SOC ANALYST


Security team trying to find out who is responsible for the incident
CISO

Contents:

Preparing:

Congratulations on taking the first step towards a career as a SOC Analyst! As you prepare for interviews in this dynamic field, it's essential to equip yourself with the right knowledge and strategies to stand out. This comprehensive guide is designed to help you navigate SOC Analyst interviews with confidence and professionalism.

Understanding The Role:

Before diving into interview preparation, it's crucial to have a clear understanding of the SOC Analyst role. Learn about the responsibilities, skills, and qualifications typically required for this position. Familiarize yourself with common tools and technologies used in Security Operations Centers (SOCs) to demonstrate your readiness for the role.

Company Insight: Researching Your Potential Employer

Research the company you're applying to thoroughly. Understand whether they provide support to multiple businesses simultaneously or if they operate an internal SOC. If you have connections at the company, such as a friend or acquaintance, consider reaching out to gain insights into the company culture and potential challenges.

Preparing for Interviews:

Effective preparation is key to interview success. Explore practical tips and strategies to help you prepare mentally and emotionally for SOC Analyst interviews. From researching the company and understanding industry trends to practicing common interview questions, we'll cover everything you need to know to impress potential employers.

Salary Strategy: Navigating Compensation Discussions

During the interview, refrain from discussing salary expectations upfront. Instead, opt for a response that indicates flexibility, such as, "I believe my salary expectations align with industry standards. I'm open to discussing specifics during the proposal stage." Additionally, familiarize yourself with the salary range for the position you're seeking. Seek advice from online forums like Reddit or other reliable sources to ensure you have a realistic understanding of salary expectations.

WHAT SHOULD YOU EXPECT?

Below is a list of the topics on which questions can be asked in the interview.

Security Analyst

- Basic terminologies
- Network fundamentals
- Operating system fundamentals
- Malware analysis fundamentals
- How to analyze attacks (phishing, malware...)

Incident Responder

- Incident response prosedure
- How to detect and remediate specific kind of attack (like golden ticket, phishing
- etc.) Ransomware remediation process

GENERAL QUESTIONS

How do you keep yourself updated with information security?

- Reading daily infosec news from different resources.
- The Hacker News
- Malwarebytes Labs
- HackRead
- ThreatPost
- By following infosec related social media accounts. Telegram channels
- Joining newsletters related to cyber security

What are black hat, white hat and gray hat?

Blat hat: Black-Hat Hackers are those hackers who enter the system without taking owners' permission. These hackers use vulnerabilities as entry points. They hack systems illegally. They use their skills to deceive and harm people. (GeeksforGeeks)

White hat: White-Hat Hackers are also known as Ethical Hackers. They are certified hackers who learn hacking from courses. These are good hackers who try to secure our data, websites. With the rise of cyberattacks organizations and governments have come to understand that they need ethical hackers. (GeeksforGeeks)

Gray hat: Gray-Hat Hackers are a mix of both black and white hat hackers. These types of hackers find vulnerabilities in systems without the permission of owners. They don't have any malicious intent. However, this type of hacking is still considered illegal. But they never share information with black hat hackers. They find issues and report the owner, sometimes requesting a small amount of money to fix it. (GeeksforGeeks)

GENERAL QUESTIONS

What is port scanning?

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. (Avast)

Do you know any programming language?

While this question is up to you, having a basic understanding of programming languages can be a plus for the interview.

How can you define Blue Team and Red Team basically?

Red team is attacker side, blue team is defender side.

What is firewall?

Firewall is a device that allows or blocks the network traffic according to the rules.

Explain Security Misconfiguration

It is a security vulnerability caused by incomplete or incorrect misconfiguration.

Explain vulnerability, risk and threat.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (src: NIST)

Risk: the level of impact on agency operations (including mission functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (src: NIST)

Threat: Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (src: NIST)

GENERAL QUESTIONS

What is compliance?

Following the set of standards authorized by an organization, independent part, or government.

What is MITRE ATT&CK?

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. (MITRE ATT&CK)

Do you have any project that we can look at?

If you do have any project to show, make sure that you prepare it before the interview.

Explain 2FA.

