SOC Analyst Guide For Beginners

In this chapter, you will learn what a **security operations center** (**SOC**) analyst is and the average salary range for this career in the United States. You will also learn about the career progression options and learn common interview questions for the role.

The following topics will be covered in this chapter:

- What is a SOC analyst?
- How much can you make in this career?
- What other careers can you do?
- Common interview questions for a SOC analyst career

What is a SOC analyst?

SOC analysts work as members of a managed security services team. There are typically three tiers of SOC analysts, and job-specific duties may vary based on the organization you work for:

- **SOC level 1 (tier 1) analysts** typically monitor security tools, such as **endpoint detection and response** (**EDR**) and **security information and event management** (**SIEM**) tools, to identify potential anomalous activity on networks and systems. If anomalous activity is detected, they then escalate it to level 2 analysts.
- **SOC level 2 (tier 2) analysts** investigate anomalous behavior. In some instances, they may perform **incident response** (**IR**) duties and initial malware analysis. You might build IR playbooks and perform scripting to automate routine tasks. You might also see level 2 skills being requested for incident responder job postings. Your tier 2 SOC analyst might also set up the access for jump boxes and do light forensic investigation work.
- **SOC level 3 (tier 3) analysts** perform IR and also typically perform threat hunting and threat profiling. They may also do some work in reverse engineering malware and digital forensics depending on their organization. You might see these job openings listed as incident responders or threat analysts/hunters. One thing to keep in mind if you are transitioning from another career to cybersecurity is you can often find non-traditional jobs at a cybersecurity product company and use this as the starting point for your career. As an example, if you are transitioning from selling used cars, you could get a job with the sales team at a security company such as Splunk. The company will then train you on all of their cybersecurity product and service offerings for free, then in 6 to 12 months, you will have a better chance of getting a cybersecurity job because you will then have experience at Splunk and you have experience with their different product offerings so you have in-demand skills. Many people focus on getting jobs as a SOC analyst or penetration tester because that's what their guidance counselor tells them to do, but it is often a better idea to look at non-traditional jobs to get your start in a cybersecurity career because others are not applying for those jobs. If you look at the Splunk company website, you will see hundreds of open non-traditional jobs, at the time of writing, that can be leveraged to get your start in a rewarding cybersecurity career.

How much can you make in this career?

SOC analyst salaries can vary significantly by location, company, and other factors. In the United States, you can expect to make between $60,000 and $85,000 for an entry-level SOC level 1 role.

What other careers can you do?

A career as a SOC analyst builds a solid foundational skill set and can help you prepare for many cybersecurity careers. Some examples are a forensic investigator, reverse engineer, penetration tester, GRC analyst, and CISO.

Common interview questions for a SOC analyst career

In the following sections, you will learn about common interview questions, including general knowledge, attack types, and tools, that you might experience in interviews for a SOC analyst position. The questions are listed with answers. A key item to note is that you want to keep your answers as short as possible during the interview and then just ask the interviewer whether they need you to expand upon the subject.

Remember that *clear and concise make the interview nice*.

General SOC knowledge questions

In this section, you will see some general SOC knowledge questions that might be asked in a SOC analyst interview:

- **What is information security and how is it achieved?**

  Information security just means protecting the confidentiality, integrity, and availability of information. It is achieved through risk management, where you identify the valuable information, identify any assets related to that information, identify vulnerabilities, identify threats to the CIA of the information, and identify the impact to the information and the organization if an incident occurs.

- **Explain risk, vulnerability, and threat.**

  Vulnerability is a weakness in a system. Vulnerabilities are weaknesses. This means there is a gap in the protection of a system. A **threat** is an attacker that is trying to exploit the vulnerability for their own gain.

Risk is the measure of potential loss when the vulnerability is exploited by the threat actor.

If you think of a house, a vulnerability (weakness) might be not paying the bill for your alarm monitoring company. A threat actor (burglar in this case) might use this weakness to get into your house. You would need to analyze the risk to see whether you have valuables inside of your home that justify the cost of paying for the alarm monitoring service.

- **What is the difference between asymmetric and symmetric encryption, and which one is better?**

  Symmetric encryption uses the same key to encrypt and decrypt. Asymmetric encryption uses different keys to encrypt and decrypt.

