National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Security Operations Center (SoC)

Top 50 Questions and Answers

Placement Cell, NFSU Goa
January 31, 2025

Security Operations Center (SoC) - Top 50 Questions

1. **What is a Security Operations Center (SoC)?** A centralized unit that monitors and defends an organization's security posture in real-time.

2. **What are the primary functions of a SoC?** Threat detection, incident response, continuous monitoring, and log analysis.

3. **How does a SoC differ from traditional IT operations?** IT operations manage system performance, while a SoC focuses on cybersecurity.

4. **What is SIEM, and why is it important in a SoC?** Security Information and Event Management (SIEM) collects, analyzes, and correlates logs to detect threats.

5. **What is an Intrusion Detection System (IDS)?** A tool that detects and alerts on suspicious activity in the network.

6. **What are Indicators of Compromise (IoCs)?** Forensic clues like unusual traffic or file changes that indicate a security breach.

7. **What is the difference between IDS and IPS?** IDS detects and alerts, whereas IPS actively blocks malicious traffic.

8. **What are the key components of a SoC?** Security tools (SIEM, IDS, firewalls), security analysts, and threat intelligence platforms.

9. **What is log correlation in a SoC?** Analyzing logs from multiple sources to identify security incidents.

10. **How does a SoC monitor network traffic?** By using firewalls, IDS/IPS, and network anomaly detection tools.

11. **Who are the key members of a SoC team?** Analysts, engineers, incident responders, and security managers.

12. **How does a SoC handle security incidents?** Following the process: Detect → Analyze → Contain → Eradicate → Recover.

13. **What is threat hunting?** Proactively searching for hidden threats that evade security tools.

14. **How does a SoC respond to zero-day vulnerabilities?** By using threat intelligence, behavior analytics, and rapid patching.

15. **What is forensic analysis in a SoC?** Investigating security incidents using digital evidence from logs and endpoints.

16. **How do Security Operations Centers handle DDoS attacks?** By using rate limiting, anomaly detection, and DDoS mitigation services.

17. **What is a security playbook?** A set of predefined response actions for handling security incidents.

18. **How does a SoC detect phishing attacks?** By monitoring email traffic, scanning attachments, and training employees.

Security Operations Center (SoC) - Top 50 Questions

19. **What is malware analysis in a SoC?** Analyzing malicious software behavior to understand its impact.

20. **How does encryption support SoC security?** Encryption ensures data confidentiality by converting it into unreadable formats.

21. **What is User and Entity Behavior Analytics (UEBA)?** UEBA detects anomalies by analyzing normal behavior patterns of users and systems.

22. **What role does AI play in a SoC?** AI enhances threat detection, automates analysis, and reduces false positives.

23. **What is the MITRE ATT CK framework?** A globally accessible knowledge base of adversary tactics and techniques.

24. **What is endpoint detection and response (EDR)?** EDR monitors and responds to security threats on individual devices.

25. **How does a SoC handle insider threats?** By monitoring user behavior and using access control policies.

26. **What is lateral movement in a cyber attack?** When attackers move deeper into a network after an initial compromise.

27. **What is a honeypot in cybersecurity?** A decoy system designed to attract and detect attackers.

28. **What is a security incident vs. an event?** An event is any occurrence, while an incident is a confirmed security breach.

29. **What is a vulnerability assessment?** A systematic review of security weaknesses in a system.

30. **How does a SoC prevent data exfiltration?** Using Data Loss Prevention (DLP) tools to block unauthorized data transfers.

31. **What is the difference between penetration testing and vulnerability scanning?** Penetration testing actively exploits vulnerabilities, while scanning only detects them.

32. **How do Security Operations Centers handle ransomware?** By maintaining backups, using behavior-based detection, and blocking malicious domains.

33. **What is a red team vs. a blue team in cybersecurity?** Red teams simulate attacks, while blue teams defend against them.

34. **What is zero-trust security?** A model where no user or device is automatically trusted.

35. **What are the benefits of a cloud-based SoC?** Scalability, global threat intelligence, and cost efficiency.

36. **How do SoCs integrate with DevSecOps?** By embedding security into the development pipeline.

37. **What is the role of compliance in a SoC?** Ensuring adherence to security regulations (e.g., GDPR, NIST, ISO 27001).

38. **How does an SoC detect and analyze security threats in real time?**
SoCs use a combination of real-time monitoring, log analysis, and machine learning algorithms to detect unusual behavior and potential threats.

39. **What types of attacks are commonly detected by a SoC?**
Common attacks detected include malware infections, DDoS attacks, phishing, ransomware, and data breaches.

40. **How do Security Operations Centers handle Distributed Denial-of-Service (DDoS) attacks?**
SoCs deploy DDoS mitigation strategies, including traffic filtering, rate-limiting, and using specialized DDoS protection services.

41. **What role do automated security tools play in threat detection in a SoC?**
Automated tools help identify patterns and flag suspicious activities, reducing the workload on analysts and enabling faster response times.

42. **How does machine learning support threat detection in a Security Operations Center?**
Machine learning models analyze vast amounts of data to detect anomalies and potential threats, enhancing the accuracy and speed of threat detection.

43. **How does an SoC respond to zero-day vulnerabilities?**
SoCs use threat intelligence, patch management, and rapid incident response protocols to mitigate the risks of zero-day vulnerabilities.

44. **What is a Security Incident, and how is it handled in a SoC?**
A security incident is an event that threatens the confidentiality, integrity, or availability of data. SoCs respond by identifying, containing, and mitigating the incident.

45. **How does an SoC manage cyber threats on endpoints?**
SoCs monitor endpoints using endpoint detection and response (EDR) tools to detect malicious activity and respond to threats in real time.

46. **How does an SoC handle phishing attacks?**
SoCs detect phishing attempts through email filtering, user training, and rapid response to block phishing sites or malicious links.

47. **What is the process for incident response in a SoC?**
The incident response process involves identifying the incident, containing it, mitigating damage, investigating, and restoring normal operations.

48. **What is the role of a firewall in a Security Operations Center?**
Firewalls act as a barrier to prevent unauthorized access to the network and provide logs that can be analyzed for potential threats.

49. **How does an IDS (Intrusion Detection System) support SoC operations?**
IDS monitors network traffic for suspicious patterns and alerts the SoC team of potential intrusions, aiding in the detection of attacks.

50. **What is the importance of encryption in a SoC?**
Encryption protects sensitive data, ensuring confidentiality and integrity during storage and transmission, making it harder for attackers to exploit.