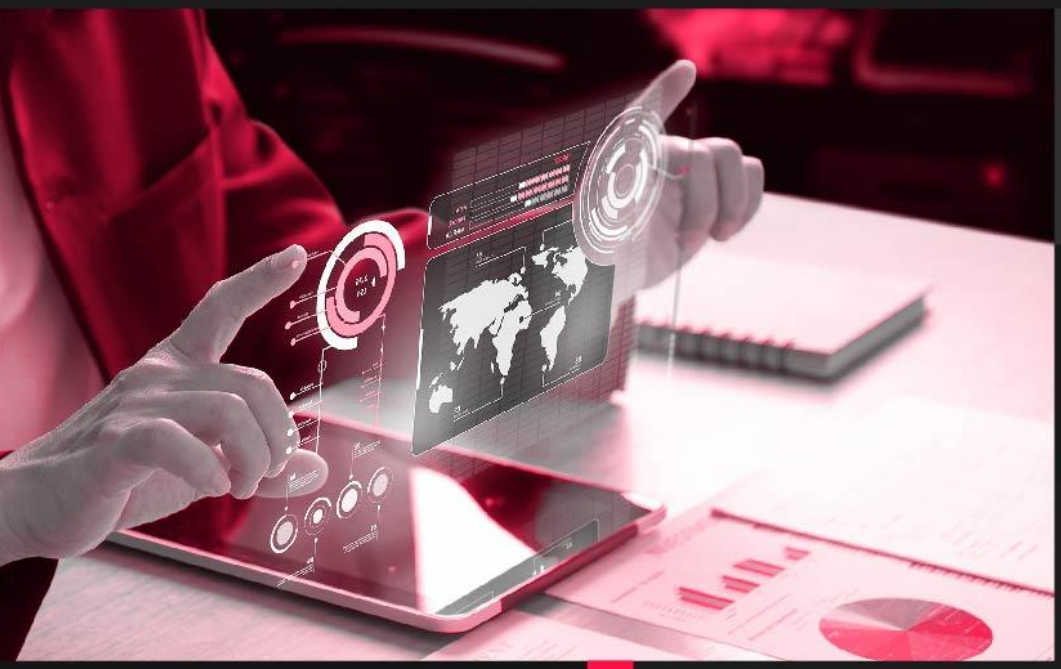
INFOSECTRAIN

SOC Analyst Interview Questions and Answers



About us

InfosecTrain is one of the finest Security and Technology Training and Consulting organization, focusing on a range of IT Security Trainings and Information Security Services. InfosecTrain was established in the year 2016 by a team of experienced and enthusiastic professionals, who have more than 15 years of industry experience. We provide professional training, certification & consulting services related to all areas of Information Technology and Cyber Security.

Due to the rapid increase in data breach incidents and sophisticated attacks, organizations are investing heavily in technologies and security solutions. The deployment of a security operation center (SOC) is a cost-effective strategy against these cyber threats. The SOC team deals with security incidents within the organization. The SOC Analyst plays a vital role in the SOC team by monitoring the log data, identifying suspicious activities, and reporting to the higher authorities. It could be an excellent platform to start your career in cybersecurity. A candidate must have a basic knowledge of networking, malware analysis, and incidence response.

This article outlines the most common SOC Analyst interview questions and answers to help you get selected for a SOC Analyst job role. The questions test the knowledge of candidates about various SOC processes, networking, and web application security.

Question 1: Explain the SOC team architecture?

Answer: The SOC team consists of different levels. The following diagram exhibits a traditional SOC team hierarchy.

Nowadays, there are additional job roles included in the SOC team hierarchy. These job roles are as follows:

- Threat Intelligence Analyst
- Threat Hunter
- Incident Handler
- Digital Forensic Investigator
- Red Team Specialist
- Incident Response Automation Engineer

Question 2: What are the responsibilities of L1 and L2 Security Analyst?

Answer: Responsibilities of L1 Security Analyst:

- Monitoring security incidents 24/7 from various SOC entry channels (SIEM, e-mail, firewall, IDS, IPS)
- Analysis of the triggered security incidents
- Raising tickets for validated incidents
- Formulate remediation strategies with the incident response team
- Helping L2 security analyst and SOC Lead in preparing reports

Responsibilities of L2 Security Analyst

- A detailed evaluation of escalated alerts
- Helping L1 security analyst in the assessment of alerts
- Troubleshooting the issues with SIEM
- Assisting in the remediation planning after a security incident has occurred

(The interviewer may ask this question to check the awareness of a candidate about the job responsibilities)

Question 3: What are the advantages of having a SOC team?