  Both have benefits and drawbacks. Symmetric encryption is normally faster than asymmetric, but the key needs to be transferred over an unencrypted channel. Asymmetric is slower but more secure. It's best to use a hybrid of the two.

- **What is an IPS and how does it differ from an IDS?**

  An **intrusion detection system** (**IDS**) detects an intrusion and then will just alert the administrator for them to take further action.

  An **intrusion protection system** (**IPS**) will detect the intrusion and then take action to prevent the intrusion.

- **What is the difference between encryption and hashing?**

  Encryption is reversible and hashing is one-way. Hashing can be cracked in some cases using rainbow tables and collision attacks, but it is not reversible. Hashing ensures the integrity of data, and encryption ensures the confidentiality of data. A simple way to remember the difference between the two is that hashing protects the integrity of data and is one-way, and encryption is used to protect the data itself and is two-way, meaning once you encrypt something, you can then decrypt it to see the data in its original form.

- **What is a security misconfiguration?**

  A security misconfiguration is where the network, application, or device, for example, is configured to allow an attacker to exploit it easily. One of the most common security misconfigurations in both the consumer and B2B space is the use of default login credentials. Another common security misconfiguration involves cloud environments, where access to sensitive data is not restricted.

- **What are black hat, white hat, and gray hat hackers?**

  Black hat is used to describe someone who does not have the authorization to access systems or data but attempts to do so anyway. A white hat (ethical) hacker has permission from the owner. A gray hat hacker hacks without permission but does it for the greater good. A good example of a gray hat was the hacker that hacked home **wireless access points** (**WAPs**) to update the firmware, so users would be protected against a critical vulnerability (`https://www.zdnet.com/article/a-mysterious-grey-hat-is-patching-peoples-outdated-mikrotik-routers/`).

- **What is a firewall?**

  A firewall is like a gate guard. Based on a set of predefined rules, it either allows traffic or not, similar to a gate guard allowing you to go through the gate and visit Oprah or not.

  In modern networks, firewalls are still used but there is really no *perimeter* anymore due to things such as **bring your own device** (**BYOD**).

- **How do you keep yourself updated with the information security news?**

  This question helps the interviewer understand your passion and motivation for the role. You can use something such as **Feedly** to aggregate cybersecurity news into a single location for review or just follow some of the more common sources of news (such as Threatpost, The CyberWire, and The Hacker News). No one expects you to know everything that is going on, but you should have a good idea of the major news each week in the cyber world.

- **The world has recently been hit by an attack (that is, SolarWinds). What would you do to protect your organization as a security professional?**

  If you have some experience, you can answer this using that as an example. If this is your first cyber role, then focus on the IR steps listed in *NIST SP 800-61*.

- **What is the CIA triad?**

  The CIA triad can be defined as follows:

  - **Confidentiality** is just making sure that only the right people, systems, or applications can access data. Think of confidentiality as locking your data in a safe, and only giving access to people you trust.
  - **Integrity** is making sure the data has not been altered.
  - **Availability** is making sure the right users can access the right information when they need to. In some industries, such as critical infrastructure, availability comes before confidentiality and integrity on the priority list.

- **HIDS and NIDS – which one is better and why?**

  A **host intrusion detection system** (**HIDS**) is just an IDS that lives on a host machine. A drawback of host-based detection is it can consume a lot more processing power than a **network intrusion detection system** (**NIDS**). Both HIDSs and NIDSs perform similar actions, but an HIDS offers more visibility into suspicious activity on the endpoint.

- **What is a security policy?**

  A security policy is a document that outlines how to protect an organization from threats, and the procedures for responding to incidents.

- **What are the core principles of information security?**

  The core principles are as follows:

  - Confidentiality
  - Integrity
  - Availability

- **What is non-repudiation (as it applies to IT security)?**

  Non-repudiation basically means that neither the sender nor receiver of the information can deny that they processed the information. The sender or receiver could be human-to-human communication, human-to-machine, or machine-to-machine.

- **What is the relationship between information security and data availability?**

  Information security entails protecting data and ensuring that only authorized entities can access the data. Data availability just means that the authorized entities can access the data when they need to.

