Question 1
Which step of the NIST Incident Response Lifecycle involves the investigation and validation of alerts? 1 / 1 point
Analysis
Detection
Recovery
Discovery
Correct

Question 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
Standardization
Transparency
Reliability
Correct

Question 3
After a ransomware incident, an organization discovers their ransomware playbook needs improvements. A security analyst is tasked with changing the playbook documentation. Which documentation best practice does this scenario highlight? 1 / 1 point
Be accurate
Know your audience
Update regularly
Be concise
Correct

Question 4
Fill in the blank: Inconsistencies in the collection and logging of evidence cause a _____ chain of custody. 1 / 1 point
secure
broken
forensic
missing
Correct

Question 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? 1 / 1 point
Non-automated
Semi-automated
SOAR
Automated
Correct

Question 6
What are the steps of the triage process in the correct order? 1 / 1 point
Receive and assess, assign priority, collect and analyze
Assign priority, receive and assess, collect and analyze
Receive and assess, collect and analyze, assign priority
Collect and analyze, assign priority, receive and assess
Correct

Question 7
Fill in the blank: Containment is the act of limiting and _____ additional damage caused by an incident. 1 / 1 point
eradicating
detecting
removing
preventing
Correct

Question 8
Fill in the blank: Eradication is the complete _____ of all the incident elements from affected systems. 1 / 1 point
disconnection
isolation
prevention
removal
Correct

Question 9
Fill in the blank: A lessons learned meeting should be held within ____ weeks of an incident. 1 / 1 point
two
three
four
five
Correct

Question 10
What does a final report contain? Select three. 1 / 1 point
Incident details
Correct
Recommendations
Correct
Updates
Timeline
Correct