Answer: The following are the advantages of having a SOC team in an organization:

- SOC team provides continuous monitoring and analysis of security events. Therefore it helps in detecting intrusion and prevents any potential attacks.
- The approach of the SOC team is proactive rather than being reactive.
- The SOC team also ensures that the organization stays compliant with the existing regulations or policies.
- The SOC team provides a complete overview of the organization's security posture by correlating all the events taking place over the network.
- With the expertise of a SOC team, an organization can respond quickly to external threats and security incidents.

Question 4: What is the three-way handshake?

Answer: A three-way handshake (also known as TCP-3way handshake) is a mechanism to establish a connection between the client and server over a TCP/IP network. In this mechanism, the client and server send each other the synchronization and acknowledgment packets before an actual data transmission occurs.

Three-way handshake mechanism: In this mechanism, the client sends an SYN TCP packet to the server asking for a connection (synchronizing) request and a sequence number. The server responds with the SYN/ACK packet, acknowledging the connection request and assigning a sequence number. The client again sends an ACK packet to accept the response of the server.

Question 5: What documents do you create in SOC?

Answer: SOC team creates the following documents:

- Log source onboarding
- Log source decommissioning
- Threat intelligence gathering procedures
- Threat hunting methodologies
- New use case development procedures
- Data configuration backup procedures

Question 6: What is data leakage? Explain in your own words.

Answer: Data leakage refers to the exposure or transmission of an organization's sensitive data to the external recipient. The data may be transmitted or exposed via the internet or by physical means.

The following factors can be responsible for data leakage:

- Most of the data losses are accidental. For example, an employee may unintentionally be transmitting information to the wrong recipient.
- Disgruntled employees
- Insecure backup storage
- System breach by a hacker
- Systems not properly configured
- Inappropriate security control measures

Question 7: List the steps to develop the Data Loss Prevention (DLP) strategy?

Answer: The steps to develop and implement a DLP strategy are as follows:

Step1: prioritizing the critical data assets

Step2: categorizing the data based on its source

Step3: analyzing which data is more prone to the risks

Step4: monitor the transmission of the data

Step5: developing control measures to mitigate the data leakage risk

Question 8: What is the difference between TCP and UDP?

Answer: The difference between TCP and UDP is as follows:

TCP(Transfer Layer Protocol)	UDP(User Datagram Protocol)
TCP is a connection-oriented protocol	UDP is a datagram oriented protocol
TCP is reliable as it guarantees the delivery of data packets to the destination	UDP is not reliable as it does not guarantee the delivery of data packets to the destination
TCP Provides a thorough error checking mechanism	UDP provides a basic error checking mechanism
TCP is heavyweight	UDP is lightweight
TCP is slower as compared to UDP	UDP IS faster than TCP
Failed data packets are retransmitted in TCP	In UDP, there is no re-transmission for failed data packets
Example: HTTP, SSH, HTTPS, SMTP	Example: TFTP, VoIP, online multiplayer games

Question 9: What is the difference between firewall deny and drop?

Answer: DENY RULE: If the firewall is set to deny rule, it will block the connection and send a reset packet back to the requester. The requester will know that the firewall is deployed.

DROP RULE: If the firewall is set to drop rule, it will block the connection request without notifying the requester.

It is best to set the firewall to deny the outgoing traffic and drop the incoming traffic so that attacker will not know whether the firewall is deployed or not.

Question 10: What is the difference between SIEM and IDS?

Answer: SIEM (security incident and event management system) and IDS (intrusion detection system) are used by the organizations to protect the network and systems efficiently. Both collect the log data, but unlike SIEM, IDS does not facilitate event correlation and centralization of log data. Therefore, IDS can only detect intrusions. The SIEM allows Security Analysts to take security measures and preventive actions against a possible or ongoing attack.

Question 11: Explain different SOC models?

Answer: There are three types of models in SOC:

- **In-house model:** In this SOC model organization has its security operation center. All the resources, technologies, and processes are managed within the organization.
- **MSSP (Managed security service provider):** In MSSP, a security service provider team helps the organization monitor and manage the security incidents.