- **What is the difference between logical and physical security? Can you give an example of both?**

  Physical security is preventing unauthorized entities from physically accessing things they should not have access to. For example, you put up a fence around your house, set up CCTV cameras, get an alarm system, and get a dog. These are all examples of physical security controls to stop unauthorized access.

  Logical security covers the electronic form of preventing unauthorized access. You might do this through something such as using encryption for data in transit and rest so no one else can read the data.

- **What's an acceptable level of risk?**

  This depends on the risk appetite of the organization.

- **Can you give me an example of common security vulnerabilities?**

  For this question, I would keep it simple and focus on a few things such as security misconfigurations, **identity and access management** (**IAM**) of third parties, and credential reuse. You can then ask the interviewer whether they need you to expand on anything else.

- **Are you familiar with any security management frameworks, such as ISO/IEC 27002?**

  If you didn't know what this is, look it up. *ISO 27002* is just a framework of security controls organizations can use to help improve their security posture. You should have at least a high-level understanding of popular security control frameworks.

- **What is a security control?**

  Security controls are safeguards, parameters, and countermeasures used to protect data, services, and business operations.

- **What are the different types of security controls?**

  There are three main types of security controls:

  - **Technical controls** are also known as **logical controls**. Examples of technical controls include things such as using encryption, ACLs, firewalls, IDS/IPS, SIEM tools, and anti-virus software.
  - **Administrative controls** are policies, procedures, or guidelines that help the organization manage its risk. The implementation of administrative controls is executed by people and is called the **operational controls**.
  - **Physical security controls** include things such as CCTV cameras, alarm systems, security guards, ID scanners, locks, and biometrics.

- **What is information security governance?**

  Information security governance is the accountability framework for security in an organization. In many cases, C-level executives will set the risk appetite for the organization and define compliance and performance objectives. A cybersecurity manager will then identify how to implement security and set risk tolerance so that the organization does not exceed the risk appetite.

- **Are open source projects more or less secure than proprietary ones?**

  This depends on the size of the project, the background of the developers, and the quality controls in place. Many hiring managers are looking for you to list out a few pros and cons for both of them. This shows them you are able to think through projects that might use one or the other.

- **Who do you look up to within the field of information security? Why?**

  Hopefully, you answer *Ken Underhill* for this one, but even if you don't, just know that this question is being asked to see whether you are willing to accept mentorship from more experienced professionals. If you don't have any senior cybersecurity professionals you follow on social media, it could indicate to the hiring manager that you are not that interested in cybersecurity or that you are against taking advice from other team members.

- **How would you find out what a POST code means?**

  Power on self test (**POST**) is a diagnostic check your computer runs during the boot process. Unless you have the beep codes memorized, the answer to this question is simply *I would search online*.

  Some of the POST (beep) codes are as follows:

  - **One beep**: This is a refresh failure, so you might need to check your memory card or the motherboard.
  - **Two beeps**: This is a parity error.
  - **Three beeps**: This is a memory error.
  - **Four beeps**: This is a timer failure.
  - **Five beeps**: This is a processor failure.
  - **Six beeps**: This is a keyboard controller failure.
  - **Seven beeps**: This is a virtual mode exception error.
  - **Eight beeps**: This is a display memory failure.

- **What is the chain of custody?**

  The chain of custody is essentially the paper trail showing who has handled evidence from the time the evidence was collected until the time it is presented in a court of law.

- **Do you prefer filtered ports or closed ports on your firewall?**

  My answer for this one would be closed ports. By closing ports, I limit the attack surface.

- **What is a honeypot?**

  At a high level, a honeypot is designed to attract adversaries so you can see how they are attacking systems. This can help your detection capabilities by helping you understand what actions the threat actor needs to take at each stage of the Cyber Kill Chain for the adversary to be successful in their attack. You can then build detection for those actions and stop attacks.

- **What information security challenges are faced in a cloud computing environment?**

  There are many challenges. A few you should answer with are IAM, security misconfigurations, visibility into your cloud infrastructure and assets, and insider threats.

- **How many bits do you need for an IPv4 subnet mask?**

  Subnet masks are 32 bits for IPv4.

