Explore your course 4 scenario: Cymbal Bank

Learn about the course 4 lab and activity scenarios

This reading introduces the lab and activity scenarios for course 4, which focuses on the foundations of incident detection such as incident management, threat hunting, documentation, business continuity, and more. Building a strong foundation of cloud security knowledge is crucial for protecting cloud resources, sensitive data, and maintaining compliance with industry regulations and standards.

This certificate offers you an opportunity to apply your knowledge and skills in cloud security to a scenario where you work as a junior cloud security analyst at Cymbal Bank, a fictitious financial organization.

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

Your role

As a cloud junior cloud security analyst at the international retail bank Cymbal Bank, you've assisted in the roll out of Cymbal Bank's digital transformation strategy. You've worked to ensure that cloud resources meet regulatory compliance and are securely configured and deployed. In your upcoming tasks, you will collaborate closely with other team members to recreate, analyze, and remediate security incidents.

Your tasks

You'll find this Cymbal Bank scenario in the following course 4 labs and activity:

- **Determine the difference between normal activity and an incident**: In this module 1 lab, to put your incident response skills, you'll recreate threat findings relating to two user accounts. You'll then compare the details of these findings to identify normal user activity and suspicious activity.
- **Explore false positives through incident detection**: In this module 2 lab, you'll recreate a false positive alert to understand why the alert was triggered.
- **Analyze audit logs using BigQuery**: In this module 3 lab, you'll set up a test environment to recreate a high severity security incident that was recently remediated by the security team.
- **Document a timeline of events**: In this module 3 activity, you'll first analyze the details of a phishing incident. You'll then use the information from a phishing alert to create a chronological timeline of events leading up to the phishing incident.
- **Recover VMs with Google Backup and DR Service**: In this module 4 lab, you'll assist the Incident Response Team with remediation efforts by restoring a virtual machine (VM) from a known good backup.

With each completed task, you'll gain an in-depth understanding of the processes involved in responding and recovering from a cloud security incident. Completing the course labs and activity will help you acquire the skills necessary to effectively move through the lifecycle of a security incident to identify, document, and mitigate threats.

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.*

Your deliverables

The course 4 labs and activity provide you with the opportunity to gain valuable practice and apply your new skills as you complete the following:

- Analyze alerts and logs to identify the difference between normal activity and a security incident.
- Analyze logs to determine if an event is a false positive.
- Investigate suspicious activity from a service account.
- Construct a chronological timeline of events leading up to a security incident.
- Restore affected VMs from a backup.

Good luck! Your Cymbal Bank colleagues are eager to leverage your expertise in maintaining a secure and compliant cloud environment.

Key takeaways

The course 4 labs and activity are intended for you to practice and apply the skills you've learned in a workplace scenario. Incident response efforts are a concentrated, team effort and understanding how to apply the processes involved in incident response can help limit damage and protect critical systems. Once you complete the labs and activity, you'll have work examples that you can add to your portfolio to showcase your skills to future employers.

Resources for more information

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

- **Guide to event threat detection reading** available in course 4 module 1
- **Guide to false positive analysis reading** available in course 4 module 2
- **Guide to log queries, exports, and analysis reading** available in course 4 module 3
- **Guide to backups and VM recovery reading** available in course 4 module 4