Question 1
Fill in the blank: Security teams can use _____ to examine network logs and identify events of interest. 1 / 1 point
port filtering
security information and event management (SIEM) tools
baseline configuration
network segmentation
Correct
Security teams can use security information and event management (SIEM) tools to examine network logs and identify events of interest. SIEM tools collect and analyze log data to monitor critical activities in an organization.

Question 2
What is a basic principle of port filtering? 1 / 1 point

Allow users access to only areas of the network that are required for their role.
Allow ports that are used by normal network operations.
Block all ports in a network.
Disallow ports that are used by normal network operations.
Correct
A basic principle of port filtering is to allow ports that are used by normal network operations. Any port that is not being used by the normal network operations should be disallowed to protect against vulnerabilities.

Question 3
A security professional creates different subnets for the various departments in their business, ensuring users have access that is appropriate for their particular roles. What does this scenario describe? 1 / 1 point
Patch updates
Network log analysis
Network segmentation
Firewall maintenance
Correct
This scenario describes network segmentation, which involves creating isolated subnets for different departments in an organization.

Question 4
Data in restricted zones should have the same encryption standards as data in other zones. 1 / 1 point

True
False
Correct
Restricted zones on a network, which contain highly classified or confidential data, should have much higher encryption standards than data in other zones to make them more difficult to access.