- **What are the layers of the OSI model?**

  I've listed the layers in the list that follows, but you will also want to understand how data flows through these layers and understand what the term *encapsulation* means. I've listed encapsulation as the next question, but typically they (OSI and then encapsulation) will be asked about concurrently in a real job interview:

  - **Layer 1** – The physical layer, which is where raw bitstream is transferred over a physical medium (that is, fiber optic cable, copper cables, and electromagnetic waves).
  - **Layer 2** – The data link layer that controls the transfer of data between nodes on the same LAN segment and contains the sub-layers of **media access control** (**MAC**) and **logical link control** (**LLC**). This layer is where you see the MAC address (example – `ff:ff:ff:ff:ff:ff`) and the information at this layer is labeled as `frames`.

- **Layer 3** – The network layer, which decides what path the data will take. This layer transports and routes the packets across network boundaries. Information at this layer is labeled as a packet and this is where IP routing lives. An example of an **Internet Protocol version 4** (**IPv4**) address at this layer would be `192.168.0.55` and an example of an **Internet Protocol version 6** (**IPv6**) address at this layer would be `2001:0DB6:AC10:FE01:0000:0000:0000:0000` or written in the shorter version `2001:0DB6:AC10:FE01::::`. Some of the protocols at this layer are **Address Resolution Protocol** (**ARP**), **Reverse Address Resolution Protocol** (**RARP**), **Domain Name System** (**DNS**), **Internet Control Message Protocol** (**ICMP**), And **Dynamic Host Configuration Protocol** (**DHCP**).
- **Layer 4** – The transport layer, which transmits the data using protocols such as **Transmission Control Protocol** (**TCP**) And **User Datagram Protocol** (**UDP**). The transport layer is responsible for segmenting the data from applications into a manageable size and the information is labeled as a segment at this layer. The UDP protocol is faster than TCP but it just sends the data and doesn't care whether the data was received on the other end. With TCP, a three-way handshake is established, which allows the sender to know the data was received by the intended recipient.
- **Layer 5** – The session layer, which maintains connections and controls the ports and sessions. The session layer handles the creation, use, and break down of a session. It also handles token management for the session.
- **Layer 6** – The presentation layer, which is where data is presented in a usable format and also where data is encrypted. This layer preserves the syntax of the data that is being transmitted and also handles compression and decompression of the data.
- **Layer 7** – The application layer, where interaction with applications occurs. Some examples of the protocols at layer 7 are **Hypertext Transfer Protocol** (**HTTP**), **Secure Shell** (**SSH**), **File Transport Protocol** (**FTP**), And **Simple Mail Transfer Protocol** (**SMTP**).

- **What is encapsulation?**

  As data moves through the layers of the OSI model, each layer encapsulates the data by adding a header and sometimes a trailer to the data.

> **Note**
> One thing I've noticed before in interviews is that the hiring managers mistakenly think data encapsulation is just encryption of the data. Yes, encryption of the data can occur at the presentation layer, but it doesn't always happen. This goes to show you that *experienced* professionals can still make mistakes on the fundamentals.

- **What are the three ways to authenticate a person?**

  They are as follows:

  - Using something you know, such as your password
  - Using something you have, such as a smart ID card
  - Using something you are, such as a fingerprint

- **What is worse in firewall detection, a false negative or a false positive? And why?**

  A false negative is worse because you don't know that an attack has occurred.

- **What is the primary reason most companies haven't fixed their vulnerabilities?**

  Contrary to what media outlets claim, there could be a number of reasons why a company hasn't fixed vulnerabilities. I would just list out a few and then ask the interviewer whether they want you to go into more detail.

  Many media outlets will state the cost of fixing vulnerabilities is more than the cost of a data breach to the company. This is correct in many cases.

  Another reason might be the company is running legacy applications that don't allow them to update to the latest OS version. I ran into this a few years ago at a healthcare company that was still running the Windows 2000 server.

  There's also the issue of unpatchable vulnerabilities and vulnerabilities that are not a significant risk to the organization.

- **What is the three-way handshake? How can it be used to create a DOS attack?**

  The TCP three-way handshake is a way to establish communication between a client and server. A SYN packet is sent from the client to the server. The server acknowledges the communication (ACK) and also sends back its own SYN packet. The client then confirms receipt with an **ACK** packet.

  That's the simple definition. Some interviewers may want you to go deeper into this where you discuss sequencing.

