labs/471969)

experimentLabschedule1 hour 30 minutesuniversal\_currency\_alt2 Creditsshow\_chartIntroductory

important icon **IMPORTANT:**  
  
screenshot icon Take screenshots of your work for each task to add to your portfolio.  
  
desktop/laptop icon Make sure to complete this hands-on lab on a desktop/laptop only.  
  
check icon There are only 5 attempts permitted per lab.  
  
quiz target icon As a reminder – it is common to not get every question correct on your first try, and even to need to redo a task; this is part of the learning process.  
  
timer icon Once a lab is started, the timer cannot be paused. After 1 hour and 30 minutes, the lab will end and you’ll need to start again.  
  
tip icon For more information review the **Lab technical tips** reading.

**Activity overview**

This lab is part of the capstone project. In this lab, you’ll apply your knowledge of cloud cybersecurity to identify and remediate vulnerabilities.

You’ll be given a scenario, and a set of tasks to complete in Google Cloud Security Command Center. These tasks will require you to use your skills to work to analyze and remediate active vulnerabilities relating to a security incident, answer questions about the vulnerabilities, and complete challenges that will assess your cloud cybersecurity skills.

There are also a number of challenges in the lab. A challenge is a task where you will be asked to complete the task on your own without instructions.

By successfully completing this lab, you will demonstrate your ability to identify, prioritize, and remediate security vulnerabilities and misconfigurations within the cloud environment. These are essential skills to enhance the security posture of Google Cloud environments, reducing the risk of data breaches, unauthorized access, and other security incidents.

**Scenario**

For the last year, you've been working as a junior cloud security analyst at Cymbal Retail. Cymbal Retail is a market powerhouse currently operating 170 physical stores and an online platform across 28 countries. They reported $15 billion in revenue in 2022, and currently employ 80,400 employees across the world.

Cymbal Retail boasts a vast customer base with a multitude of transactions happening daily on their online platform. The organization is committed to the safety and security of its customers, employees, and its assets, ensuring that its operations meet internal and external regulatory compliance expectations in all the countries it operates in.

Recently, the company has experienced a massive data breach. As a junior member of the security team, you’ll help support the security team through the lifecycle of this security incident. You'll begin by identifying the vulnerabilities related to the breach, isolate and contain the breach to prevent further unauthorized access, recover the compromised systems, remediate any outstanding compliance related issues, and verify compliance with frameworks.

Here’s how you'll do this task: **First** you’ll examine the vulnerabilities and findings in Google Cloud Security Command Center. **Next**, you’ll shut the old VM down, and create a new VM from a snapshot. **Then**, you’ll evoke public access to the storage bucket and switch to uniform bucket-level access control. **Next**, you’ll limit the firewall ports access and fix the firewall rules. **Finally**, you’ll run a report to verify the remediation of the vulnerabilities.

**Task 1. Analyze the data breach and gather information**

One morning, the security team detects unusual activity within their systems. Further investigation into this activity quickly reveals that the company has suffered a massive security breach across its applications, networks, systems, and data repositories. Attackers gained unauthorized access to sensitive customer information, including credit card data, and personal details. This incident requires immediate attention and thorough investigation. The first step towards understanding the scope and impact of this breach is to gather information and analyze the available data.

In this task, you'll examine the vulnerabilities and findings in Google Cloud Security Command Center to determine how the attackers gained access to the data, and which remediation steps to take.

***Important:****The vulnerabilities listed in this section rely on specific security checks being run beforehand. If some checks haven't run yet, the related vulnerabilities might not appear in the Security Command Center when you complete the steps in this section. Don't worry though! You can still use the information provided in this task to analyze the available findings and proceed with the remediation steps in the tasks that follow.*

**First**, navigate to the Security Command Center to view an overview of the active vulnerabilities.

**El primer paso viendo lo sucedido va a ser, reunir y analizar la información disponible para entender el alcance y el impacto de la brecha.**

1. In the Google Cloud console, in the **Navigation menu** (navigation_menu), click **Security > Overview**. The Security Command Center Overview page opens.

**Accedemos a Risk overview para visualizar el estado de seguridad:**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. Scroll down to **Active vulnerabilities**. This provides an overview of current security vulnerabilities or issues that need attention within the Google Cloud environment.

