SOC Analyst Interview Questions

SOC Analyst Interview Questions

Q1. What is a Security Operations Center (SOC)?

A Security Operations Center (SOC) is a centralized facility where security professionals continuously monitor, detect, analyze, and respond to cybersecurity incidents. The SOC’s goal is to protect an organization by identifying threats and neutralizing them before harm occurs.

Q2. What are the main functions of a SOC?

1. Monitoring – Continuous surveillance of network traffic and systems.

2. Detection – Identifying anomalies and suspicious behavior.

3. Analysis – Investigating alerts and correlating data.

4. Response – Containment and remediation.

5. Prevention – Proactive defense strategies.

Q3. What is the difference between SOC and NOC?

• SOC: Focused on cybersecurity threats and incident response.

• NOC: Focused on network performance, uptime, and connectivity.

Q4. What are SOC tiers?

• Tier 1 – Alert monitoring and triage.

• Tier 2 – Advanced investigation and incident response.

• Tier 3 – Threat hunting, forensics, advanced correlation.

Q5. What tools are commonly used in a SOC?

• SIEM – Log aggregation, alerts, correlation.

• EDR – Endpoint detection and response.

• IDS/IPS – Intrusion detection/prevention.

• Firewalls & Proxy logs.

• SOAR – Automated playbooks and workflows.

Q6. What is a SIEM, and why is it important?

A SIEM aggregates logs, correlates events, and alerts on suspicious activity.

Benefits:

• Centralized logging

• Real-time alerting

• Compliance reporting

• Threat correlation

Q7. What is log analysis?

Reviewing and interpreting system and application logs to identify anomalies, unauthorized access, or malicious activity.

Q8. What is an alert in SOC?

A system-generated notification from SIEM/IDS indicating possible malicious behavior.

Q9. What is alert fatigue?

Analysts receive too many alerts—often false positives—leading to burnout or missed threats.

Q10. What is incident triage?

Steps:

1. Review alert details

2. Validate authenticity

3. Determine severity

4. Escalate if needed

Q11. What are Indicators of Compromise (IOCs)?

Examples:

- Malicious IPs/domains
- File hashes
- Suspicious email addresses
- Registry changes
- Unusual login patterns

Q12. Difference between event, alert, incident:

- Event – Any observable occurrence.
- Alert – Notification triggered by suspicious activity.
- Incident – Confirmed security breach.

Q13. What is threat intelligence?

Collection and analysis of threat data—used for anticipating and detecting attacks.

Q14. Difference between proactive and reactive SOC:

- Reactive: Responds after attacks.
- Proactive: Hunting, vulnerability management, continual improvement.

Q15. What is a SOC playbook?

A documented procedure for handling a specific incident type (e.g., phishing).

Q16. What is threat hunting?

Proactively searching for threats that evade detection systems.

Q17. False positive vs false negative:

- False positive – Benign activity flagged as malicious.
- False negative – Threat missed entirely.

Q18. What is escalation?

Tier 1 forwards complex cases to higher tiers.

Q19. What is an Incident Response Plan (IRP)?

Steps for detecting, analyzing, containing, eradicating, and recovering from incidents.

Q20. What is containment?

Actions to limit threat spread:

- Isolate hosts
- Block IPs/domains
- Disable accounts

Q21. What is eradication?

Removing malware, attacker footholds, and vulnerabilities.

Q22. What is recovery?

Returning systems to normal operation.

Q23. Why is documentation important?

- Compliance

- Knowledge sharing
- Post-incident analysis
- Continuous improvement

Q24. What is correlation in SIEM?

Linking related events to detect meaningful attack patterns.

Q25. What is a baseline?

Defines normal behavior; deviations trigger alerts.

Q26. Common types of security incidents:

1. Phishing
2. Malware
3. Data exfiltration
4. Insider threats
5. DDoS
6. Unauthorized access
7. Web application attacks

Q27. What is vulnerability management?

Identifying, prioritizing, and remediating vulnerabilities.

Q28. SOC KPIs:

- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- False positive rate
- Incident closure rate

Q29. Role of Tier 1 SOC analyst:

- Monitor alerts
- Triage alerts
- Identify false positives
- Escalate real threats
- Document findings

Q30. Soft skills for SOC analysts:

- Critical thinking
- Attention to detail
- Communication
- Stress management
- Team collaboration

Q31. Role of SIEM in threat detection:

- Central monitoring
- Correlation
- Visualization dashboards
- Forensics via historical analysis

Q32. How does log correlation work?

Example:

Event 1: Multiple failed logins

Event 2: Successful login

Event 3: Privilege escalation

→ Possible brute-force attack

Q33. What are correlation rules?

Logic-based triggers (threshold, behavior, pattern).

Q34. Custom use cases:

Example: Data exfiltration detection.

Q35. What is threat modeling?

