CYBER SECURITY ANALYST INTERVIEW SESSION SIMULATION

BY IZZMIER IZZUDDIN

INTRODUCTION

Interviewer: Hi [Candidate's Name], welcome to the interview. How are you doing today?

Candidate: I'm doing well, thank you. How are you?

Interviewer: I'm good, thanks. Could you start by telling me a little bit about yourself and your background in cybersecurity?

Candidate: Certainly. My name is [Candidate's Name], and I have a degree in [Your Degree] from [Your University]. I have been working in the cybersecurity field for [X] years, starting as a cybersecurity analyst L1. During this time, I've been involved in monitoring and responding to security incidents, performing vulnerability assessments, and working with SIEM tools such as QRadar. I'm currently working at [Company name] in [Location], focusing on cybersecurity customer success and incident response.

Interviewer: That's great. Can you tell me more about your current role at [Company name] and what your day-to-day responsibilities are?

Candidate: In my current role at [Company name], I am responsible for [Elaborate your job scope].

Interviewer: It sounds like you have a lot of experience in different areas of cybersecurity. Before we dive into the technical questions, could you tell me what interests you the most about working in cybersecurity?

Candidate: What I find most interesting about working in cybersecurity is the constantly evolving nature of the field. There are always new threats and challenges, which require continuous learning and adaptation. I enjoy the problem-solving aspect of identifying and mitigating risks, as well as the opportunity to work on different projects, such as vulnerability assessments, incident response, and compliance. It's a field where you can make a significant impact by protecting valuable information and systems from potential threats.

Interviewer: That's a great perspective. Now, let's move on to some cybersecurity general knowledge and technical questions to understand your expertise further.

GENERAL CYBERSECURITY KNOWLEDGE

Interviewer: Welcome to the interview. Let's begin with some general cybersecurity knowledge. Can you explain the CIA Triad?

Candidate: The CIA Triad stands for Confidentiality, Integrity, and Availability. Confidentiality ensures that sensitive information is accessed only by authorized individuals. Integrity ensures that the information is accurate and has not been

tampered with. Availability ensures that information and resources are accessible to authorized users when needed.

Interviewer: Great. What is the difference between a vulnerability, a threat, and a risk?

Candidate: A vulnerability is a weakness in the system. A threat is a potential cause of an unwanted impact on the system, such as a hacker or malware. Risk is the potential for loss or damage when a threat exploits a vulnerability. It's typically assessed as a combination of the likelihood of the event and the impact of the event.

NETWORK SECURITY

Interviewer: Moving on to network security, what is a firewall, and how does it work?

Candidate: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted network and an untrusted network, allowing only authorized traffic to pass through and blocking malicious traffic.

Interviewer: Explain the differences between TCP and UDP.

Candidate: TCP (Transmission Control Protocol) is connection-oriented, meaning it establishes a connection before transmitting data and ensures that data is delivered in the correct order and without errors. UDP (User Datagram Protocol) is connectionless and does not guarantee delivery, order, or error-checking. TCP is used for applications where reliability is crucial, like web browsing and email, while UDP is used for applications where speed is more important than reliability, like video streaming and online gaming.

Interviewer: What is an IDS/IPS, and how do they differ?

Candidate: An IDS (Intrusion Detection System) monitors network traffic for suspicious activity and alerts the administrator when such activity is detected. An IPS (Intrusion Prevention System) not only detects suspicious activity but also takes action to prevent it, such as blocking traffic from a malicious IP address.

Interviewer: Describe how a VPN works and its purpose.

Candidate: A VPN (Virtual Private Network) creates a secure, encrypted connection over a less secure network, typically the internet. It allows users to send and receive data as if their devices were directly connected to a private network, providing privacy and security by encrypting the data traffic.

Interviewer: What are the common ports for HTTP, HTTPS, FTP, SSH, and DNS?

Candidate: HTTP: 80, HTTPS: 443, FTP: 21, SSH: 22, DNS: 53.

THREATS AND ATTACK VECTORS

Interviewer: Let's talk about threats and attack vectors. What is a phishing attack, and how would you prevent it?

