Congratulations! You passed!

Grade received 100%
Latest Submission Grade 100%
To pass 80% or higher
Go to next item

Weekly challenge 1

Quiz • 50 min

Review Learning Objectives

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

- Security incidents and events are unrelated.
- Security incidents and events are the same.
- All security incidents are events, but not all events are security incidents.
- All events are security incidents, but not all security incidents are events.

Correct

Submit your assignment
Try again
Due Jun 11, 11:59 PM +08
Attempts 3 every 24 hours
Receive grade
To Pass 80% or higher
Your grade 100%
View Feedback
We keep your highest score

Like Dislike Report an issue

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

- A system that only includes regulatory standards and guidelines
- The method of closing an investigation
- The process used to document events
- 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. **1 / 1 point**

- [x] Preparation

Correct

- [x] Containment, Eradication, and Recovery

Correct

- [ ] Protection
- [x] Detection and Analysis

Correct

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

- [x] Security analyst

Correct

- [ ] Incident manager
- [x] Incident coordinator

Correct

- [x] Technical lead

Correct

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

- [ ] Simulations
- [ ] Financial information
- [x] Incident response procedures

Correct

- [x] System information

Correct

6. Which of the following best describes how security analysts use security tools? **1 / 1 point**

- They only use a single tool to monitor, detect, and analyze events.
- They only use documentation tools for incident response tasks.
- They use a combination of different tools for various tasks.
- They only use detection and management tools during incident investigations.

Correct

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

- [x] Provide clear and concise explanations of concepts and processes.

Correct

- [ ] Write documentation using technical language.
- [ ] Provide documentation in a paper-based format.
- [x] Write documentation in a way that reduces confusion.

Correct

8. What is the difference between an intrusion detection system (IDS) and an intrusion prevention system (IPS)? **1 / 1 point**

- An IDS stops intrusive activity whereas an IPS monitors system activity and alerts on intrusive activity.
- An IDS and an IPS both have the same capabilities.
- An IDS monitors system activity and alerts on intrusive activity whereas an IPS stops intrusive activity.
- An IDS automates response and an IPS generates alerts.

Correct

9. What is the difference between a security information and event management (SIEM) tool and a security orchestration, automation, and response (SOAR) tool? **1 / 1 point**

- SIEM tools and SOAR tools have the same capabilities.
- SIEM tools use automation to respond to security incidents. SOAR tools collect and analyze log data, which are then reviewed by security analysts.
- SIEM tools collect and analyze log data, which are then reviewed by security analysts. SOAR tools use automation to respond to security incidents.
- SIEM tools are used for case management while SOAR tools collect, analyze, and report on log data.

Correct

10. What happens during the data collection and aggregation step of the SIEM process? Select two answers. **1 / 1 point**

- [ ] Data is cleaned and transformed.
- [x] Data is collected from different sources.

Correct

- [x] Data is centralized in one place.

Correct

- [ ] Data is analyzed according to rules.