← Back **Weekly challenge 1**
Graded Quiz • 50 min

Due Jun 11, 11:59 PM +08

Get started with the course

The incident response lifecycle

Incident response operations

Incident response tools

Review: Introduction to detection and incident response

Video: Wrap-up
47 sec

Reading: Glossary terms from week 1
10 min

Quiz: Weekly challenge 1
10 questions

Congratulations! You passed!

Grade received 87.50% **Latest Submission Grade** 85% **To pass** 80% or higher

Go to next item

Weekly challenge 1

Quiz • 50 min

Review Learning Objectives

Submit your assignment

Due Jun 11, 11:59 PM +08 **Attempts** 3 every 24 hours

Try again

Receive grade

To Pass 80% or higher

Your grade
87.50%

View Feedback
We keep your highest score

Like **Dislike** **Report an issue**

1. Which of the following is an example of a security incident? **1 / 1 point**

○ A company's experiences increased traffic volumes on their website because of a new product release.
○ An authorized user emails a file to a customer.
○ An extreme weather event causes a network outage.
● Multiple unauthorized transfers of sensitive documents to an external system.

✓ **Correct**

2. What is the NIST Incident Response Lifecycle? **1 / 1 point**

○ The process used to document events
○ A system that only includes regulatory standards and guidelines
○ The method of closing an investigation
● A framework that provides a blueprint for effective incident response

✓ **Correct**

3. Which of the following are phases of the NIST Incident Response Lifecycle? Select three answers. **0.75 / 1 point**

☑ Preparation

✓ **Correct**

☑ Protection

☒ **This should not be selected**
Please review the video on incidents.

☑ Containment, Eradication, and Recovery

✓ **Correct**

☑ Detection and Analysis

✓ **Correct**

4. What are some roles included in a computer security incident response team (CSIRT)? Select three answers. **0.75 / 1 point**

☑ Incident coordinator

✓ **Correct**

☑ Incident manager

☒ **This should not be selected**
Please review the video on incident response teams.

☑ Security analyst

✓ **Correct**

☑ Technical lead

✓ **Correct**

5. What are some common elements contained in incident response plans? Select two answers. **0.5 / 1 point**

☑ System information

✓ **Correct**

☑ Simulations

☒ **This should not be selected**
Please review the video about the incident response plan.

☑ Incident response procedures

✓ **Correct**

☑ Financial information

☒ **This should not be selected**
Please review the video about the incident response plan.

6. A cybersecurity analyst receives an alert about a potential security incident. Which type of tool should they use to examine the alert's evidence in greater detail? **1 / 1 point**

○ A documentation tool
○ A detection tool
○ A recovery tool
● An investigative tool

✓ **Correct**

7. Which of the following methods can a security analyst use to create effective documentation? Select two answers. **0.5 / 1 point**

☑ Write documentation in a way that reduces confusion.

✓ **Correct**

☑ Provide clear and concise explanations of concepts and processes.

✓ **Correct**

☑ Write documentation using technical language.

☒ **This should not be selected**
Please review the video on documentation.

☑ Provide documentation in a paper-based format.

☒ **This should not be selected**
Please review the video on documentation.

8. Fill in the blank: An intrusion detection system (IDS) _____ system activity and alerts on possible intrusions. **1 / 1 point**

○ protects
○ analyzes
○ manages
● monitors

✓ **Correct**

9. Which process uses a variety of applications, tools, and workflows to respond to security events? **1 / 1 point**

○ Intrusion prevention system (IPS)
○ Security information and event management (SIEM)
○ Intrusion detection system (IDS)
● Security orchestration, automation, and response (SOAR)

✓ **Correct**

10. A cybersecurity professional is setting up a new security information and event management (SIEM) tool for their organization and begins identifying data sources for log ingestion. Which step of the SIEM does this scenario describe? **1 / 1 point**

● Collect data
○ Analyze data
○ Normalize data
○ Aggregate data

✓ **Correct**