Candidate: A phishing attack is a type of social engineering attack where an attacker sends fraudulent emails or messages pretending to be a legitimate entity to trick individuals into revealing sensitive information, such as passwords or credit card numbers. To prevent phishing attacks, users should be educated to recognize suspicious emails, organizations should use email filtering technologies, and multifactor authentication should be implemented to add an extra layer of security.

Interviewer: Describe the difference between a virus, worm, and Trojan horse.

Candidate: A virus attaches itself to a legitimate program and spreads when the infected program is executed. A worm is a standalone malware that replicates itself to spread to other computers without user intervention. A Trojan horse disguises itself as a legitimate program but contains malicious code that can cause harm once executed.

Interviewer: What is a DDoS attack, and how can you mitigate it?

Candidate: A DDoS (Distributed Denial of Service) attack involves overwhelming a network or service with a flood of traffic from multiple sources, causing it to become unavailable to legitimate users. Mitigation techniques include using firewalls and intrusion prevention systems, deploying DDoS protection services, and having a response plan to quickly address the attack.

Interviewer: Explain SQL Injection and how to prevent it.

Candidate: SQL Injection is an attack where malicious SQL statements are inserted into an entry field for execution, allowing attackers to access or manipulate the database. Prevention methods include using parameterized queries or prepared statements, validating and sanitizing user inputs, and employing proper error handling to avoid revealing database information.

Interviewer: What is a Man-in-the-Middle (MitM) attack?

Candidate: A Man-in-the-Middle (MitM) attack occurs when an attacker intercepts and potentially alters the communication between two parties without their knowledge. This can be prevented by using encryption protocols like SSL/TLS for secure communication, employing strong authentication methods, and avoiding unsecured public Wi-Fi networks.

INCIDENT RESPONSE

Interviewer: What steps would you take in responding to a security incident?

Candidate: First, I would identify and contain the incident to prevent further damage. Then, I would gather and analyse relevant data to understand the scope and impact of the incident. Next, I would eradicate the root cause, such as removing malware or patching vulnerabilities. After that, I would recover affected systems and data, ensuring they are secure. Finally, I would document the incident, perform a post-incident review to improve future response, and implement measures to prevent recurrence.

Interviewer: How do you handle false positives in a SIEM system?

Candidate: Handling false positives involves tuning the SIEM system to reduce noise while ensuring true threats are detected. This can be done by refining correlation rules, creating more specific filters, and leveraging threat intelligence feeds to distinguish between benign and malicious activity. Regularly reviewing and adjusting the system based on incident response feedback is crucial to maintaining an effective balance.

Interviewer: Describe the importance of log analysis in incident response.

Candidate: Log analysis is crucial in incident response because it helps identify the source and nature of an attack, track the actions of an attacker, and determine the extent of the compromise. By analysing logs, responders can reconstruct events, detect anomalies, and gather evidence for remediation and legal purposes.

Interviewer: Explain the steps you would take to investigate a suspected malware infection.

Candidate: First, I would isolate the affected system to prevent the malware from spreading. Next, I would run a full malware scan using reputable antivirus or antimalware tools. I would then analyse system and application logs to identify suspicious activities or changes. Additionally, I would review running processes, services, and network connections for signs of malware. Once the malware is identified, I would remove it, restore affected files from backups if available, and update security measures to prevent future infections.

SECURITY TOOLS AND TECHNOLOGIES

Interviewer: What is a SIEM, and why is it important in cybersecurity?

Candidate: A SIEM (Security Information and Event Management) system collects, correlates, and analyses security event data from various sources across the network to detect and respond to security incidents in real-time. It is important because it provides a centralized view of the security posture, enables the detection of sophisticated threats, and supports compliance reporting and forensic investigations.

Interviewer: Describe your experience with any EDR (Endpoint Detection and Response) tools.

Candidate: In my previous role, I used EDR tools such as CrowdStrike and Carbon Black. These tools provided real-time monitoring, threat detection, and response capabilities for endpoints. I used them to investigate suspicious activities, contain and remediate threats, and perform forensic analysis to understand the root cause of incidents.

Interviewer: What is penetration testing, and how is it different from vulnerability scanning?

