

◊ EASY (Q1–Q10)

Q1. A log is best defined as:

- A. Backup of a system
- B. Record of events generated by systems or applications
- C. Network packet stream
- D. Encrypted database

Q2. Which log type records authentication and authorization events?

- A. Application log
- B. System log
- C. Security log
- D. Debug log

Q3. SIEM stands for:

- A. Secure Internet Event Model
- B. Security Information and Event Management
- C. System Integrity Event Monitor
- D. Secure Infrastructure Event Module

Q4. Which protocol is most commonly used for log forwarding?

- A. FTP
- B. SMTP
- C. Syslog
- D. SNMP

Q5. What is the primary function of a log analyzer?

- A. Block attacks
- B. Analyze and interpret log data
- C. Encrypt logs
- D. Capture packets

Q6. Which port is traditionally used by Syslog over UDP?

- A. 21
- B. 22
- C. 443
- D. 514

Q7. Which SIEM component displays dashboards and reports?

- A. Correlation engine
- B. Storage layer
- C. Visualization layer
- D. Log collector

Q8. BASE is commonly used with which IDS?

- A. OSSEC

- B. Zeek
- C. Snort
- D. Suricata

Q9. Which log field indicates when an event occurred?

- A. Event ID
- B. Timestamp
- C. Severity
- D. Hostname

Q10. Centralized logging primarily helps in:

- A. Faster routing
 - B. Event correlation and investigation
 - C. Reducing bandwidth
 - D. Packet encryption
-

❖ MEDIUM (Q11–Q25)

Q11. Why is log normalization required in SIEM?

- A. Reduce log size
- B. Convert logs into a common format
- C. Encrypt logs
- D. Improve packet capture

Q12. Which SIEM component performs pattern matching across events?

- A. Log forwarder
- B. Correlation engine
- C. Storage node
- D. Agent

Q13. Which log source is most useful for detecting brute-force attacks?

- A. Web access logs
- B. Authentication logs
- C. DNS logs
- D. Proxy logs

Q14. Why is time synchronization (NTP) critical for SIEM?

- A. Reduce CPU usage
- B. Ensure accurate event correlation
- C. Encrypt timestamps
- D. Prevent log deletion

Q15. Which Syslog transport provides reliability?

- A. UDP

- B. ICMP
- C. TCP
- D. ARP

Q16. Which SIEM feature reduces false positives?

- A. Raw log storage
- B. Correlation rules
- C. Packet sniffing
- D. Encryption

Q17. In Snort + Syslog architecture, Snort primarily acts as:

- A. Log storage
- B. Alert generator
- C. Correlation engine
- D. Visualization tool

Q18. Which log management phase defines how long logs are stored?

- A. Collection
- B. Normalization
- C. Retention
- D. Correlation

Q19. What is event correlation?

- A. Encrypting multiple logs
- B. Linking related events to detect attacks
- C. Compressing log files
- D. Removing duplicate logs

Q20. Which event pattern indicates possible brute-force activity?

- A. Single login failure
- B. Multiple failed logins in short time
- C. System reboot
- D. Log rotation

Q21. Why agent-based log forwarding is preferred in enterprises?

- A. Lower cost
- B. Reliable delivery and buffering
- C. No configuration needed
- D. Faster packet routing

Q22. Which SIEM layer stores indexed logs?

- A. Collection layer
- B. Correlation layer
- C. Storage/indexing layer
- D. Visualization layer

Q23. Which security risk arises from unsecured log forwarding?

- A. Increased latency
- B. Log tampering or injection
- C. Packet duplication
- D. Larger log size

Q24. BASE mainly provides:

- A. Packet capture
- B. Alert visualization and querying
- C. Log encryption
- D. IPS blocking

Q25. Which event severity usually requires immediate SOC response?

- A. Informational
 - B. Low
 - C. Medium
 - D. Critical
-

△ HARD (Q26–Q40)

Q26. Which correlation rule best detects lateral movement?

- A. Single firewall deny
- B. Login from new host followed by privilege escalation
- C. One failed login
- D. DNS query

Q27. Why SIEM correlation is more effective than single-log analysis?

- A. Encrypts data
- B. Identifies multi-stage attack patterns
- C. Reduces storage
- D. Replaces IDS

Q28. Which SIEM action is triggered after correlation rule match?

- A. Log normalization
- B. Automated alert or response
- C. Log archival
- D. Dashboard refresh

Q29. Which scenario is a false positive?

- A. Confirmed malware execution
- B. Legitimate admin login flagged as attack
- C. SQL injection detected
- D. DDoS traffic identified

Q30. Why Syslog is commonly integrated with SIEM?

- A. Performs correlation
- B. Centralizes log transport
- C. Encrypts logs at rest
- D. Replaces agents

Q31. Which correlation technique uses time-based conditions?

- A. Static correlation
- B. Temporal correlation
- C. Spatial correlation
- D. Signature matching

Q32. Why log integrity is critical in forensics?

- A. Reduce log size
- B. Ensure evidence admissibility
- C. Improve alerting
- D. Faster searching

Q33. Which log source is most valuable for insider-threat detection?

- A. DNS logs
- B. Authentication & authorization logs
- C. Proxy logs
- D. Printer logs

Q34. Which Syslog limitation affects reliability?

- A. Large packet size
- B. Lack of encryption
- C. Unreliable delivery over UDP
- D. High latency

Q35. How does BASE support SOC analysts?

- A. Blocks traffic
- B. Provides web-based IDS alert analysis
- C. Performs packet sniffing
- D. Correlates multi-vendor logs

Q36. Which correlation rule best detects compromised host behavior?

- A. Normal browsing
- B. Malware alert followed by outbound C2 traffic
- C. Successful login
- D. System backup

Q37. Why SIEM cannot fully replace human analysts?

- A. No storage
- B. No alerts

- C. Requires contextual judgment
- D. No dashboards

Q38. Which SIEM challenge increases operational cost?

- A. Centralization
- B. False positives
- C. Log normalization
- D. Indexing

Q39. Which architecture best supports enterprise log analysis?

- A. Standalone log analyzer
- B. Syslog server only
- C. SIEM with correlation and centralized logging
- D. Firewall logs only

Q40. Which integration provides maximum security visibility?

- A. Firewall only
- B. IDS only
- C. IDS + SIEM + log correlation
- D. Antivirus only