

Activity: Create your final report



Activity Overview

Congratulations on completing the capstone project lab! You've demonstrated your dedication and skills in safeguarding digital systems and protecting valuable information. As you reflect on your accomplishment, remember that the field of cloud cybersecurity is ever-evolving, and continuous learning is crucial for staying ahead of emerging threats.

In this activity, you will create a final incident report that summarizes the details of the data breach from the capstone project that you previously completed.

A final report provides a documented record of the incident, enables communication with stakeholders, ensures compliance with legal obligations, and promotes continuous learning and improvement in how organizations respond to future security incidents. Compiling documentation such as a final report is an essential aspect of cloud security when closing an incident. As a cloud security analyst, you'll create this documentation to communicate your security findings and support investigations.

Be sure to complete this activity before moving on. The next course item will quiz your comprehension, and then you'll be provided with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then, access the supporting materials before moving on to the next course item to take the quiz.

You've helped support the security team at Cymbal Retail by mitigating the impact of a data breach, identifying and remediating the vulnerabilities associated with the incident, and improving the overall security posture of Cymbal Bank's cloud environment.

Now that the security team has successfully contained, eradicated, and recovered from the security incident, it's time for the incident to come to a close. The team has transitioned into

the next phase of the incident response lifecycle: post-incident activity. In this final phase, the team is preparing to host a lessons learned meeting where all of the stakeholders involved will evaluate the incident, assess the response actions, and identify areas for improvement. In order to prepare for this meeting, a final report must be created. A final report provides a comprehensive review of a security incident.

You have been tasked with helping contribute to the final report. Each member of your team has been asked to fill out sections of the final report. The security team manager will then review and finalize the report so that it can be used in the lessons learned meeting, where it will be presented to Cymbal Retail stakeholders. You'll be responsible for completing the following sections of the report: **Executive Summary, Response and remediation, and Recommendations.**

First, you'll access and analyze the major details involved with the data breach incident. Then, you'll organize the incident's details in the relevant sections of the final report template.


Step-By-Step Instructions

Consult the supporting materials to answer the quiz questions in the asset that follows. After you complete the quiz, you can compare your work to the exemplar provided.

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the questions.



 **RIGHT CLICK LINKS TO OPEN IN NEW TAB** 

Link to template: [Final report template](#)

Link to supporting materials: [Data breach details](#)

Step 2: Review the incident details



The **Data breach details** document contains the details about the data breach. Review the document to obtain the following key details you'll use to complete the report:

- The vulnerabilities that contributed to the data breach
- Each remediation action taken to address the identified vulnerabilities

- The actions the malicious actor took to exploit the vulnerabilities

Step 3: Executive summary



Review the **Investigation** section of the template to understand the findings related to the attack. In the **Executive summary** section of the template, write a paragraph (**10–20 sentences**) that provides a high-level summary of the security incident. Be sure to include the key findings and other critical information related to the data breach, such as:

- What happened
- How it happened
- Which specific cloud resources were affected by the incident

Step 4: Response and remediation



In the **Response and remediation** section of the template, refer to the **Containment and eradication measures** and **Recovery measures** subheadings. For each subheading, write **5–10 sentences** in a numbered list format that describe the specific response and remediation actions efforts that you took as part of the incident response. Be specific when describing each action. For example, a recovery action can include the reimaging of an infected virtual machine.

Step 5: Recommendations



In the **Recommendations** section of the template, provide **2–4 suggestions (2–5 sentences each)** for improving either processes and procedures involved in the incident response plan and/or recommendations to implement new security controls to mitigate future risks.

Step 6: Access the quiz and answer questions about the report



Go to the next course item and answer the quiz questions. Then compare your answers to the feedback provided.

Pro Tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response



Be sure to address the following points in your completed activity:

- 10–20 sentences that captures the major details of the data breach in the **Executive summary** section
- 5–10 sentences that details the containment, eradication, and recovery actions that Cymbal Retail took in response to the data breach in the **Response and remediation** section
- 2–4 suggestions (2–5 sentences each) in the **Recommendations** section for improving Cymbal Retail's cloud security either through improved security controls or improved processes and procedures