**Aquí, podemos identificar los problemas de seguridad que necesitan ser solucionados para proteger la infraestructura y como vemos hay algún que otro problema.**

Interfaz de usuario gráfica, Tabla

Descripción generada automáticamente

1. Select the **Findings By Resource Type** tab. The security findings or vulnerabilities based on the type of cloud resource affected (e.g., instances, buckets, databases) are organized. By reviewing active vulnerabilities and findings by resource type, you can prioritize and address security issues effectively.

**Organizamos las vulnerabilidades según el recurso afectado (instancias, buckets…) pinchando en Findings by resource type.**

Imagen que contiene Tabla

Descripción generada automáticamente

You'll note that there are both high and medium severity findings relating to the **Cloud Storage bucket**, the **Compute Instance virtual machine**, and the **firewall**

Which three resource types are listed with high severity findings?

* Network, Subnetwork, and compute.Instance
* Bucket, Subnetwork, and ServiceAccountKey
* Network, Firewall, and Bucket
* Bucket, compute.Instance, and Firewall

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Next**, navigate to the PCI DSS report.

1. In the **Security Command Center** menu, click **Compliance**. The Compliance page opens.

**A continuación, accedemos a Compliance para ver las normas de cumplimiento.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. In the **Google Cloud compliance standards** section, click **View details** in the **PCI DSS 3.2.1** tile. The PCI DSS 3.2.1 report opens.

**Entramos en PCI DSS 3.2.1 que es un estándar de seguridad de datos.**

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

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

**Hacemos click en Findings para ordenar las vulnerabilidades activas en la parte superior de la lista.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

As you examine the PCI DSS 3.2.1 report, notice that it lists the rules that are non-compliant, which relate to the data breach:

* **Firewall rule logging should be enabled so you can audit network access**: This medium severity finding indicates that firewall rule logging is disabled, meaning that there is no record of which firewall rules are being applied and what traffic is being allowed or denied. This is a security risk as it makes it difficult to track and investigate suspicious activity.
* **Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389**: This high severity finding indicates that the firewall is configured to allow Remote Desktop Protocol (RDP) traffic for all instances in the network from the whole internet. This is a security risk as it allows anyone on the internet to connect to the RDP port on any instance in the network.
* **Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22**: This high severity finding indicates that the firewall is configured to allow Secure Shell (SSH) traffic to all instances in the network from the whole internet. SSH is a protocol that allows secure remote access to a computer. If an attacker can gain access to a machine through SSH, they could potentially steal data, install malware, or disrupt operations.
* **VMs should not be assigned public IP addresses**: This high severity finding indicates that a particular IP address is actively exposed to the public internet and is potentially accessible to unauthorized individuals. This finding is considered a potential security risk because it could allow attackers to scan for vulnerabilities or launch attacks on the associated resource.
* **Cloud Storage buckets should not be anonymously or publicly accessible**: This high severity finding indicates that there is an Access Control List (ACL) entry for the storage bucket that is publicly accessible which means that anyone on the internet can read files stored in the bucket. This is a high-risk security vulnerability that needs to be prioritized for remediation.
* **Instances should not be configured to use the default service account with full access to all Cloud APIs**: This medium severity finding indicates that a particular identity or service account has been granted full access to all Google Cloud APIs. This finding is considered a significant security risk because it grants the identity or service account the ability to perform any action within the Google Cloud environment, including accessing sensitive data, modifying configurations, and deleting resources.

Since you're focusing on identifying and remediating the issues related to the security incident, please disregard the following findings as they do not relate to the remediation tasks you’re completing:

* **VPC Flow logs should be Enabled for every subnet VPC Network**: There are a number of low severity findings for Flow Logs disabled. This indicates that Flow Logs are not enabled for a number of subnetworks in the Google Cloud project used for this lab. This is a potential security risk because Flow Logs provide valuable insights into network traffic patterns, which can help identify suspicious activity and investigate security incidents.
* **Basic roles (Owner, Writer, Reader) are too permissive and should not be used**: This medium severity finding indicates that primitive roles are being used within the Google Cloud environment. This is a potential security risk because primitive roles grant broad access to a wide range of resources.
* **An egress deny rule should be set**: This low severity finding indicates that no egress deny rule is defined for the monitored firewall. This finding raises potential security concerns because it suggests that outbound traffic is not restricted, potentially exposing sensitive data or allowing unauthorized communication.