1. **Dedicated MSSP:** In the dedicated MSSP, the team works for a client using its technology and resources.
2. **Shared MSSP:** In the shared MSSP team of services providers, use his technology and logs, and security incidents are managed at its data center.

- **Hybrid SOC model:** It is the blend of in-house and MSSP SOC models. In the hybrid SOC model, level-1 monitoring is managed by MSSP, and level-2 monitoring is run by the organization (client) itself.

Question 12: What is the Runbook in SOC?

Answer: A runbook, also known as a standard operating procedure (SOP), consists of a set of guidelines to handle security incidents and alerts in the Security Operation Centre. The L1 Security Analyst generally uses it for better assessment and documentation of the security events.

Question 13: What is the difference between the Red Team and the Blue Team?

Answer: The red team and blue team consist of highly skilled cybersecurity professionals. Both teams play an important role in strengthening the security posture of an organization.

Red Team: The red team plays an offensive role. The team conducts rigorous exercises to penetrate the security infrastructure and identify the exploitable vulnerabilities in it. The red team is generally hired by the organization to test the defenses.

Blue Team: The blue team plays a defensive role. The blue team's role is to defend the organization's security infrastructure by detecting the intrusion. The members of a blue team are internal security professionals of the organization.

Question 14: Define a Phishing attack and how to prevent it?

Answer: Phishing is a type of social engineering attack in which an attacker obtains sensitive information from the target by creating urgency, using threats, impersonation, and incentives. Spear phishing, e-mail spam, session hijacking, smishing, and vishing are types of phishing attacks.

Ways to prevent a phishing attack:

- Raising awareness about phishing attack among employees
- Conducting testing campaigns to check the awareness of the employees
- Implementing two-factor authentication
- Monitoring the behavior of employees
- Applying email filters to identify spams

Question 15: What is the cross-site scripting (XSS) attack, and how to prevent it?

Answer: Cross-site scripting: In the cross-site scripting attack, the attacker executes the malicious scripts on a web page and can steal the user's sensitive information. With XSS vulnerability, the attacker can inject Trojan, read out user information, and perform specific actions such as the website's defacement.

Countermeasures:

- Encoding the output
- Applying filters at the point where input is received
- Using appropriate response headers
- Enabling content security policy
- Escaping untrusted characters

Question 16: Explain the SQL injection vulnerability and give countermeasures to prevent it?

Answer: SQL injection: SQL injection is a famous vulnerability in the web application that allows hackers to interfere in communication taking place between a web application and its database. Hackers inject malicious input into the SQL statement to compromise the SQL database. They can retrieve, alter, or modify the data. In some cases, it allows attackers to perform DDOS attacks.

Countermeasures:

- Using parameterized queries
- Validating the inputs
- Creating stored procedures
- Deploying a web application firewall
- Escaping untrusted characters