An attacker can use this for a **denial-of-service** (**DoS**) attack by simply sending a SYN packet to the server. The server will then respond with a SYN/ACK and be waiting for an ACK response from the attacker. Instead, the attacker keeps sending SYN packets and the server's bandwidth is eaten up by its responses to the SYN packets.

- **What are some of the responsibilities of level 1 and 2 SOC analysts?**

  This question helps the interviewer understand how much you know about the role and its common responsibilities.

  Some responsibilities of a level 1 (tier 1) SOC analyst include monitoring for malicious and anomalous behavior in network and system traffic through tools such as SIEMs and IDSs, using ticketing systems, and escalating suspicious activity found to level 2 analysts for review.

  Level 2 (tier 2) SOC analysts perform triaging of alerts using playbooks. Level 2 analysts may also tune the collection tools to help reduce false positives and use the MITRE ATT&CK framework (`https://attack.mitre.org/`) to identify security gaps in the organization's defensive posture. At this level, you will also remove malware from end user systems and write YARA rules to detect and stop future attacks.

- **What are the steps to building a SOC?**

  This is normally a question asked as a more senior level 2 or 3 SOC analyst. A goal here is to see how you would use your knowledge and experience to architect a SOC from the ground up. The steps to building a SOC include the following:

  1. Develop your SOC strategy: The key to developing your strategy is to understand the current state of your organization and perform the following:

  - Assess your existing capabilities.
  - Delay non-core functions until your core functions are sufficiently mature.
  - Identify and define business objectives from stakeholders.

  2. Design your SOC solution:

  - Choose a few business-critical use cases (for example, a phishing attack).
  - Define your initial solution based on these use cases.
  - Consider that your solution must be able to meet the future needs of the organization.

Remember, a narrow scope will help reduce the time to initial implementation, which will help you achieve results faster.

3. Create processes, procedures, and training:

- Identify and analyze threats to determine the nature and extent of risk to the organization.
- Implement countermeasures to mitigate threat actors and the associated risk.

4. Prepare your environment before deploying the SOC:

- Ensure SOC staff desktops, laptops, and mobile devices are secured.
- Limit remote access for SOC staff (and third parties if applicable).
- Require MFA for all accounts.

5. Implement your solution and leverage technology where applicable:

- Deploy your log management infrastructure.
- Onboard your minimum collection of critical data sources.
- Deploy your security analytics capabilities.
- Deploy your **Security orchestration, automation and response** (**SOAR**) solution.
- Begin deploying use cases to focus on end-to-end threat detection and response.
- Incorporate threat intelligence feeds.
- Employ detection engineering.
- Incorporate automation.

6. Implement and test your use cases:

- Test your use cases.
- Analyze the security and reliability of your security solution.

7. Maintain and improve your SOC:

- Tune to improve detection accuracy.
- Add other systems as inputs or outputs.
- Review the SOC, SOC roles, and staff counts.

- **What is data protection in transit versus data protection at rest?**

  The protection for the data in both of these scenarios is to encrypt the data. As the name implies, data protection in transit just means you are protecting the data from end to end while it's being transmitted. Data at rest just means the data is protected while it is being stored.

- **Is it an issue to give all users administrator-level access?**

  Yes, this is an issue, and you will want to implement the principle of least privilege as part of IAM.

- **How do you protect your home WAP?**

  Turn off broadcasting of your SSID, update the firmware, change the default credentials, and use strong and unique passwords and MFA.

- **How can you tell whether a remote server is running IIS or Apache?**

  You can run a simple scan with a tool such as *Nmap* to see what it is running and the version. You could also do banner grabbing.

- **How often should you perform patch management?**

  This depends on a number of factors. Some patches might need to be applied immediately, while you might cycle others on a specific date. Microsoft has its famous Patch Tuesday, but not all organizations implement patches on this day. It's usually best to test patches on non-production systems and networks, so you can identify whether the patch is breaking anything else.

- **What is Docker?**

  Docker uses OS-level virtualization and delivers infrastructure as code through containers. What does this mean? It means you can run a virtualized infrastructure at low or no cost on just about any computer you have. What does this mean for a company? It usually means significant infrastructure savings.