**Estas brechas de seguridad comparten el denominador común de exponer vulnerabilidades significativas dentro del entorno de Google Cloud. Todas ellas involucran configuraciones inseguras o prácticas deficientes que podrían facilitar el acceso no autorizado o la explotación por parte de actores malintencionados. Desde la falta de registro de reglas de firewall, que limita la capacidad de monitorear y responder a actividades sospechosas, hasta permitir conexiones abiertas desde cualquier dirección IP a servicios críticos como RDP y SSH, estas deficiencias comprometen la integridad y seguridad de los sistemas y datos alojados en la plataforma. Además, la asignación de direcciones IP públicas a instancias y la configuración de accesos públicos a buckets de almacenamiento reflejan una falta de control adecuado sobre los activos digitales, aumentando el riesgo de exposición a amenazas externas.**

The following table pairs the rules listed in the report with their corresponding findings category. This will assist you when examining the findings according to resource type later:

|  |  |
| --- | --- |
| **Findings category** | **Rule** |
| Firewall rule logging disabled | Firewall rule logging should be enabled so you can audit network access |
| Open RDP port | Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389 |
| Open SSH port | Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22 |
| Public IP address | VMs should not be assigned public IP addresses |
| Public bucket ACL | Cloud Storage buckets should not be anonymously or publicly accessible |
| Full API access | Instances should not be configured to use the default service account with full access to all Cloud APIs |
| Flow logs disabled | VPC Flow logs should be Enabled for every subnet VPC Network |
| Primitive roles used | Basic roles (Owner, Writer, Reader) are too permissive and should not be used |
| Egress deny rule not set | An egress deny rule should be set |

Overall, these findings indicate a critical lack of security controls and non-compliance with essential PCI DSS requirements; they also point to the vulnerabilities associated with the data breach.

**A continuación vamos a analizar detalladamente las vulnerabilidades dentro del entorno de Google Cloud en SCC.**

1. In the Google Cloud console, in the **Navigation menu** (navigation_menu), click **Security > Findings**. The **Findings** page opens.

**Accedemos a Findings.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. In the **Quick filters** panel, in the **Resource Type** section, select the checkbox for the **Google Cloud storage bucket** resource type.

**Dentro de tipo de recurso en los filtros, vamos a filtrar por Google Cloud Storage Bucket**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

The following active findings pertaining to the storage bucket should be listed:

* **Public bucket ACL**: This finding is listed in the PCI DSS report, and indicates that anyone with access to the internet can read the data stored in the bucket.
* **Bucket policy only disabled**: This indicates that there is no explicit bucket policy in place to control who can access the data in the bucket.
* **Bucket logging disabled**: This indicates that there is no logging enabled for the bucket, so it will be difficult to track who is accessing the data.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Estas vulnerabilidades comparten la característica de señalar deficiencias críticas en la configuración de seguridad del bucket de almacenamiento en Google Cloud. En conjunto, destacan vulnerabilidades significativas que comprometen la integridad y privacidad de los datos almacenados. La ACL pública del bucket expone los datos a cualquier usuario de Internet, mientras que la falta de una política explícita del bucket permite un acceso potencialmente no autorizado. Además, la ausencia de registro para el bucket dificulta la auditoría y la respuesta efectiva ante actividades sospechosas o incidentes de seguridad. Estas deficiencias indican la necesidad urgente de implementar controles adecuados para proteger adecuadamente los datos sensibles almacenados en el entorno de Google Cloud.**

1. In the **Quick filters** panel, in the **Resource Type** section, uncheck **Google Cloud storage bucket,** andselect the checkbox for the **Google compute instance** resource type.

