50 Frequently Asked Inquiry Questions in Cybersecurity

Core SOC & SIEM Operations

1. What is the role of a SOC Analyst? A SOC Analyst monitors, analyzes, and responds to cybersecurity incidents using SIEMs, EDR, threat intel, and SOPs. Their role varies from alert triage (L1) to deep investigations and threat hunting (L2/L3).

2. What are false positives and how do you reduce them? False positives are benign activities wrongly flagged as threats. They are reduced by fine-tuning correlation rules, creating baselines, using threat intelligence, and implementing risk-based alerting.

3. Explain the alert triage process. It involves verifying alert context, checking related logs (source IP, destination, port, process), validating IOC hits, cross-verifying with EDR/SOAR, and escalating or closing with proper documentation.

4. What is a use case in SIEM? A use case is a specific detection logic to identify threats or anomalies. For example: Multiple failed logins followed by a successful login from a new location.

5. How do you onboard a new log source into QRadar? Identify log format, install DSM (if needed), configure protocol (Syslog/API), validate log ingestion via Log Activity, and categorize events into QIDs for parsing.

6. What are QIDs and AQL in QRadar? QIDs (QRadar ID) are standardized identifiers for normalized events. AQL (Ariel Query Language) is used to search and filter logs in QRadars Ariel database.

7. How do you perform threat hunting in SIEM? Using MITRE ATT&CK framework, search for TTPs like suspicious PowerShell commands, credential dumping, unusual parent-child process relations, and DNS exfiltration patterns.

8. What is rule tuning in SIEM? Adjusting detection rules to reduce false positives and improve detection fidelity by refining filters, thresholds, and incorporating threat intel.

9. How do you deal with alert fatigue? Prioritize alerts via severity, confidence score, threat context, and automate responses using SOAR. Regular tuning and suppression rules also help.

10. Explain the difference between correlation and aggregation in SIEM. Correlation detects patterns across events; aggregation groups similar events to reduce noise and improve alert clarity.

50 Frequently Asked Inquiry Questions in Cybersecurity

Incident Response & Real-Time Analysis

11. Walk through your malware incident response process. Identify IOC/process hash, isolate host via EDR, gather memory and disk artifacts, check network activity, eliminate persistence mechanisms, and restore via clean backup.

12. How do you respond to a ransomware alert? Quarantine affected system, disconnect network, check for lateral movement, collect encryption note/hash, notify stakeholders, block C2 domains, and start recovery.

13. What is the difference between an event and an incident? An event is any observable occurrence. An incident is a confirmed or suspected breach or threat needing a response.

14. What is MITRE ATT&CK and how do you use it? Its a knowledge base of adversary tactics and techniques. Its used to map detections, enrich threat hunts, and design defensive coverage.

15. What is lateral movement? Its when an attacker moves within a network post-initial access to expand control or escalate privileges. Tools like BloodHound help in detection.

EDR / CrowdStrike / Defender

16. What is the difference between AV and EDR? AV blocks known threats using signatures. EDR monitors behavior, records endpoint activity, and responds to suspicious actions in real time.

17. What is CrowdStrike Falcon used for? It's an EDR platform that provides real-time endpoint monitoring, IOC detection, isolation, threat intelligence, and incident response tools.

18. How do you isolate a machine in Defender/CrowdStrike? Use the isolate device feature from the console to cut network communication except to the EDR cloud console.

19. How does CrowdStrike detect fileless malware? Via behavioral analysisdetecting suspicious scripts, PowerShell, WMI usage, or LOLBins, even when no file is written to disk.

20. Compare Microsoft Defender with CrowdStrike. Defender is native to Windows, integrates with the MS ecosystem, and offers basic EDR. CrowdStrike offers deeper telemetry, superior threat intel, and wider OS support.

SOAR, Automation, and Playbooks

21. What is a SOAR platform? SOAR (Security Orchestration, Automation, and Response) helps automate repetitive SOC tasks, integrate tools, and streamline incident response workflows.

22. Give an example of a SOAR playbook. Phishing playbook: Ingest email Extract IOCs Check VT/ThreatIntel Block URLs/IPs Auto-reply to user Close ticket.

23. How do you design a good playbook? Identify repeatable tasks, define decision points, minimize false positives, log every step, and ensure easy rollback or manual override.