2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. (Authy)

Could you share some general endpoint security product names?

- Antiviru
- s EDR
- XDR
- DLP

NETWORK

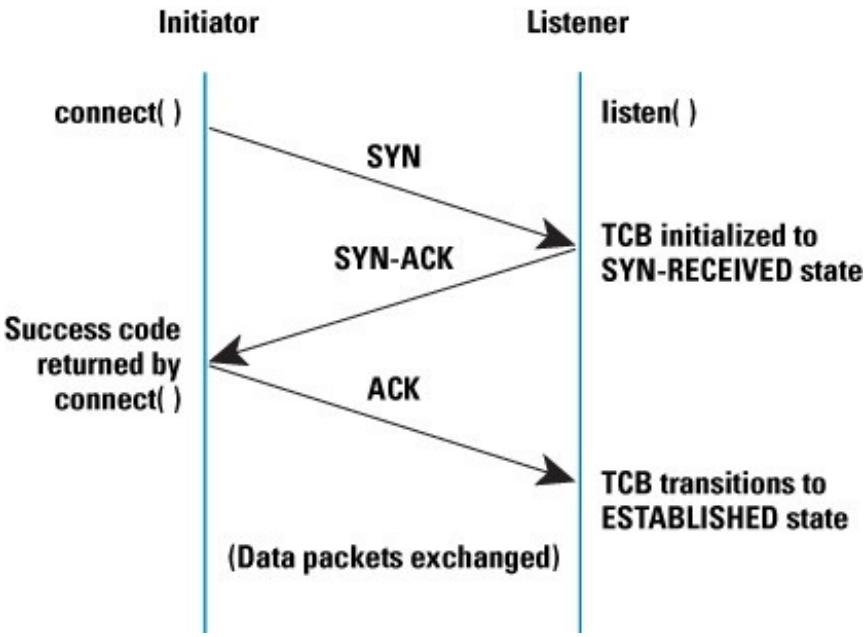
What is OSI Model? Explain each layer.

The **Open Systems Interconnection model** (**OSI model**) is a conceptual model that describes the universal standard of communication functions of a telecommunication system or computing system, without any regard to the system's underlying internal technology and specific protocol suites. (Wikipedia)

1. **Physical layer:** The Physical Layer is responsible for the transmission and reception of unstructured raw data between a device, such as a network interface controller, Ethernet hub or network switch and a physical transmission medium. It converts the digital bits into electrical, radio, or optical signals.
2. **Data link layer:** The data link layer provides node-to-node data transfer—a link between two directly connected nodes. It detects and possibly corrects errors that may occur in the physical layer. It defines the protocol to establish and terminate a connection between two physically connected devices. It also defines the protocol for flow control between them. IEEE 802 divides the data link layer into two sublayers: a. Medium access control (MAC) layer – responsible for controlling how devices in a network gain access to a medium and permission to transmit data. b. Logical link control (LLC) layer – responsible for identifying and encapsulating network layer protocols, and controls error checking and frame synchronization.
3. **Network layer:** The network layer provides the functional and procedural means of transferring packets from one node to another connected in "different networks".
4. **Transport layer:** The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source host to a destination host from one application to another across a network, while maintaining the quality-of-service functions. Transport protocols may be connection-oriented or connectionless.

NETWORK

What is three-way handshake?



TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other.
The client chooses an initial sequence number, set in the first SYN packet. The server also chooses its own initial sequence number, set in the SYN/ACK packet.
Each side acknowledges each other's sequence number by incrementing it; this is the acknowledgement number. The use of sequence and acknowledgment numbers allows both sides to detect missing or out-of-order segments.
Once a connection is established, ACKs typically follow for each segment. The connection will eventually end with a RST (reset or tear down the connection) or FIN (gracefully end the connection). (ScienceDirect)

NETWORK

What is TCP/IP Model? Explain the difference between OSI and TCP/IP model.

The TCP/IP model is the default method of data communication on the Internet. It was developed by the United States Department of Defense to enable the accurate and correct transmission of data between devices.
TCP/IP divides communication tasks into layers that keep the process standardized, without hardware and software providers doing the management themselves. The data packets must pass through four layers before they are received by the destination device, then TCP/IP goes through the layers in reverse order to put the message back into its original format. (Fortinet)
TCP/IP Model contains four layers. The layers are:
1.Application Layer
2.Transport Layer
3.Internet Layer
4.Network Access Layer

What is ARP?