**Ahora filtramos por Google Compute Instance.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

The following active findings that pertain to the virtual machine named **cc-app-01** should be listed:

* **Malware bad domain**: This finding indicates that a domain known to be associated with malware was accessed from the google.compute.instance named cc-app-01. Although this finding is considered to be of low severity, it indicates that malicious activity has occurred on the virtual machine instance and that it has been compromised.
* **Compute secure boot disabled**: This medium severity finding indicates that secure boot is disabled for the virtual machine. This is a security risk as it allows the virtual machine to boot with unauthorized code, which could be used to compromise the system.
* **Default service account used**: This medium severity finding indicates that the virtual machine is using the default service account. This is a security risk as the default service account has a high level of access and could be compromised if an attacker gains access to the project.
* **Public IP address**: This high severity finding is listed in the PCI DSS report and indicates that the virtual machine has a public IP address. This is a security risk as it allows anyone on the internet to connect to the virtual machine directly.
* **Full API access**: This medium severity finding is listed in the PCI DSS report, and indicates that the virtual machine has been granted full access to all Google Cloud APIs.

Captura de pantalla de computadora

Descripción generada automáticamente

**Estas vulnerabilidades comparten el riesgo de exponer vulnerabilidades críticas en las instancias de máquinas virtuales en Google Cloud. Revelan problemas como accesos comprometidos a través de dominios de malware, la deshabilitación del arranque seguro que permite la ejecución de código no autorizado, el uso de cuentas de servicio predeterminadas con amplios privilegios, la asignación de direcciones IP públicas que facilitan el acceso desde Internet, y el acceso completo a todas las APIs de Google Cloud, que podría ser mal utilizado por atacantes para comprometer el sistema. Estas deficiencias subrayan la importancia de implementar controles de seguridad robustos para proteger adecuadamente las instancias virtuales en la nube.**

These findings indicate the virtual machine was configured in a way that left it very vulnerable to the attack. To remediate these findings you'll shut the original VM (cc-app-01) down, and create a VM (cc-app-02) using a clean snapshot of the disk. The new VM will have the following settings in place:

* No compute service account
* Firewall rule tag for a new rule for controlled SSH access
* Secure boot enabled
* Public IP address set to None

1. In the **Time range** field, expand the drop-down, and select **Last 30 days**. This will ensure the list includes findings for the last 30 days.
2. In the **Quick filters** panel, in the **Resource Type** section, uncheck **Google compute instance**, and select the checkbox for the **Google compute firewall** resource type.

**Y por último, filtramos por Google Compute Firewall.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

The following active findings should be listed that pertain to the firewall:

* **Open SSH port**: This high severity finding indicates that the firewall is configured to allow Secure Shell (SSH) traffic to all instances in the network from the whole internet.
* **Open RDP port**: This high severity finding indicates that the firewall is configured to allow Remote Desktop Protocol (RDP) traffic to all instances in the network from the whole internet.
* **Firewall rule logging disabled**: This medium severity finding indicates that firewall rule logging is disabled. This means that there is no record of which firewall rules are being applied and what traffic is being allowed or denied.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Y estas vulnerabilidades tienen la característica de exponer vulnerabilidades críticas relacionadas con la configuración del firewall en Google Cloud:**

**Permiten acceso desde cualquier dirección de Internet a todas las instancias de la red, tanto para SSH como para RDP, lo cual aumenta el riesgo de accesos no autorizados.**

**Además, la falta de registro de reglas de firewall dificulta la capacidad de monitorear y auditar qué tráfico se permite o deniega, lo que compromete la capacidad de detectar y responder adecuadamente a actividades maliciosas.**

Which of the following findings are listed as high severity findings?

* Public IP address, Default service account used, Full API access, and Firewall rule logging disabled
* Firewall rule logging disabled, Compute secure boot disabled, Public IP address, and Bucket logging disabled
* Public bucket ACL, Public IP address, Open SSH port, and Open RDP port

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Bucket policy only disabled, Bucket logging disabled, Malware bad domain, and Compute secure boot disabled

**Task 2. Fix the Compute Engine vulnerabilities**

In this task, you'll shut down the vulnerable VM **cc-app-01** and create a new VM from a snapshot taken before the malware infection. VM snapshots are effective in restoring the system to a clean state, and ensures that the new VM will not be infected with the same malware that compromised the original VM.

**Vamos a crear una nueva máquina desde una snapshot hecha, antes de que estuviera infectada por malware, con esto conseguimos, solucionar la vulnerabilidad sin ningún tipo de problema.**

1. In the Google Cloud console, click the **Navigation menu** (navigation_menu).
2. Select **Compute Engine > VM instances**. The VM instances page opens.