Candidate: Penetration testing involves simulating real-world attacks to identify and exploit vulnerabilities in a system, providing a comprehensive assessment of the security posture. It is typically conducted manually by skilled testers. Vulnerability scanning, on the other hand, is an automated process that scans systems for known vulnerabilities and provides a report. Penetration testing is more thorough and provides insights into potential attack vectors, while vulnerability scanning is quicker and helps identify common vulnerabilities.

Interviewer: Explain the purpose of using multi-factor authentication (MFA).

Candidate: Multi-factor authentication (MFA) enhances security by requiring users to provide two or more verification factors to gain access to a system. This reduces the risk of unauthorized access, even if one factor, such as a password, is compromised. Common factors include something the user knows (password), something the user has (security token or smartphone), and something the user is (biometric verification).

OPERATING SYSTEMS AND APPLICATIONS

Interviewer: How do you secure a Windows/Linux server?

Candidate: Securing a Windows/Linux server involves several steps: keeping the operating system and applications up to date with the latest patches, configuring firewalls to control access, using strong authentication methods, disabling unnecessary services and ports, implementing least privilege access controls, enabling logging and monitoring, and performing regular backups. Additionally, employing security tools like antivirus, intrusion detection/prevention systems, and vulnerability scanners helps ensure the server remains secure.

Interviewer: What are some common security practices for web applications?

Candidate: Common security practices for web applications include input validation and sanitization to prevent injection attacks, using HTTPS to encrypt data in transit, implementing strong authentication and authorization mechanisms, regularly updating and patching software, conducting security testing such as penetration testing and

code reviews, employing security headers, and monitoring and logging application activities.

Interviewer: Describe the concept of least privilege and its importance.

Candidate: The principle of least privilege involves granting users and systems the minimum level of access required to perform their tasks. This reduces the risk of accidental or malicious actions that could compromise security. By limiting access rights, organizations can minimize the potential damage from compromised accounts or systems and improve overall security posture.

Interviewer: What are common methods to secure databases?

Candidate: Common methods to secure databases include enforcing strong authentication and access controls, encrypting sensitive data at rest and in transit, regularly applying patches and updates, implementing database activity monitoring and auditing, using firewalls to restrict access, and performing regular backups. Additionally, configuring database permissions according to the principle of least privilege and conducting security assessments help ensure database security.

REAL-WORLD SCENARIOS AND PROBLEM-SOLVING

Interviewer: You receive an alert about unusual outbound traffic from a server. How would you investigate?

Candidate: First, I would review the alert details to understand the nature and scope of the traffic. Then, I would examine the server logs to identify any unusual activity or connections. Next, I would check the running processes and services on the server for any suspicious behaviour. I would also investigate the destination IP addresses to determine if they are known malicious sites. Finally, I would isolate the server if necessary and conduct a thorough forensic analysis to identify and remove any malware or threats.

Interviewer: A user reports their system is behaving strangely and files are disappearing. What steps do you take?

Candidate: I would start by isolating the affected system to prevent further potential spread of any malware. Then, I would gather information from the user about the symptoms and timeline. I would perform a full malware scan and check for any suspicious processes or services. Additionally, I would review system and application logs for any unusual activity. Once the cause is identified, I would remove the malware, recover any lost files from backups if available, and take steps to prevent future incidents, such as updating security software and educating the user.

Interviewer: How would you handle a data breach involving customer information?

Candidate: First, I would contain the breach to prevent further data loss. Then, I would conduct a thorough investigation to determine the scope and impact of the breach, identifying how it occurred and what data was compromised. Next, I would notify affected customers and regulatory authorities as required. I would work on eradicating the root cause, such as patching vulnerabilities or strengthening security controls. Finally, I would review and improve security policies and procedures to prevent future breaches and perform a post-incident analysis to learn from the incident.

Interviewer: Explain how you would secure a network after detecting unauthorized access.

Candidate: First, I would isolate the affected systems to prevent further unauthorized access. Then, I would investigate the incident to determine the entry point and scope of the intrusion. Next, I would implement measures to remove any malicious presence, such as resetting compromised credentials, patching vulnerabilities, and deploying security updates. I would also review and update firewall rules, access controls, and network segmentation to enhance security. Additionally, I would monitor the network for any signs of lingering threats and perform a post-incident analysis to strengthen the network's defences.

