

1.

Which step of the NIST Incident Response Lifecycle involves the investigation and validation of alerts?

1 / 1 point

☐

Discovery

☐

Detection

☐

Recovery

☒

Analysis

☒

Correct

2.

In incident response, documentation provides an established set of guidelines that members of an organization can follow to complete a task. What documentation benefit does this provide?

1 / 1 point

☐

Integrity

☐

Reliability

☒

Standardization

☐

Transparency

☒

Correct

3.

An organization is working on implementing a new security tool, and a security analyst has been tasked with developing workflow documentation that outlines the process for using the tool. Which documentation benefit does this scenario outline?

1 / 1 point

☐

Quality

☒

Standardization

☐

Clarity

☐

Transparency

☒

Correct

4.

Chain of custody documents establish proof of which of the following? Select two answers.

1 / 1 point

☐

Quality

☒

Reliability

☒

Correct

☒

Integrity

☒

Correct

☐

Validation

5.

An analyst is responding to a distributed denial of service attack (DDoS). They take several manual steps outlined in the organization’s DDoS playbook. Which type of playbook did they use to respond to the incident?

0 / 1 point

☐

SOAR

☒

Semi-automated

☐


Non-automated

☐

Automated

☒

Incorrect

Please review [the video on playbooks](#) .

6.

A security analyst gets an alert involving a phishing attempt. Which step of the triage process does this scenario outline?

1 / 1 point

☐

Add context

☒

Receive and assess

☐

Assign priority

☐

Collect and analyze

☒

Correct

7. After a security incident involving an exploited vulnerability due to outdated software, a security analyst applies patch updates. Which of the following steps does this task relate to?

1 / 1 point

- ☐ Response
- ☒ Eradication
- ☐ Reimaging
- ☐ Prevention

✔ Correct

8. Which step of the NIST Incident Response Lifecycle involves returning affected systems back to normal operations?

1 / 1 point

- ☒ Recovery
- ☐ Containment
- ☐ Response
- ☐ Eradication

✔ Correct

9. What questions can be asked during a lessons learned meeting? Select three answers.

1 / 1 point

- ☒ What could have been done differently?

✔ Correct

- ☒ What were the actions taken for recovery?

✔ Correct

- ☐ Which employee is to blame?

- ☒ What time did the incident happen?

✔ Correct

10. What does a final report contain? Select three.

0.5 / 1 point

- ☒ Incident details

✔ Correct

- ☒ Timeline

✔ Correct

- ☒ Updates

✘ This should not be selected  
Please review [the video on post-incident activity](#).

- ☐ Recommendations