The **Address Resolution Protocol** (**ARP**) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite. (Wikipedia)

What is DHCP?

The **Dynamic Host Configuration Protocol** (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

NETWORK

Could you share some general network security product names?

- Firewal
- I IDS
- IPS
- WAF

What is the key difference between IDS and IPS?

IDS only detect the traffic but IPS can prevent/block the traffic.

How can you protect yourself from Man-in-the-middle attacks?

While answering this question vary different scenarios, encryption is the key point for being safe.

WEB APPLICATION SECURITY

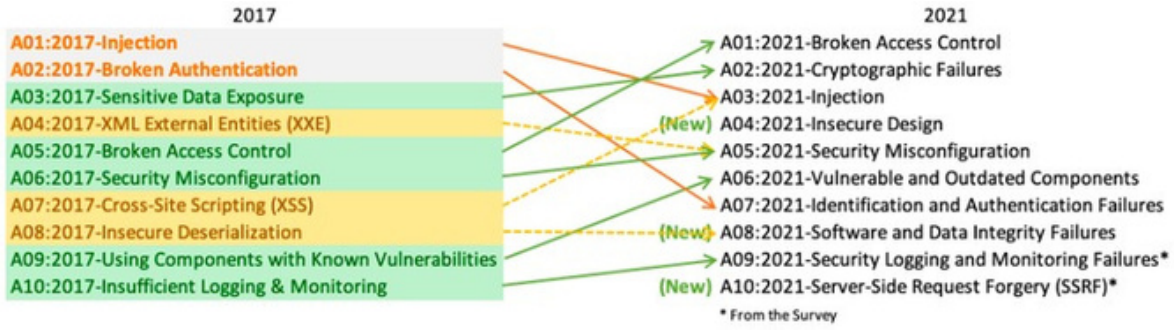
What are the HTTP response codes?

1XX: Informational **2XX:** Success **3XX:** Redirection **4XX:** Client-side error **5XX:** Server-side error

For example, 404 is 'server cannot find the requested resource'.

Explain OWASP Top Ten.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. (OWASP)



WEB APPLICATION SECURITY

What is SQL injection?

SQL Injections are critical attack methods where a web application directly includes unsanitized data provided by the user in SQL queries. (LetsDefend)

Explain SQL injection types.

There are 3 types of SQL Injections. These are:

1. **In-band SQLi (Classical SQLi)**: If a SQL query is sent and a replied to over the same channel, we call these In-band SQLi. It is easier for attackers to exploit these compared to other SQLi categories.
2. **Inferential SQLi (Blind SQLi):** SQL queries that receive a reply that cannot be seen are called Inferential SQLi. They are called Blind SQLi because the reply cannot be seen.
3. **Out-of-band SQLi**: If the reply to a SQL query is communicated over a different channel then this type of SQLi is called Out-of-band SQLi. For example, if the attacker is receiving replies to his SQL queries over the DNS this is called an out-of-band SQLi.

How to prevent SQL injection vulnerability?

- **When examining a web request check all areas that come from the user:** Because SQL Injection attacks are not limited to the form areas, you should also check the HTTP Request Headers like User-Agent.
- **Look for SQL keywords:** Look for words like INSERT, SELECT, WHERE within the data received from users.
- **Check for special characters:** Look for apostrophes (‘), dashes (-), or parentheses which are used in SQL or special characters that are frequently used in SQL attacks within the data received from the user.
- **Familiarize yourself with frequently used SQL Injection payloads:** Even though SQL payloads change according to the web application, attackers still use some common payloads to check for SQL Injection vulnerabilities. If you are familiar with these payloads, you can easily detect SQL Injection payloads. You can see some frequently used SQL Injection payloads here.

WEB APPLICATION SECURITY

What is XSS and how XSS can be prevented?