**Entramos en VM instances.**

Gráfico

Descripción generada automáticamente con confianza media

The current VM **cc-app-01** should be listed under VM instances. This is the vulnerable VM that has been compromised and must be shut down.

1. Select the checkbox for the **cc-app-01** VM.
2. Click **Stop**.

**Seleccionamos cc-app-01 y la ponemos en modo stop.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. A pop-up will appear asking you to confirm that the VM should be stopped, click **Stop**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Click **Check my progress** to verify that you have completed this task correctly.

|  |
| --- |
| Shut down the vulnerable VM  Check my progress |

Escala de tiempo

Descripción generada automáticamente

1. In the action bar, click **+ Create instance**.

**Una vez parada la máquina, entramos en Create instance.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. In the **Name** field, type **cc-app-02**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. In the **Machine type** section, expand the drop-down, select **Shared-core**, and then select **e2-medium**.

Texto

Descripción generada automáticamente

1. In the **Boot disk** section, click **Change**. The Boot disk dialog opens.

**En la sección Boot disk, pulsamos Change.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Select the **Snapshots** tab.
2. Expand the **Snapshot** drop-down menu, and select **cc-app01-snapshot**.
3. Click **Select**.

**Dentro del apartado Snapshot, seleccionamos la única snapshot que está hecha de la otra máquina.**

**Y pinchamos en select.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. In the **Identity and API access** section, expand the **Service accounts** drop-down menu, and select **Qwiklabs User Service Account**.

**Indicamos que se utilice la cuenta Qwicklabs User.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Expand the **Advanced options** section.
2. Expand the **Networking** section.

Imagen que contiene Forma

Descripción generada automáticamente

1. In the **Network tags** field, type **cc**. You'll use this tag to apply firewall rules to this specific VM.

**Dentro del apartado Networking, asignamos el tag cc.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. In the **Network interfaces** section, expand the **default** network.
2. Expand the **External IPv4 address** drop-down menu, and select **None**.

**No queremos que tenga IP externa, por lo que marcamos None.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click **Create**.

Interfaz de usuario gráfica

Descripción generada automáticamente

**Ahora la máquina se está creado a raíz de la snapshot de la otra máquina antes de tener malware.**

1. Select the checkbox for the **cc-app-02** VM.
2. Click **Stop**.
3. A pop-up will appear asking you to confirm that the VM should be stopped, click **Stop**.

Paramos la máquina una vez creada.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Wait for the **cc-app-02** VM to be stopped before you continue.

1. In the **VM instances** section, click the **cc-app-02** link. The cc-app-02 page opens.
2. In the **cc-app-02** toolbar, click **Edit.** The Edit cc-app-02 instance page opens.

**Entramos a editar la configuración.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. Scroll down to the **Security and access** section, and under **Shielded VM**, select the checkbox for the **Turn on Secure Boot** option. This will address the **Compute secure boot disabled** finding.

**Activamos el Arranque seguro para mejorar la seguridad.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. Click **Save**.

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente con confianza media

1. In the **Compute Engine** menu, select **VM instances**.
2. Select the checkbox for the **cc-app-02** VM.
3. Click **Start/Resume**.

**Volvemos a iniciar la máquina y ya la tendríamos correctamente configurado a raíz de la snapshot.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. A pop-up will appear asking you to confirm that the VM should be started, click **Start**.

**Comprobación desde la consola de Google Cloud.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

The **cc-app-02** VM instance will restart and the **Secure Boot disabled** finding will be remediated.

Click **Check my progress** to verify that you have completed this task correctly.

|  |
| --- |
| Create a new VM from existing snapshot  Check my progress |

Escala de tiempo

Descripción generada automáticamente

Challenge: Delete the compromised VM

Delete the compromised VM **cc-app-01**.

**Por último, eliminamos la primera máquina para cerrar la brecha de seguridad.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Click **Check my progress** to verify that you have completed this task correctly.

|  |
| --- |
| Delete the compromised VM  Check my progress |

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Task 3. Fix Cloud Storage bucket permissions**

In this task, you'll revoke public access to the storage bucket and switch to uniform bucket-level access control, significantly reducing the risk of data breaches. By removing all user permissions from the storage bucket, you can prevent unauthorized access to the data stored within.

