Congratulations! You passed!

Grade received 90%
Latest Submission Grade 90%
To pass 80% or higher

Weekly challenge 1

Quiz • 50 min

Review Learning Objectives

Retake the assignment in **23h 56m**
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 events are security incidents, but not all security incidents are events.
- Security incidents and events are the same.
- All security incidents are events, but not all events are security incidents.

Correct
To Pass 80% or higher

Your grade 90%
View Feedback
We keep your highest score

Try again
Retake the quiz in **23h 56m**

Submit your assignment
Due Jun 11, 11:59 PM +08 **Attempts** 3 every 24 hours
Receive grade

2. A security team uses the NIST Incident Response Lifecycle to support incident response operations. How should they follow the steps to use an approach most effectively? **0 / 1 point**

- Skip irrelevant steps.
- Complete the steps in any order.
- Overlap the steps as needed.
- Only use each step once.

Incorrect
Please review the video on incidents.

3. Which step does the NIST Incident Response Lifecycle begin with? **1 / 1 point**

- Detection and Analysis
- Preparation
- Containment, Eradication and Recovery
- Post-Incident Activity

Correct

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

- [x] Technical lead

Correct

- [x] Incident coordinator

Correct

- [x] Security analyst

Correct

- [ ] Incident manager

5. What is an incident response plan? **1 / 1 point**

- A document that outlines a security team's contact information
- A document that outlines the procedures to take in each step of incident response
- A document that contains policies, standards, and procedures
- A document that details system 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**

- An investigative tool
- A recovery tool
- A documentation tool
- A detection tool

Correct

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

- [ ] Provide documentation in a paper-based format.
- [ ] Write documentation using technical language.
- [x] Provide clear and concise explanations of concepts and processes.

Correct

- [x] Write documentation in a way that reduces confusion.

Correct

8. Fill in the blank: An intrusion prevention system (IPS) monitors systems and _____ intrusive activity. **1 / 1 point**

- detects
- stops
- reports
- pauses

Correct

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

- Intrusion detection system (IDS)
- Security information and event management (SIEM)
- Intrusion prevention system (IPS)
- 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 collection
- data normalization
- data analysis
- data aggregation

Correct