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. (OWASP)

For XSS attacks to be successful, an attacker needs to insert and execute malicious content in a webpage. Each variable in a web application needs to be protected. Ensuring that **all variables** go through validation and are then escaped or sanitized is known as perfect injection resistance. Any variable that does not go through this process is a potential weakness. Frameworks make it easy to ensure variables are correctly validated and escaped or sanitised.

However, frameworks aren't perfect and security gaps still exist in popular frameworks like React and Angular. Output Encoding and HTML Sanitization help address those gaps.

WEB APPLICATION SECURITY

What is IDOR?

Insecure **D**irect **O**bject **R**eference (IDOR), is a vulnerability caused by the lack of an authorization mechanism or because it is not used properly. It enables a person to access an object that belongs to another.
Among the highest web application vulnerability security risks published in the 2021 OWASP, IDOR or “Broken Access Control” takes first place.

What is RFI?

Remote File Inclusion (RFI), is the security vulnerability that occurs when a file on different server is included without sanitizing the data obtained from a user.

What is LFI?

Local File Inclusion (LFI), is the security vulnerability that occurs when a local file is included without sanitizing the data obtained from a user.

Explain the difference between LFI and RFI?

LFI differs from RFI because the file that is intended to be included is on the same web server that the web application is hosted on.

CRYPTOGRAPHY

What are encoding, hashing, encryption?

Encoding: Converts the data in the desired format required for exchange between different systems.
Hashing: Maintains the integrity of a message or data. Any change did any day could be noticed.
Encryption: Ensures that the data is secure and one needs a digital verification code or image in order to open it or access it.

What is the difference between hashing and encryption?

- **Hashing:** Hashing is the process of converting the information into a key using a hash function. The original information cannot be retrieved from the hash key by any means. (GeeksforGeeks)
- **Encryption:** Encryption is the process of converting a normal readable message known as plaintext into a garbage message or not readable message known as Ciphertext. The ciphertext obtained from the encryption can easily be transformed into plaintext using the encryption key. (GeeksforGeeks)
- **Difference:**

Hashing and encryption, though both used for data security, serve different purposes. Think of hashing like a fingerprint. You can't recreate the original data from a hash, but it's a unique identifier that lets you know if the data has been tampered with.
Encryption scrambles the information itself, like locking a message in a box. Only someone with the key can unlock it and read the original message. So, hashing is for verifying data integrity, while encryption is for keeping data confidential.

MALWARE ANALYSIS

What is the name of the software that compiles of the written codes?

Compiler

What is the name of the software that translates machine codes into assembly language?

Disassembler

What is the difference between static and dynamic malware analysis?

Static Analysis: It is the approach of analyzing malicious software by reverse engineering methods without running them. Generally, by decompile / disassemble the malware, each step that the malware will execute is analyzed, hence the behavior / capacity of the malware can be analyzed.

Dynamic Analysis: It is the approach that examines the behavior of malicious software on the system by running it. In dynamic analysis, applications that can examine registry, file, network and process events are installed in the system, and their behavior is examined by running malicious software.

EVENT LOG ANALYSIS

Which event logs are available default on Windows?

- Security
- Application
- System

With which security Event ID can the Successfully RDP connection be detected?

4624

With which event id can failed logons be detected?

4625

Which field of which event should I look at so that I can detect RDP logons?

You can detect RDP logon activities with event ID 4624. "Logon Type" value should be **10**.

THREAT INTELLIGENCE

What is Cyber Threat Intelligence (CTI)?

Threat intelligence is the analysis of data using tools and techniques to generate meaningful information about existing or emerging threats targeting the organization that helps mitigate risks. Threat Intelligence helps organizations make faster, more informed security decisions and change their behavior from reactive to proactive to combat the attacks. (eccouncil)

What is TAXII in Cyber Threat Intelligence (CTI)?

TAXII, short for Trusted Automated eXchange of Intelligence Information, defines how cyber threat information can be shared via services and message exchanges. (anomali)

Name some of the Threat Intelligence Platforms

IBM X Force Exchange, Cisco Talos, OTX AlienVault

What are the types of Threat Intelligence?

- Strategic Threat Intelligence
- Tactical Threat Intelligence
- Technical Threat Intelligence
- Operational Threat Intelligence