Question 1
Do detection tools have limitations in their detection capabilities? 1 / 1 point
Yes
No
Correct
Detection tools have limitations in their detection capabilities. Detection tools are an important part of incident detection and response, but they cannot detect everything. Additional methods of detection can be used to improve coverage and accuracy.

Question 2
Why do security analysts refine alert rules? Select two answers. 1 / 1 point
To reduce false positive alerts
Correct
Security analysts refine alert rules to improve the accuracy of detection technologies and reduce false positive alerts. Rules are adjusted to match the activity intended to be detected.
To increase alert volumes
To create threat intelligence
To improve the accuracy of detection technologies
Correct
Security analysts refine alert rules to improve the accuracy of detection technologies and reduce false positive alerts. Rules are adjusted to match the activity intended to be detected.

Question 3
Fill in the blank: _____ involves the investigation and validation of alerts. 1 / 1 point
Analysis
Honeypot
Threat hunting
Detection
Correct
Analysis involves the investigation and validation of alerts.

Question 4
What are some causes of high alert volumes? Select two answers. 1 / 1 point
Misconfigured alert settings
Correct
Misconfigured alert settings and broad detection rules are some causes of high alert volumes.
Sophisticated evasion techniques
Refined detection rules
Broad detection rules
Correct
Misconfigured alert settings and broad detection rules are some causes of high alert volumes.