- **Are VXLANs scalable?**

  Yes, VXLANs are used for their scalability in comparison to using a traditional VLAN for network segmentation.

- **What is the difference between TCP and UDP?**

  TCP is connection-orientated and UDP is a connectionless protocol. This means TCP will attempt to establish the three-way handshake. UDP is usually faster than TCP communication.

- **What is a playbook/runbook in SOC?**

  A playbook, also known as a **standard operating procedure** (**SOP**), consists of a set of guidelines to handle security incidents and alerts in the SOC. For example, if credentials were compromised, the playbook would help the level 1 SOC analyst know what actions they should take.

- **What is the difference between firewall deny and drop?**

  If the firewall is set to a **deny rule**, it will block the connection and send a reset packet back to the sender. This alerts the sender that there is a firewall being used.

  If the firewall is set to a **drop rule**, it will block the connection request without notifying the sender. It is recommended that you configure the firewall to deny egress (outbound) traffic and set the incoming traffic to just drop, so an attacker doesn't know you are filtering the traffic with a firewall.

- **Explain the different SOC models.**

  There are three types of models in SOC:

  - An in-house model, where all the resources, technology, processes, and SOC employee training are managed within the organization.
  - A **managed security service provider** (**MSSP**), where a third-party security service provider manages all of the resources, technology, processes, and training of SOC staff.
  - A hybrid SOC model, where level 1 is outsourced to an MSSP and then the organization has level 2 and above in-house. Many large companies use this model.

- **What is DNS?**

  DNS is basically the phone book (I might be giving my age away with this example) of the internet. As an example, let's say that you type `google.com` in your browser and the domain name (`google.com`) is then translated to an IP address (`192.168.0.1` for this example) for Google's servers so you can see the information on their website. This eliminates the need for you to memorize every server IP address of Google.

There are four DNS servers involved in your request to access Google's web page:

- The **DNS recursor** receives queries from clients and then makes any additional requests to satisfy the client's DNS query. This is similar to you requesting a book from the library and the librarian looking up the shelf that the book is on and then handing the book to you.
- The **root nameserver** is the first step in translating human-readable information (that is, `google.com`) into an IP address. Using our library analogy, this is like the index card that tells you the book is in the non-fiction section. Using our `google.com` example, this nameserver would tell you that the web page you want is in the *Google* section of the library.
- The **top-level domain** (**TLD**) nameserver is the next step and hosts the last portion of the hostname (`.com` in our `google.com` example). In our library example, this would be the librarian telling you that the book is on shelf 12 of the *Google* section.
- The **authoritative** nameserver can be thought of as the master index card that tells you specifically where the book is in the library.

One thing to keep in mind is that DNS uses multiple servers and not a single server.

- **You receive an email from your bank stating that there is a problem with your account. The email states you need to log in to your account to verify your identity and even provides a link to your bank. If you don't verify your identity, the email states that your account will be frozen. Tomorrow is payday and you need to pay your rent that is past due via a wire transfer in the morning. What should you do?**

  This is a simple phishing attack, and the question is designed to test your general knowledge of phishing since you might have end users calling the SOC with this issue. In this example, you should not click any links or documents in that email. Instead, visit the bank's website URL directly or call your bank. You should also change the password for your bank account. Most banks don't typically contact you via email if there is an issue with your account.

  After answering this question, you can ask the interviewer whether they need you to explain what phishing is.

- **A friend of yours sends you an e-card via email. To view the e-card, you have to click on an attachment. What do you do?**

  The answer is you don't click anything. Your friend's email address could have been spoofed and/or the attachment could be infected, and your friend simply didn't realize that before sending it to you.

- **You are a new level 1 SOC analyst and receive a call from the IT helpdesk to ensure you can access all systems. The IT helpdesk person is friendly to you and asks you to confirm your password, so they can verify you meet the minimum complexity requirements. What do you do?**

  This is a **vishing** (**phishing via phone**) attack. One part of this answer is to hang up the phone, but before you do, I would try to get as much information as possible from the individual. I've had this happen before and I was able to get a postal mailing address (I told them I wanted to personally mail them a thank you card for being so helpful) out of the individual. The mailing address turned out to be a mailbox at a UPS store, but it was an additional clue for law enforcement to hopefully catch the criminal calling me.

