

SOC Incident Response Interview Questions

1. **“You are a tier 1 SOC analyst, responsible for monitoring the SOC inbox for user-reported incidents. The SOC receives an email from the VP of Human Resources stating that they can’t access their personal cloud drive. The VP knows this against company policy, but the VP is adamant that this is required for legitimate business requirements.”**
 - a. Do you process the access request for the VP?
 - b. What is your response to the VP?
 - c. Who else should you include in the reply email?
2. **“You are monitoring the SIEM dashboard for new security events. A network IDS alert is triggered, and you begin investigating. You see a large amount of network traffic over UDP port 161 originating from dozens of internal IP addresses, all with the same, internal destination IP address. Some quick Googling shows that UDP port 161 is used for by the Simple Network Management Protocol and the byte count of the traffic is miniscule.”**
 - a. Do you think this is data exfiltration?
 - b. If this is not data exfiltration, what legitimate services could cause this alert?
 - c. What team could provide an explanation for the traffic?

3. What is an investigation methodology?

An investigation methodology is a framework or guidelines that gave you instruction or point you a direction at what you should do during an investigation. Describe what I will do, what tool I will use.

Example:

- a. First step
 - Determine the severity
 - CVSS Common Vulnerability Scoring System
 - Assessing
 - What happens?
 - When?
 - How?
 - What did you do?
 - When did you notice?
 - Create the timeline
 - How many people affected?
 - What is the effect / lost / impact?
 - What's the impact for doing OOOX (Shut down X system)?
- b. Second step
 - If life & death incident > move all the living away
 - Look into the logs
 - Collect the logs
 - Stop the incident from spreading (contain / isolate / shutdown)
 - Impact analysis / damage analysis
- c. Third step
 - Start investigation
 - Collect the logs

- Firewalls, IDS/IPS, web app, web server, server logs
- Container > docker engine logs, K8s logs
- Collect whatever is available
- Analyze the logs
 - What will you do?
 - If SIEM, mention the tools; Splunk, AlienVault, QRadar
 - Utilize the SIEM, correlate the logs
 - Create the chain of events
 - Find answers for Who What When Why How

4. If there is a suspicious network security event found and you are assigned to investigate:

- a. What will you first do?
 - Depends on the severity of the event, I will either isolate the system or start collecting information I need.
- b. What will you need to do?
- c. I'll need to notify proper personnel who is in charge, escalate the severity of the event if needed, document every event and the time it happened.
- d. What info do you need?
 - If possible, I'll try to collect every information that I can get. If not, I'll try to get at least the logs from security devices like IDS or SIEM and make sure they are properly timestamped.
- e. What's your plan to investigate?
 - I'll follow the incident response procedure that I learnt in CISSP, which is notification, escalation, reporting, system isolation, forensic analysis, evidence handling
- f. Who do you need to talk to?
 - Manager of the security operation team, the manager of the system where the event happened, and legal counsel if required
- g. Ask: who do I work for?
 - System owners, all the people that are impacted
- h. What results should you show?
 - A timeline of when each events happened and how each of them are related, also provide a brief information about what the impact might be if possible
 - What action has been taken, how to prevent things from happening again, find root cause to fix the problem
- i. How long is an investigation going to take?
 - It depends on the size and the complexity of the event
 - Depends on many things and how much resource do I have
- j. How do you know if it's a true incident or not?
 - It will be evaluated by all the actions made by the attacker along with the all the information we gather, basically it will be determined by experience
 - IoC / IoA (Indicator of Compromise / Indicator of Attack)
 - Look for indicator / evidence by going through logs and SIEM
- k. How do you determine the chain of events happened in an incident?
 - By finding some related parts in the information that we gathered, for example, a same source IP may indicate that two events are done by a same user.
 - Find evidence in logs that we gathered
- l. What open-source tools will you use to investigate an incident?