24. How does SOAR help reduce MTTR? By automating investigation, enrichment, and containment steps, SOAR drastically reduces Mean Time to Respond (MTTR).

25. What are some common SOAR tools? Palo Alto Cortex XSOAR, Splunk SOAR, IBM Resilient, Microsoft Sentinel Playbooks (Logic Apps).

Vulnerability Management & GRC

50 Frequently Asked Inquiry Questions in Cybersecurity

26. What is the vulnerability lifecycle? Discover Prioritize (CVSS, exploitability) Remediate (patch/workaround) Validate Report.

27. How do you prioritize vulnerabilities? Use CVSS, exploit availability, asset criticality, exposure level, and threat intelligence.

28. What tools are used in VM? Nessus, Qualys, Rapid7 InsightVM, Microsoft Defender for Endpoint (TVM module).

29. What is a gap assessment? Identifying differences between current security posture and required compliance/security framework (e.g., ISO 27001, NIST).

30. How do you close a VM audit finding? Implement fix Re-scan and verify Document evidence (screenshots, logs) Submit to auditor.

Network Security, Port Attacks & Protocols

31. What are some critical port-based attacks? Port 3389 (RDP brute-force), Port 445 (SMB exploits like EternalBlue), Port 53 (DNS tunneling), Port 80/443 (web app attacks)

32. How do you detect port scanning? SIEM rules for multiple destination ports from a single source IP in short time. Tools: Zeek, Snort, Suricata.

33. What is DNS tunneling? Exfiltrating data over DNS queries. Detect via unusually long domain names, high query volume to unknown domains.

34. What is a pivot attack? After compromise, attacker uses one host to move into other internal systems (via RDP, SMB, WinRM, etc.).

35. How do you defend against brute-force login attempts? Implement account lockout policies, MFA, SIEM alerts for login anomalies, and GeoIP blocking.

Reporting, KPIs, Metrics

36. What KPIs do you track in SOC? MTTD, MTTR, Incident closure rate, False positive ratio, Use case effectiveness, Analyst response SLA

37. How do you report incident trends? Using dashboards, pie charts for severity split, time-based bar graphs, monthly metrics, and threat actor patterns.

38. What is the value of RCA in SOC? Root Cause Analysis helps prevent repeat incidents, improves response strategy, and enhances controls.

39. How do you handle SIEM outages or delay in logs? Communicate with log source owners, check EPS rate, collector health, time sync issues, and apply failover logging plans.

40. Whats the difference between IOC and TTP? IOC = Indicators (IP, hash, domain); TTP = Techniques (behaviors, how an attacker operates), based on MITRE ATT&CK.

General, Interviews, and Real-World

41. What do you do when you dont know an alerts root cause? Acknowledge, escalate with available data, seek peer input, and continue parallel investigation. Never guess.

42. What does defense-in-depth mean? Layered security controls across perimeter, endpoint, network, identity, data, and application levels.

50 Frequently Asked Inquiry Questions in Cybersecurity

43. What is zero trust? Never trust, always verify. Access is granted based on identity, device health, and context, not location or network.

44. How do you stay updated in cybersecurity? Following threat intel feeds, CVE feeds, MITRE updates, blogs (SANS, CISA, Krebs), and hands-on labs.

45. What is the difference between red, blue, and purple team? Red: Attacker simulation; Blue: Defender/monitoring; Purple: Collaboration to improve detection via feedback loops.

46. What are LOLBins and why are they dangerous? Living-Off-the-Land Binaries like rundll32.exe, wmic.exe used by attackers to evade detection because they're native OS tools.

47. What are stealth malware and fileless attacks? Malware that avoids detection by using memory-only execution, script-based attacks, and hiding inside legitimate processes.

48. What are the stages of a cyber kill chain? Recon Weaponize Deliver Exploit Install C2 Action. Helps in understanding and disrupting attack stages.

49. Whats your incident documentation process? Include timeline, alert details, systems involved, steps taken, RCA, evidence artifacts, and lessons learned.

50. Why should we hire you for a Senior SOC role? I bring layered experience in alert triage, SIEM tuning, threat hunting, incident response, and mentoring junior analysts, with a proven record of improving detection and response workflows.