Identifying threats, targets, and attack paths using frameworks like MITRE ATT&CK; or STRIDE.

Q36. What is MITRE ATT&CK;?

A knowledge base of adversary behaviors. Enables:

- Mapping detection rules
- Identifying visibility gaps
- Building playbooks

Q37. What is the Cyber Kill Chain?

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objectives

Q38. Detection vs prevention:

- Detection: Identify threats.

- Prevention: Block threats.

Q39. Common SIEM log sources:

- Firewalls
- Endpoints
- Servers
- Applications
- Cloud services

Q40. What is normalization?

Standardizing different log formats into a common schema.

Q41. What is parsing?

Extracting meaningful fields (IPs, usernames, timestamps).

Q42. What is enrichment?

Adding contextual data:

- Geolocation
- User identity
- Threat intelligence
- IOC mapping

Q43. Real-time vs historical analysis:

- Real-time – Immediate detection
- Historical – Root-cause, deeper analysis

Q44. What is a SIEM dashboard?

Visualizations of:

- Login trends
- Attack sources
- Severity metrics

Q45. Examples of SIEM queries:

- Detect failed logins
- Users logging in from two countries within one hour

Q46. Challenges in SIEM:

- High false positives
- Poor log integration
- Lack of expertise
- Performance issues
- Ineffective rules

Q47. Baseline anomaly detection:

Alerts on deviations from normal behavior.

Q48. Importance of asset inventory:

- Correct correlation
- Prioritization
- Identifying rogue devices

Q49. IDS vs IPS:

- IDS – Detects
- IPS – Blocks

Q50. Network-based detections:

- DNS anomalies
- Data transfers to unknown IPs
- Suspicious HTTP traffic

Q51. What is endpoint telemetry?

Device-level data for behavior analysis.

Q52. IOC vs IOA:

- IOC – Evidence of breach
- IOA – Signs of attack in progress

Q53. False positive rate:

Percentage of alerts that are benign; lower is better.

Q54. Severity levels:

- Low
- Medium
- High

Q55. Event correlation window:

Time range events must occur within to trigger rules.

Q56. Use case library:

Central repository of detection logic.

Q57. Threat intelligence correlation:

Matching internal events to external threat intel.

Q58. TTPs:

Tactics, Techniques, Procedures describing adversary behavior.

Q59. Behavioral analytics:

UEBA tools detect abnormal behavior patterns.

Q60. Lateral movement detection:

- SMB anomalies
- Pass-the-hash
- Remote PowerShell

Q61. Privilege escalation detection:

Indicators:

- Admin rights granted
- sudo/runas usage
- Token manipulation

Q62. Exfiltration detection:

Monitoring for unauthorized outbound transfers.

Q63. Common alert investigation steps:

1. Validate alert

2. Check logs

3. Enrich with intel

4. Document and escalate

Q64. What is SOAR?

Automation of repetitive response tasks.

Q65. How does automation help?

Reduces workload, improves accuracy.

Q66. Case management systems:

Examples:

- TheHive
- ServiceNow
- IBM Resilient

Q67. Importance of shift handover:

Ensures continuity and prevents incident mishandling.

Q68. SOC performance metrics:

- MTTD
- MTTR
- False positive ratio
- Closure rate

Q69. Playbook automation:

Automated steps for handling attacks.

Q70. Escalation matrix:

Defines who to contact during incidents.

Q71. Incident Response lifecycle:

1. Preparation

2. Identification

3. Containment

4. Eradication

5. Recovery

6. Lessons learned

Q72. Difference between containment, eradication, recovery:

- Containment – Stop spread
- Eradication – Remove threat
- Recovery – Restore systems

Q73. Root cause analysis:

Determining why an incident happened.

Q74. Role of Tier 3 analysts:

- Deep forensics
- Reverse engineering
- Attack vector correlation
- Strategy advising

Q75. Volatile vs non-volatile data:

- RAM (volatile)
- Logs/files (non-volatile)

Q76. Forensics tools:

- Volatility, Autopsy
- FTK, EnCase
- Wireshark, NetworkMiner
- MFT/Registry tools

Q77. Memory forensics:

Detects in-memory attacks like fileless malware.

Q78. Packet analysis:

Inspection of network traffic.

Q79. IOC enrichment:

Checking IOCs against:

- WHOIS
- Threat feeds
- VirusTotal
- AbuseIPDB

Q80. Threat hunting vs IR:

- Hunting – Proactive
- IR – Reactive

Q81. Threat hunting steps:

1. Form hypothesis

2. Collect data

3. Analyze

4. Validate findings

5. Create new detection rules

Q82. Hypothesis-driven vs data-driven hunting:

- Hypothesis — Based on intel
- Data-driven — Pattern discovery

Q83. Data sources for threat hunting:

- Endpoint telemetry
- DNS logs
- Proxy logs
- Firewall logs
- Authentication logs