Weekly challenge 1

Quiz • 50 min

Congratulations! You passed!

Grade received 87.50%
Latest Submission grade 87.50%
To pass 80% or higher

Go to next item

Review Learning Objectives

Submit your assignment
Try again
Due Jun 11, 11:59 PM +08
Attempts 3 every 24 hours

Receive grade
Your grade 87.50%
To Pass 80% or higher
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 experiences increased traffic volumes on their website because of a new product release.
- Multiple unauthorized transfers of sensitive documents to an external system.
- An authorized user emails a file to a customer.
- An extreme weather event causes a network outage.

Correct

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

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

Correct

3. Which core functions of the NIST Cybersecurity Framework relate to the NIST Incident Response Lifecycle? Select two answers. **0.5 / 1 point**

- [x] Discover

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

- [x] Investigate

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

- [x] Respond

Correct

- [x] Detect

Correct

4. Fill in the blank: A specialized group of security professionals who are trained in incident management and response is a _____. **1 / 1 point**

- risk assessment group
- forensic investigation team
- threat hunter group
- computer security incident response team

Correct

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

- 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 outlines a security team's contact information
- 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**

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

Correct

7. What are the qualities of effective documentation? Select three answers. **0.75 / 1 point**

- [x] Consistent

Correct

- [x] Brief

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

- [x] Accurate

Correct

- [x] Clear

Correct

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

- protects
- analyzes
- monitors
- manages

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 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.
- 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 and SOAR tools have the same capabilities.

Correct

10. What happens during the data collection and aggregation step of the SIEM process? Select two answers. **0.5 / 1 point**

- [x] Data is cleaned and transformed.

This should not be selected
Please review the video on SIEM and SOAR.

- [x] Data is analyzed according to rules.

This should not be selected
Please review the video on SIEM and SOAR.

- [x] Data is centralized in one place.

Correct

- [x] Data is collected from different sources.

Correct