Question 1
Which section of a final report contains a high-level overview of the security incident? 1 / 1 point
Timeline
Agenda
Recommendations
Executive summary
Correct
The executive summary section of a final report contains a high-level overview of the security incident.

Question 2
What are the goals of a lessons learned meeting? Select two answers. 1 / 1 point
Identify areas of improvement
Correct
The goals of lessons learned meetings are for security teams to review and reflect on a security incident, and identify areas of improvement.
Identify an employee to blame
Review and reflect on a security incident
Correct
The goals of lessons learned meetings are for security teams to review and reflect on a security incident, and identify areas of improvement.
Develop a final report

Question 3
Fill in the blank: In the NIST Incident Response Lifecycle, reviewing an incident to identify areas for improvement during incident handling is known as the _____. 1 / 1 point
Containment, Eradication and Recovery phase
Detection and Analysis phase
Preparation phase
Post-incident activity phase
Correct
In the NIST Incident Response Lifecycle, reviewing an incident to identify areas for improvement during incident handling is known as the Post-incident activity phase.

Question 4
An organization has recovered from a ransomware attack that resulted in a significant disruption to their business operations. To review the incident, the security team hosts a lessons learned meeting. The team realizes that they could have restored the affected systems more quickly if they had a backup and recovery plan in place. Which question would have most likely helped the security team come to this conclusion? 1 / 1 point
Who discovered the incident?
What could have been done differently?
How was the incident detected?
When did the incident happen?
Correct
By asking what could have been done differently, the security team can identify areas of weakness in their incident response process, such as the lack of a backup and recovery plan.