

TOP 30

Security Operations Center (SOC)

Interview Questions & Answers 



+1 (646) 980-6267



www.thinkcloudly.com



info@thinkcloudly.com

The SOC Analyst (L1 & L2) interview questions and answers shared here are based on personal understanding, learning, and experience. These are intended solely for reference and educational purposes.

It's highly recommended to customize the responses according to one's own knowledge, real-time exposure, tools used, and practical scenarios to sound authentic and confident during interviews.



30 QUESTIONS AND ANSWERS

Q.1. What is a Security Operations Center (SOC)?

A SOC is a centralized team that continuously monitors, detects, analyzes, and responds to cybersecurity incidents in real time within an organization.

Q.2. What are the primary responsibilities of an L1 SOC Analyst?

L1 Analysts monitor alerts, perform initial triage, escalate confirmed incidents, and document findings.

Q.3. What is a SIEM and how is it used in SOC operations?

L1 Analysts monitor alerts, perform initial triage, escalate confirmed incidents, and document findings.

30 QUESTIONS AND ANSWERS

Q.4. What is the difference between a false positive and a false negative in security alerts?

- A false positive is an alert triggered without a real threat.
- A false negative is when a real threat goes undetected.

Q.5. What is phishing in the context of cybersecurity?

Phishing is a technique used by attackers to trick individuals into revealing sensitive information via deceptive emails or websites.

Q.6. What steps are typically followed after receiving a security alert?

Review the alert, analyze log details, validate the event, check for indicators of compromise (IOCs), and escalate if necessary.

Q.7. What does the CIA triad represent in information security?

- **Confidentiality:** Restricting access to authorized users
- **Integrity:** Ensuring data is not altered
- **Availability:** Ensuring systems and data are accessible when needed

Q.8. How can suspicious login activity be identified in log data?

By reviewing login times, geolocations, multiple failed login attempts, or access from unfamiliar devices/IPs.

Q.9. What are Indicators of Compromise (IOCs)?

IOCs are data points that suggest a security breach, such as malicious IPs, file hashes, domains, or registry changes.

30 QUESTIONS AND ANSWERS

Q.10. What tools are commonly used to investigate alerts?

Common tools include SIEM platforms (e.g., Splunk), WHOIS, VirusTotal, Shodan, and endpoint monitoring tools.

Q.11. What is the function of a firewall?

A firewall filters incoming and outgoing network traffic based on security rules to block unauthorized access.

Q.12. How are alerts prioritized in a SOC environment?

Alerts are prioritized based on impact, criticality of the affected asset, and potential threat severity.

30 QUESTIONS AND ANSWERS

Q.13. What is triage in cybersecurity incident management?

Triage is the process of evaluating and categorizing alerts to determine which require immediate attention or escalation.

Q.14. What is a brute-force attack?

It is an attack where an intruder attempts to gain access by systematically guessing passwords.

Q.15. What is the purpose of a ticketing system in SOC operations?

Ticketing systems are used to document, assign, track, and manage the lifecycle of security incidents.

Q.16. How does the role of an L2 SOC Analyst differ from L1?

L2 Analysts conduct deeper investigations, validate escalated incidents, perform threat hunting, and assist in incident response.

Q.17. What are the phases of the Incident Response lifecycle?

- Preparation
- Detection & Analysis
- Containment
- Eradication
- Recovery
- Lessons Learned

Q.18. What is threat hunting in a SOC environment?

Threat hunting involves proactively searching for undetected threats using behavioral analytics, hypotheses, and threat intelligence.

30 QUESTIONS AND ANSWERS

Q.19. How is malware analysis typically conducted?

Malware analysis involves checking file behavior, hashes, static and dynamic analysis, and running samples in sandboxes.

Q.20. What is meant by lateral movement in a cyberattack?

Lateral movement refers to an attacker's progression through a network after gaining initial access, aiming to reach critical systems.

Q.21. How is the MITRE ATT&CK framework utilized in investigations?

It helps map observed tactics and techniques to known attacker behavior, aiding in detection, analysis, and response planning.

30 QUESTIONS AND ANSWERS

Q.22. How is log correlation useful in incident investigation?

Log correlation connects events across multiple sources to reveal hidden patterns and understand attack vectors.

Q.23. How can a phishing attack be validated?

By analyzing email headers, inspecting URLs or attachments, checking sender authenticity, and reviewing recipient actions.

Q.24. What steps should be followed when handling a ransomware incident?

Isolate infected systems, identify malware, review encryption behavior, preserve evidence, and initiate incident response protocol.

30 QUESTIONS AND ANSWERS

Q.25. What are some common indicators of privilege escalation?

Unusual privilege assignments, access to sensitive files, execution of system-level commands, or group membership changes.

Q.26. How can a complex incident be resolved and documented?

By conducting root cause analysis, mitigating the threat, documenting steps taken, and updating playbooks for future reference.

Q.27. What are threat intelligence feeds and why are they important?

Threat intel feeds provide up-to-date data on known threats (IPs, domains, hashes), helping analysts stay ahead of new attacks.

30 QUESTIONS AND ANSWERS

Q.28. How is endpoint telemetry analyzed during an investigation?

Using EDR tools to assess file activity, process behavior, registry modifications, and network connections on the affected endpoint.

Q.29. What is the purpose of packet analysis tools like Wireshark?

These tools capture and inspect network packets to detect anomalies, unauthorized data transfer, or malicious traffic.

Q.30. How can SOC processes be continuously improved?

By refining detection rules, updating response playbooks, reducing false positives, automating tasks, and training the team.

“

Crack your SOC interview with
confidence—practice with
Thinkcloudly's simple and effective
questions!



”



+1 (646) 980-6267



www.thinkcloudly.com



info@thinkcloudly.com