- **What is cognitive cybersecurity?**

  Cognitive cybersecurity is the application of **artificial intelligence** (**AI**), patterned on human thought processes, to detect threats and protect physical and digital systems. It uses data mining, pattern recognition, and natural language processing to simulate the human brain.

- **What is the difference between SIEM and IDS systems?**

  SIEM and IDS systems collect log data.

  SIEM tools facilitate event correlation to identify patterns that might indicate an attack has occurred, and centralize log data.

  IDS tools also capture log data but do not facilitate event correlation. The purpose of an IDS is to detect an intrusion and alert on the intrusion.

- **What is port blocking?**

  The answer is simply blocking ports. It's helpful to block unnecessary ports so you can reduce the attack surface. One thing to keep in mind though is that many threat actors just use ports they know will always be open (HTTPS on port `443` as an example).

- **What is ARP and how does it work?**

  Address Resolution Protocol (**ARP**) is a protocol for mapping an **Internet Protocol address** (**IP address**) to a physical machine address that is recognized in the local network.

How does it work?

I. When an incoming packet is destined for a host machine on the LAN at the gateway, the gateway asks the ARP program to find the physical host or MAC address that matches the IP address.

II. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the host machine.

III. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see whether one machine knows that it has that IP address associated with it.

- **What is port scanning?**

  Port scanning is a technique used to identify open ports and services available on a host. A threat actor can use port scanning to identify services running and identify vulnerabilities that can be exploited. A network administrator might use port scanning to verify the security policies set on the network. **Nmap** is a popular tool that can be used for port scanning.

- **A senior executive approaches you and demands that you break security policy to let her access a social media website. What do you do?**

  In this situation, I would ask why they need the access and then explain that it is against the security policy. If the executive persists, I would suggest getting your leadership team involved. Many companies have a formal process for one-off requests like this to be reviewed and approved.

- **Why would an organization bring in an outside consulting firm to perform a penetration test?**

  A couple of reasons are as follows:

  - It might be a requirement for compliance.
  - You can tap into the broad skill set and expertise of the consulting firm without needing a full internal pen-testing team.

- **What is an insider threat?**

  Insider threats are security risks that originate within the organization. They are anyone that has access to the organization's infrastructure or insider knowledge and/or access to sensitive data for the organization. Insider threats could be a third-party contractor, an executive, or a janitor. This is why they are difficult to protect against.

Not every insider threat is malicious in nature. You typically have two main types of insider threats:

- **Turncloaks** are the ones you likely think of, and they are the ones stealing data or performing malicious actions to harm the organization.
- **Pawns** are your everyday employees who are exploited by a threat actor or who make a mistake. Some examples include an employee who leaves their work laptop at the local coffee shop, which leads to data theft, and an employee falling for a vishing attack, where they reveal their login credentials to the *IT helpdesk* person on the phone.

The 2019 Verizon **Data Breach Investigation Report** (**DBIR**) showed over 30 percent of data breaches were the result of an insider threat.

It's also good in a job interview to cite some stats from the DBIR or the Ponemon Cost of a Data Breach Report. These show the interviewer that you are aware of industry reporting and trends.

- **What is a residual risk?**

  Residual risk is the risk that remains after you implement security controls.

- **What is data loss prevention (DLP)?**

  DLP tools are used to make sure that users are not sending sensitive data outside of the internal network.

  Best practices for DLP include identifying data, classifying it, prioritizing it, understanding the risks to the data, monitoring data in transit, and creating controls to protect the data. You will also want to train your employees because many will not understand how their actions can result in data loss.

- **What is an incident response plan?**

  IR plans ensure that the right people and procedures are in place to deal with threats. This allows your IR team to perform a structured investigation into events to determine the **indicator of compromise** (**IOC**) and the **tactics, techniques, and procedures** (**TTPs**) of the threat actor(s). An IR plan is like a step-by-step guide to follow if an incident occurs; however, you might jump around through different phases of the Kill Chain depending on the incident.

  NIST 800-61 is a good resource for you to learn about the different phases of incident handling and you will likely be asked some questions on 800-61 for job interviews.