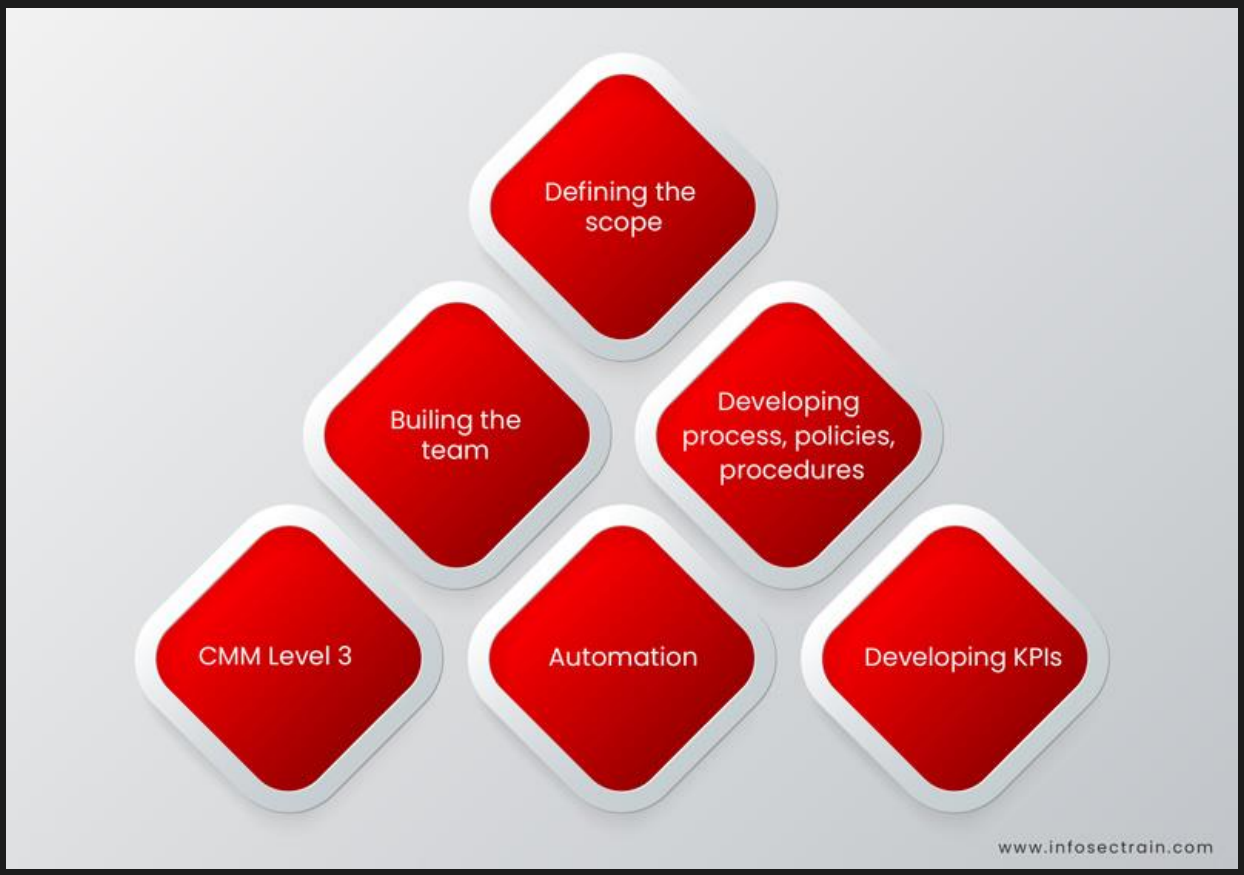
Question 17: Difference between hashing and encryption?

Answer: The difference between hashing and encryption is as follows:

Hashing	Encryption
Conversion of data into a fixed-length of unreadable strings using algorithms	Conversion of data into an unreadable string using cryptographic keys
Hashed data cannot be reverted back into readable strings	Encrypted data can be decrypted back into readable strings
The length of the hashed string is fixed	The length of the encrypted string is not fixed
No keys are used in hashing	Keys are used in encryption

Question 18: What are the SOC implementation stages?

Answer: Following are the stages in the SOC implementation:



Question 19: Being a SOC Analyst, what will you do if you found 300 alerts triggered at once?

Answer: If multiple alerts trigger at the same time, there could be the following three possibilities:

A single alert may have triggered more than once: If a single alert triggers more than once, I will distinguish the duplicate alerts.

If the alerts are different: I will prioritize them and chose the one having a higher impact.

If the alerts are for a new correlation rule: Then alerts may be misconfigured. I will inform the SIEM Engineer.

(These types of questions are asked by the interviewer to check the practical or applied knowledge of the candidates)

Question 20: What is DNS? Why is DNS monitoring essential?

Answer: The domain name system is a distributed database over the internet that enables converting user-friendly hostnames into computer-friendly IP addresses. It is known as the phonebook of the internet.

DNS plays a vital role in how an end-user in an organization connects to the internet. Whenever a client establishes a connection with a domain, its information is stored in DNS logs. DNS monitoring can disclose information such as websites visited by the employee, malicious domain accessed by an end-user, malware connecting to Command & Control server. It can help in identifying and thwarting cyberattacks.

Wrap Up

These were the frequently asked SOC Analyst interview questions that might help you get an opportunity to be a SOC team member. The interview questions may vary depending upon the organization. Be prepared for the questions regarding your background and the technologies you have worked on in your previous organization. Just like any other interview, confidence, and good communication skills are key to success.

It is recommended to validate your technical skills and expertise with the help of some industry-recognized certifications. Check out these certified SOC Analyst training program offered by the InfosecTrain:

https://www.infosectrain.com/courses/certified-soc-analyst-csa-certification-training/

https://www.infosectrain.com/courses/ibm-security-qradar-siem-training/

IND: 1800-843-7890 (Toll Free) / US: +1 657-221-1127 /
UK : +44 7451 208413

sales@infosectrain.com

www.infosectrain.com