**En el siguiente paso vamos a revocar el acceso público al bucket y cambiaremos el acceso de control a uniforme (es un método de control de acceso en Google Cloud Storage que simplifica la gestión de permisos al eliminar las ACLs) para reducir las brechas de seguridad. Después al eliminar todos los permisos de usuario del bucket, evitaremos el acceso no autorizado.**

1. In the **Navigation menu** (navigation_menu), select **Cloud Storage > Buckets**. The Buckets page opens.

**Entramos en buckets.**

Gráfico

Descripción generada automáticamente con confianza baja

1. Click the **project\_id\_bucket** storage bucket link. The Bucket details page opens.

**Entramos en nuestro project ID.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

You'll note there is a **myfile.csv** file in the publicly accessible bucket. This is the file that contains the sensitive information that was dumped by the malicious actor. Perform the following steps to address the **Public bucket ACL** finding.

1. Click the **Permissions** tab.
2. In the **Public access** tile, click **Prevent public access.**

**Dentro de permisos, revocamos el acceso público que con estos conseguimos eliminar cualquier configuración que permita a usuarios anónimos o no autenticados acceder y leer archivos almacenados en el bucket.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Click **Confirm**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Challenge: Modify storage bucket access

Switch the access control to uniform and remove permissions for the **allUsers** principals from the storage bucket to enforce a single set of permissions for the bucket and its objects. You'll also need to ensure that users who rely on basic project roles to access the bucket won't lose their access.

**Dentro de permisos cambiamos el acceso a uniforme para simplificar la gestión y simplifica la gestión de permisos al eliminar las ACLs con lo que conseguimos reducir los errores.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Y como hemos explicado en el anterior paso, eliminamos el acceso de allUsers.**

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Click **Check my progress** to verify that you have completed this task correctly.

|  |
| --- |
| Modify storage bucket access.  Check my progress |

Escala de tiempo

Descripción generada automáticamente

**Task 4. Limit firewall ports access**

In this task, you'll restrict access to RDP and SSH ports to only authorized source networks to minimize the attack surface and reduce the risk of unauthorized remote access.

Exercise extreme caution before modifying overly permissive firewall rules. The rules may be allowing legitimate traffic, and improperly restricting it could disrupt critical operations. In this lab, ensure the Compute Engine virtual machine instances tagged with target tag "cc" remain accessible via SSH connections from the Google Cloud Identity-Aware Proxy address range (35.235.240.0/20). To maintain uninterrupted management access, create a new, limited-access firewall rule for SSH traffic before removing the existing rule allowing SSH connections from any address.

Challenge: Restrict SSH access

Create a new firewall rule. This rule must restrict SSH access to only authorized IP addresses from the source network **35.235.240.0/20** to compute instances with the target tag **cc**.

**En el siguiente paso crearemos una regla que solo permita conexiones SSH desde el rango d direcciones que nos indican, solamente hacia las instancias que tengan el tag asignado de destino nombrado cc.**

**Entramos en Firewall.**

Imagen que contiene Gráfico

Descripción generada automáticamente

**Creamos una nueva regla:**

Interfaz de usuario gráfica, Aplicación, Word, Sitio web

Descripción generada automáticamente

**Como no nos piden nombre único, la vamos a llamar limit-ports.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Indicamos que solo sea de destino con tag CC.**

Imagen que contiene Aplicación

Descripción generada automáticamente

**Y en el rango de direcciones de origen 35.235.240.0/20.**

Imagen que contiene Aplicación

Descripción generada automáticamente

**En protocolos y puertos permitimos TCP-22, que es el puerto de SSH.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente con confianza media

Interfaz de usuario gráfica, Diagrama, Aplicación

Descripción generada automáticamente

**Comprobación desde la consola de Google Cloud.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Click **Check my progress** to verify that you have completed this task correctly.

|  |
| --- |
| Restrict SSH access  Check my progress |

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

**Task 5. Fix the firewall configuration**

In this task, you'll delete three specific VPC firewall rules that are responsible for allowing unrestricted access to certain network protocols, namely ICMP, RDP, and SSH, from any source within the VPC network. Then, you'll enable logging on the remaining firewall rules.