I've listed the phases as follows:

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activity

General attack knowledge questions

In this section, you will see some of the attack knowledge questions that might be asked in a SOC analyst interview:

- **What is a botnet?**

  A botnet is composed of hijacked computers that are used to perform a number of tasks, including attacks such as a DDoS. Some notable botnet infrastructures are Mirai, which hijacked IoT devices, and Emotet.

- **What are the most common types of attacks that threaten enterprise data security?**

  The answer to this will change as time progresses and new threats emerge but in general, it includes things such as malware/ransomware, DDoS/DoS attacks, phishing/**business email compromise** (**BEC**), credential stuffing, and web application attacks.

- **What is XSS and how can you mitigate it?**

  Cross-site scripting (**XSS**) is a JavaScript vulnerability in different web applications. There are different types of XSS, including reflected and stored XSS. For reflected XSS, a user enters a script on the client side and this input gets processed without getting validated. This means the untrusted input is executed on the client side, typically through the browser.

  For stored XSS, a malicious script is injected directly into a vulnerable web application and executed. This means any user visiting the web app server will be infected, even if they clear their browser cache.

- **What is CSRF?**

  Cross-site request forgery (**CSRF**) is a vulnerability in web applications where the server does not validate the request as being from a trusted client. In layperson terms, let's say you are authenticated and logged into your banking website. If the bank's site doesn't have CSRF protection, an attacker could take over your session and send requests to the bank, such as transferring the money from your account to their account.

SOC tool questions

In this section, you will see questions on common SOC tools. Please note that this list will not contain every tool and that it's more important for you to understand what the different types of tools used in a SOC are versus knowing how to use every vendor tool. It's also important to note that the answers to these questions may change as tools are updated with new features:

- **What is Splunk?**

  Splunk is a SIEM tool that is used for searching, visualizing, monitoring, and reporting data. It offers real-time insight into your data. A key thing to remember for any tool question is you should know what that type of tool does at a high level. Splunk is just one brand of tool, so it's more important for you to understand what a SIEM tool is and what it does.

- **Why is Splunk used for analyzing data?**

  It offers business insights, which means it understands patterns hidden within data and turns them into real-time business insights that can be used to make informed business decisions. This is key because there is so much data to sift through in a typical enterprise and it's important to gain actionable insights into the data. It also provides visibility into your operations and proactive monitoring.

  Your answer here should be clear and concise on a few of the value props of Splunk or another SIEM tool. You can always ask the interviewer whether they would like you to provide more context or information.

- **What do SOAR solutions provide that SIEM tools usually don't?**

  SOAR tools provide orchestration, automation, responses, and collaboration. They also allow the company to integrate multiple resources into a single location. Many larger companies build their own custom SOAR tools that are optimized for their environment.

- **Which of the following use a user's behavior as part of their process to determine anomalous behavior on a network?**
  - EDR tools
  - SIEM tools
  - SOAR tools
  - UEBA tools

  The answer is UEBA tools. **UEBA** stands for **user and entity behavior analytics**. These tools are used to detect attacks faster by aggregating data from on-premises and the cloud and from multiple devices to detect anomalous behavior on the network that might be seen when an attacker moves into lateral movement.
- **Which components listed are seen with many next-gen SIEM solutions, but not traditional SIEMs?**
  - Threat intelligence feed
  - EDR
  - SOAR
  - UEBA

  UEBA and SOAR are often seen in next-generation SIEM solutions.
- **Select all of the SIEM tools from the following:**
  - Splunk
  - QRadar
  - Cisco ASA
  - Microsoft Sentinel

  The only one listed that is not a SIEM tool is Cisco ASA, which is a firewall.

As you can see, many interview questions as a SOC analyst are around attack types and fundamental knowledge of SIEM tools. The good news is that many companies are only looking for you to have knowledge of attacks and how threat actors might attack the organization as a tier 1 SOC analyst (entry level). I would also suggest you explore the MITRE ATT&CK framework to think through how organizations can use it operationally to build detection logic in their SIEM tool and how it can be used strategically by the organization to identify gaps in their security posture.

Summary

In this chapter, you learned about the SOC analyst career and the average salary range in the United States. You also learned how this can be a stepping stone into other cybersecurity careers and you learned common interview questions asked for SOC analyst roles.

In the next chapter, you will learn about a career as a penetration tester, including common knowledge-based interview questions you might be asked.