Congratulations! You passed!

Grade received 100% **To pass** 75% or higher

Go to next item

To pass this practice quiz, you must receive 75%, or 3 out of 4 points, by answering a series of questions. Once you have completed the quiz, review the feedback statements. You can learn more about the graded and practice items in the course overview.

Activity Overview

In this activity, you will review an example of a final report and answer a series of quiz questions.

So far, you've learned about the actions involved in the Post-incident Activity phase of the NIST Incident Response Lifecycle. This includes the development of the **final report**, which is documentation that provides a comprehensive review of an incident. It includes essential details of all events related to the incident and recommendations for future prevention.

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You recently joined the security team as a level-one security operation center (SOC) analyst at a mid-sized retail company. Along with its physical store locations, your company also conducts operations in e-commerce, which account for 80% of its sales.

You are spending your first week of training becoming familiar with the company's security processes and procedures. Recently, the company experienced a major security incident involving a data breach of over one million users. Because this was a recent and major security incident, your team is working to prevent incidents like this from happening again. This breach happened before you began working at the company. You have been asked to review the final report.

To gain an understanding of the incident's life cycle, your goals for your review are as follows:

- Goal 1: Identify exactly what happened.
- Goal 2: Identify when it happened.
- Goal 3: Identify the response actions that the company took.
- Goal 4: Identify future recommendations.

***Note**: Use the incident handler's journal you started in a previous activity to take notes during the activity and keep track of your findings.*

Step-By-Step Instructions

Consult the supporting materials to answer the quiz questions that follow. After you complete the quiz, you can compare your answers to the feedback 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.

To use the supporting materials for this course item, click the link and select "Use Template."

Link to supporting materials: Final report

OR

If you don't have a Google account, you can download the supporting materials directly from the following attachment.

Final report
DOCX File

Step 2: Answer questions about the final report

1. What type of security incident was the organization affected by? **1 / 1 point**

- ○ Malware
- ○ Vishing
- ◉ Data theft
- ○ Phishing

Correct
The organization was affected by a security incident involving data theft.

2. Which section of the report includes an explanation of the root cause of the incident? **1 / 1 point**

- ○ Timeline
- ○ Recommendations
- ◉ Investigation
- ○ Executive summary

Correct
The investigation section of the final report includes an explanation of the root cause of the incident, which was a vulnerability in the e-commerce web application.

3. What did the attacker use to exploit the e-commerce web application vulnerability? **1 / 1 point**

- ○ User error
- ○ Data breach
- ◉ Forced browsing
- ○ Web server logs

Correct
The attacker used forced browsing to exploit the e-commerce web application vulnerability.

4. What recommendations did the organization implement to prevent future recurrences? Select two answers. **1 / 1 point**

- ☑ Implemented routine vulnerability scans

Correct
As part of its recommendations to prevent future recurrences, the organization implemented access control mechanisms and implemented routine vulnerability scans.

- ☑ Implemented access control mechanisms

Correct
As part of its recommendations to prevent future recurrences, the organization implemented access control mechanisms and implemented routine vulnerability scans.

- ☐ Paid the $50,000 payment request
- ☐ Provided identity protection services to the affected customers