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

English

Due Apr 28, 11:59 PM WIB

Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 80% or higher

Go to next item

1. Which of the following statements describe security incidents and events?

1 / 1 point

○ Security incidents and events are unrelated.

● All security incidents are events, but not all events are security incidents.

○ Security incidents and events are the same.

○ All events are security incidents, but not all security incidents are events.

✓ **Correct**

2. What process is used to provide a blueprint for effective incident response?

1 / 1 point

● The NIST Incident Response Lifecycle

○ The incident handler's journal

○ The NIST Cybersecurity Framework

○ The 5 W's of an incident

✓ **Correct**

3. Which core functions of the NIST Cybersecurity Framework relate to the NIST Incident Response Lifecycle? Select two answers.

1 / 1 point

□ Discover

☑ Respond

✓ **Correct**

☑ Detect

✓ **Correct**

□ Investigate

4. What is a computer security incident response team (CSIRT)?

1 / 1 point

○ A specialized group of security professionals who work in isolation from other departments

● A specialized group of security professionals who are trained in incident management and response

○ A specialized group of security professionals who focus on incident prevention

○ A specialized group of security professionals who are solely dedicated to crisis management

✓ **Correct**

5. What is an incident response plan?

1 / 1 point

○ A document that contains policies, standards, and procedures

○ A document that details system information

● A document that outlines the procedures to take in each step of incident response

○ A document that outlines a security team's contact information

✓ **Correct**

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 statement most accurately describes documentation?

1 / 1 point

○ It is a standardized format used to record information across all industries.

● It can be audio, video, or written instructions used for a specific purpose.

○ It serves as legal documentation and evidence in official settings.

○ It is always digital and stored in a centralized database.

✓ Correct

8. Fill in the blank: An intrusion prevention system (IPS) monitors systems and _____ intrusive activity.

1 / 1 point

○ reports

○ pauses

○ detects

● stops

✓ Correct

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

1 / 1 point

○ Security information and event management (SIEM)

○ Intrusion prevention system (IPS)

○ Intrusion detection system (IDS)

● Security orchestration, automation, and response (SOAR)

✓ Correct

10. Fill in the blank: During the _____ step of the SIEM process, the collected raw data is transformed to create log record consistency.

1 / 1 point

○ data aggregation

○ data analysis

○ data collection

● data normalization

✓ Correct