Question 1
A security analyst in a security operations center (SOC) receives an alert. The alert ticket describes the detection of the download of a possible malware file on an employee's computer. Which step of the triage process does this scenario describe? 1 / 1 point
Receive and assess
Assign priority
Add context
Collect and analyze
Correct
This scenario describes receive and assess, the first step of the triage process. In this step, the security analyst receives an alert and determines whether the alert is valid.

Question 2
What is triage? 1 / 1 point

The process of returning affected systems back to normal operations
The prioritizing of incidents according to their level of importance or urgency
The ability to prepare for, respond to, and recover from disruptions
A document that outlines the procedures to sustain business operations during and after a significant disruption
Correct
Triage is the prioritizing of incidents according to their level of importance or urgency.

Question 3
Fill in the blank: _____ is the act of limiting and preventing additional damage caused by an incident. 1 / 1 point

Recovery
Containment
Eradication
Resilience
Correct
Containment is the act of limiting and preventing additional damage caused by an incident.

Question 4
Which examples describe actions related to the eradication of an incident? Select two answers. 1 / 1 point
Complete a vulnerability scan
Correct
Completing a vulnerability scan and applying patches are examples of eradication actions.
Develop a business continuity plan
Apply a patch
Correct
Completing a vulnerability scan and applying patches are examples of eradication actions.
Investigate logs to verify the incident