Challenge: Customize firewall rules

Delete the **default-allow-icmp**, **default-allow-rdp**, and **default-allow-ssh** firewall rules. These rules are overly broad and by deleting them, you'll allow for a more secure and controlled network environment.

Lo que queremos ahora, es eliminar las reglas por defecto de ISCMP, SSH y RDP dado **que nosotros queremos tener un entorno de red más seguro.**

**Entramos en Firewall policies y eliminamos las 3 reglas nombradas anteriormente.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

|  |
| --- |
| Customize firewall rules  Check my progress |

Escala de tiempo

Descripción generada automáticamente con confianza baja

Challenge: Enable logging

Enable logging for the remaining firewall rules **limit-ports** (the rule you created in a previous task) and **default-allow-internal**.

Enabling logging allows you to track and analyze the traffic that is allowed by this rule, which is likely to be internal traffic between instances within your VPC.

**En este último paso, habilitaremos los logs, habiendo borrado anteriormente las reglas por defecto, consiguiendo con esto proteger mejor la red y mejorar la visibilidad de la red.**

**Accedemos a nuestra regla creada del firewall.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Entramos a editarla.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

**Marcamos On en el apartado logs.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Guardamos la configuración realizada.**

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

Click **Check my progress** to verify that you have completed this task correctly.

|  |
| --- |
| Enable logging  Check my progress |

Imagen que contiene Texto

Descripción generada automáticamente

**Task 6. Verify compliance**

After diligently addressing the vulnerabilities identified in the PCI DSS 3.2.1 report, it's crucial to verify the effectiveness of your remediation efforts. In this task, you'll run the report again to ensure that the previously identified vulnerabilities have been successfully mitigated and no longer pose a security risk to the environment.

**Habiendo abordado las vulnerabilidades del estándar PCI DSS 3.2.1, nos disponemos a confirmar la efectividad de nuestras acciones correctivas.**

**Volveremos a ejecutar el informe para asegurarnos de que las brechas ya no presentan un riesgo de seguridad para nuestra infraestructura o entorno.**

1. In the **Security Command Center** menu, click **Compliance**. The Compliance page opens.

**Entramos en compliance.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. In the **Google Cloud compliance standards** section, click **View details** in the **PCI DSS 3.2.1** tile. The PCI DSS 3.2.1 report opens.

**Accedemos al estándar.**

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

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

Volvemos a filtrar de vulnerabilidades activas y podemos comprobar que se ha solucionado correctamente.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Se han solucionado todas las vulnerabilidades principales** ✅**.**

**A pesar de haber tratado las vulnerabilidades de severidad alta y media, los registros de flujo permanecen desactivados para varias subredes. Este hallazgo seguirá apareciendo en el informe después de completar las acciones de corrección, ya que está relacionado con el entorno específico utilizado en el laboratorio.**

**Lo importante es que el problema que nos pedían está abordado.**

**Conclusion**

Great work!

You have helped the security team at Cymbal Bank to mitigate the impact of the data breach, address the identified vulnerabilities, and significantly enhanced the security posture of Cymbal Bank’s Google Cloud environment.

First, you examined and analyzed the vulnerabilities and findings in Google Cloud Security Command Centre.

Next, you shut the old VM down and created a new VM from a snapshot taken before the malware infection.

Then, you fixed the cloud storage permissions by revoking public access to the storage bucket and switching to uniform bucket-level access control. You also removed all user permissions from the storage bucket.

Next, you fixed the firewall rules by deleting the default-allow-icmp, default-allow-rdp, and default-allow-ssh firewall rules, and enabling logging for the remaining firewall rules.

Finally, you run a compliance report to confirm that the vulnerability issues have been remediated.

Remember, as a security analyst it is crucial to maintain regular security audits and implement ongoing monitoring practices for continued protection against evolving threats and vulnerabilities.

**End your lab**

Before you **end the lab**, make sure you’re satisfied that you’ve completed all the tasks. When you're ready, click **End Lab** and then click **Submit**.

Ending the lab will remove your access to the lab environment, and you won’t be able to access the work you've completed in it again.

Copyright 2024 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.