Google Cloud

Explore your course 3 scenario: Cymbal Bank

Learn about the Course 3 lab and activity scenario!

This reading introduces the lab and activity scenarios for Course 3, which focuses on core principles relating identity and access management (IAM), threat management, and automation. Building a strong foundation of cloud security knowledge is crucial for protecting cloud resources, sensitive data, and maintaining compliance with industry regulations and standards.

In this course, you will continue to hone your knowledge and skills as a junior cloud security analyst at Cymbal Bank, a fictitious financial organization. You will leverage your existing expertise and gain new insights as you take on these security challenges in a simulated cloud environment.

Note: Be sure to review the **Lab Technical Tips** reading before you begin working on the lab.

Your role

So far as a junior cloud security analyst at the international retail bank Cymbal Bank, you've helped implement risk management and compliance changes. Now, you'll switch gears and focus on security cloud configuration and deployment of cloud resources to Cymbal Bank's new cloud environment. Before these cloud resources can be accessible to customers, they'll need to be securely provisioned and configured. You'll help support this effort by identifying and fixing any vulnerabilities and misconfigurations in Cymbal Bank's cloud environment.

Your tasks

You'll find this Cymbal Bank scenario in the following Course 3 labs and activities:

- **Create a role in Google Cloud IAM**: In module 1, you'll begin supporting Cymbal Bank in securely configuring and deploying cloud resources by using identity and access

management (IAM). You'll use IAM to provide third-party auditors with secure access to a database.

- **Access a firewall and create rule**: In module 1, you'll continue configuring the secure deployment of cloud resources by testing and updating firewall rules to a demo web server.
- **Identify vulnerabilities and remediation techniques**: Then in module 2, you'll scan one of Cymbal Bank's latest banking applications for vulnerabilities. Then you'll remediate any of the vulnerabilities that you find.
- **Change firewall rules using Terraform and Cloud Shell**: In module 3, you'll need to configure a secure network with firewall rules to host the new banking application on.
- **Analyze the security of a container**: Then in module 3, you'll analyze the configuration of a container to ensure that it's secure before it's deployed to production and accessed by customers.
- **Create symmetric and asymmetric keys**: Finally in module 4, you'll support the secure transfer of data from Cymbal Bank's on-premises servers to the new cloud environment by creating cryptographic keys.

Throughout your exploration of these tasks, you'll expand your knowledge on IAM, perimeter protection, vulnerability management, automation, and data protection. Completing these course labs and activities will help you to better understand how to better identify threats so that you can secure cloud resources and protect sensitive data.

Note: *The story, all names, characters, and incidents portrayed in this project are fictitious. No identification with actual persons (living or deceased) is intended or should be inferred. And, the data shared in this project has been created for pedagogical purposes.*

Deliverables

With the course labs and activities, you will gain valuable practice and apply your new skills as you complete the following:

- Utilize identity and access management (IAM) to create and manage user accounts in a cloud environment
- Analyze firewall rules, test web server connections, and create firewall rules to block connections to unnecessary ports to improve security
- Utilize application vulnerability scanners to identify and mitigate vulnerabilities to ensure application security before deployment
- Utilize infrastructure-as-code (IaC) to provision a VPC network
- Review container configurations and provide recommendations to improve container security
- Create and maintain encryption keys to facilitate the secure transmission of this data

Good luck! Your Cymbal Bank team members are looking forward to collaborating with you to effectively address their cloud security challenges.

Key takeaways

The labs and activities in this course are purposefully built for you to practice and apply the skills you learned in a workplace scenario. Working as a cloud security analyst, you'll be immersed with the core principles of identity and access management (IAM), threat management, and automation. By applying these concepts, you'll build an understanding of how to safeguard cloud resources, sensitive data, and ensure compliance with industry regulations and standards. Completing these hands-on activities will not only provide you with valuable experience, you will also create tangible portfolio examples that you can use to showcase your skills to future employers.

Resources for additional information

Use the following readings to help support you as you work through the lab:

- **Guide to firewall rules reading** available in course 3 module 1
- **Guide to web application security scanning reading** available in course 3 module 2
- **Guide to automating deployment with Terraform reading** available in course 3 module 3