- I might be using a SIEM which can aggregate logs from different resource and virtualize the information, it will be able to help us find correlation between different log sources
 - System internals (for Windows)
 - Process explorer
 - TCP Viewer, see open ports and activities
 - Image dump, use sandbox to restore image and investigate
- m. What scripts will you likely write or have you written to help you investigate an incident?
- I will be writing some scripts that can identify some malicious activities and notify for me, for example, it may be finding a source IP that had sending requesting more than 10 times in a second.
- n. When do you consider the Investigation is done/complete?
- When we find the answer for the reason why we did this investigation, or when the cost of the investigation is exceeding the value of knowing the result of this investigation.
 - When the budget time is up
 - If we cannot move further > cannot find any evidence, may close the case or move to 3rd party investigation
- o. What do you do when the investigation is complete?
- Document everything and make sure is preserved for reference in the future if similar incidents happen
- p. How do you identify indicators of attack and create effective monitoring and alerting?
- Finding the root cause of the attack and see if there's any characteristic that will only appears in this type of attack, after identified the indicators of attack, I'll see if I can create firewall rules or filters to keep an eye on similar incidents that happens in the future
- q. What is Indicator of attacks? Name a few...
- Hash of a malware, known malicious source IP, unauthorized access attempts
- r. What do you do for post-mortem / lessons learned Report?
- I'll see if there's anything that we can do to help prevent similar incidents from happening again, some examples will be like firewall rules or even policy and guidelines.
 - What is the root cause

5. Often there will be stress to investigate suspected serious security incident in a tight timeline, if you only have limited info to start with, but you are required to get this analysis done in 2 days,

- a. What will you plan to do for 2 days?
- I will try to set out some goals and list the tasks that need to be done then prioritize them and start with the most important tasks.
- b. What will you plan to deliver in 2 days?
- I will be hoping to provide at least a broad picture of the incident and includes some direction of what future works can be done
- c. What if you don't have enough info to start with?
- I will be seeking for helps from others and see if we can gather information that might be able to provide us a different view that we can start with
- d. What if you can't get the report done in 2 days?
- I will provide a report of what I've done and what is currently is doing, at the same time kept on working with the investigation
- e. How often will you provide update before the deadline is up?

- I will be providing updates when any of the goals are reached or tasks are done
- f. What resources will you need?
- I will need all the logs with timestamps of the systems and devices that are related to the incident, I might also need some help from engineers of the system who have better understand about the system and how incident like that might happens.

6. How do you conduct an in-depth vulnerability assessments and information system auditing of assets (e.g., servers, Workstations, Network Appliances, Storage Devices, and Applications)?

- What is the methodology?
- What info do you need to start the assessment?
- What tools do you use to conduct a vulnerability assessment?
- What are the key items you need to ask / define before starting a vulnerability assessment? What is considered as a vulnerability in your opinion?
- If you find a vulnerability and you are not sure if it is exploitable, what will you do? What is the difference between penetration testing vs Vulnerability Assessment? What should you include in a vulnerability assessment report?
- Example
 - Ask questions: What is the scope?
 - What do you want me to assess?
 - When do you want me to do the test? Date? Time? Is this live system or testing system?
 - Is there a backup?
 - Black box? Grey box? White box? Rule of engagement?
 - Can I do OOOX attack?
- Report example
 - Executive summary
 - What did I do
 - When I start / end
 - The scope of assess
 - What test I ran
 - What I found
 - The servility of the things I found
 - Methodology
 - How did I do it
 - What tools I used
 - Vulnerabilities
 - Description of the vulnerable
 - what I found
 - How to recreate the issue (include all the steps)
 - If you cannot recreate it, it's not an issue
 - Actual risk / actual impact

Common Questions

1. You've identified an active C2 channel in your network. What do you do?
2. How do you stay up to date with the latest cyber security news?
3. Tell me about some recent vulnerabilities and why they caught your attention in the last six months.
4. Describe in as much detail as possible what happens when you type google into the address bar if your browser and hit enter
5. Are you familiar with ATT&CK? Tell me a little bit about it.
 - <https://attack.mitre.org/>
6. What is considered as an investigation?

An act of spending time and/or effort trying to find more information or an answer or a thing
7. What is a Cybersecurity event vs incident?
 - An event will be anything that happens related to cybersecurity, incident, will be an event that may cause damage or create risk to assets
8. How do you use Python to write log parsers and/or utilities in scripting languages?
9. What is DevOps? Why is it useful?
 - DevOps is a methodology that combines the software development part and the technology operation part. It makes software delivering, fixing bugs and providing updates easier and faster for both developer and operator
10. Define a Class A, B, or C network.
11. What are the seven phases of the cyber kill chain?
12. What is the purpose of the Mitre ATT&CK Framework?
13. What is the difference between TCP and UDP?
14. What are ports 80, 443, 22, 23, 25, and 53?
15. What is data exfiltration?
16. What Windows protocol is commonly used for data exfiltration?
17. Do you have a home lab? Explain it.
18. What is AWS? Explain how you've used it.
19. What is a DMZ, and why is it a common target for cyberattacks?
20. How do you automate tasks?