REGULATIONS AND COMPLIANCE

Interviewer: What is ISO/IEC 27001, and why is it important?

Candidate: ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. It is important because it helps organizations protect their information assets, comply with legal requirements, and gain trust from customers and partners.

Interviewer: Explain the basics of NIST and its relevance to cybersecurity.

Candidate: The National Institute of Standards and Technology (NIST) provides a framework and guidelines for improving critical infrastructure cybersecurity. The NIST Cybersecurity Framework (CSF) includes best practices for managing and reducing cybersecurity risks. It is relevant because it helps organizations develop robust cybersecurity programs and align their security practices with industry standards.

Interviewer: What is the purpose of PCI DSS compliance?

Candidate: PCI DSS (Payment Card Industry Data Security Standard) compliance aims to protect cardholder data by establishing a set of security standards that organizations must follow when processing, storing, or transmitting credit card information. It helps prevent data breaches and fraud by enforcing controls such as secure network configurations, encryption, access controls, and regular monitoring and testing of systems.

BEHAVIORAL AND SITUATIONAL QUESTIONS

Interviewer: Describe a time when you had to explain a technical concept to a non-technical person.

Candidate: In my previous role, I had to explain the importance of multi-factor authentication (MFA) to our HR department. I used a simple analogy, comparing MFA to a two-lock system on a door. I explained that just as having two locks on a door provides better security than one, MFA adds an extra layer of security beyond just a password. This helped them understand the concept and the importance of implementing MFA for protecting sensitive employee information.

Interviewer: Give an example of a challenging cybersecurity problem you faced and how you resolved it.

Candidate: In a previous role, we faced a ransomware attack that encrypted several critical systems. My team and I quickly isolated the affected systems to prevent further spread. We then identified the ransomware strain and used available decryptor tools to recover some of the encrypted files. For the remaining files, we restored from backups. After recovery, we conducted a thorough investigation to identify how the ransomware entered our network and implemented additional security measures, such as improved email filtering and user training, to prevent future attacks.

Interviewer: How do you stay current with cybersecurity trends and developments?

Candidate: I stay current by subscribing to cybersecurity news websites and blogs, participating in online forums and professional networks, attending webinars and conferences, and obtaining relevant certifications. Additionally, I follow security researchers and organizations on social media and take part in continuous learning through online courses and training programs.

PRACTICAL EXERCISES

Interviewer: Now, let’s move on to a practical exercise. Here's a set of logs. Can you identify any suspicious activities?

Candidate: [Reviews logs] I see multiple failed login attempts followed by a successful login from an unfamiliar IP address. This pattern suggests a potential brute force attack. Additionally, there are several unexpected outbound connections to IP addresses associated with known malicious activities. These could indicate a compromise and data exfiltration attempt.

Interviewer: Lastly, walk me through the steps you would take to address a simulated security incident where a user reports their system is behaving strangely.

Candidate: First, I would isolate the user's system to prevent potential spread of malware. Next, I would gather details from the user about the symptoms and recent activities. I would perform a full malware scan and review system logs for unusual activities. If malware is detected, I would remove it and check for any signs of further compromise. Additionally, I would restore any lost or corrupted files from backups. I would then review and strengthen security measures, such as updating software and educating the user to prevent future incidents.

CLOSING STATEMENTS

Interviewer: Thank you for your detailed responses. Do you have any questions for us?

Candidate: Thank you for the opportunity. I would like to know more about the team I would be working with and the types of projects and technologies I would be exposed to in this role.

Interviewer: Great question. Our team is collaborative and works on a variety of projects, ranging from threat detection and incident response to vulnerability management and compliance. You'll have the chance to work with advanced security tools and gain exposure to different aspects of cybersecurity.

Candidate: That sounds exciting. I look forward to the opportunity to contribute and grow with your team.

Interviewer: We're excited about the possibility as well. We'll be in touch soon regarding the next steps. Thank you for your time.