SIMULATED INTERVIEW FOR CYBERSECURITY ANALYST: QUESTIONS (INTERVIEWER) AND ANSWERS (CANDIDATE)

BY IZZMIER IZZUDDIN

General Preparation Tips For All Levels

1. **Understand The Role**
   Familiarise yourself with the specific responsibilities of L1 and L2 roles. L1 analysts typically focus on monitoring, initial triage and escalation, while L2 analysts handle deeper investigations, incident response and remediation.
2. **Research The Company And Industry**
   Study the company's cybersecurity posture, recent news and industry challenges. If applying to an MSSP, understand the client-centric nature of the work and the kinds of alerts you might encounter.
3. **Showcase Your Technical And Soft Skills**
   Cybersecurity requires a mix of technical expertise and soft skills (e.g., communication, teamwork and adaptability). Highlight both sets of skills in your examples and answers.

Interview Tips For L1 Cybersecurity Analyst Roles

1. **Emphasise Monitoring And Triage Skills**
   - Be prepared to discuss your experience or understanding of SIEM tools and alert monitoring. If you've used specific tools like Splunk, QRadar or others, mention them.
   - Explain the process of identifying and categorising alerts, distinguishing false positives from actual incidents and how you would escalate incidents to L2.
2. **Demonstrate Basic Knowledge Of Threats and Attacks**
   - Understand basic attack vectors (e.g., phishing, brute force, malware) and discuss how they might appear in logs or alerts.
   - Showcase familiarity with common threats relevant to the company's sector.
3. **Incident Handling Steps**
   - Review incident handling steps like Identification, Containment, Eradication, Recovery and Lessons Learned. L1 analysts often focus on the initial phases (Identification and basic Containment).
   - Be ready to explain how you'd respond if an alert showed potential malware or suspicious network traffic.
4. **Be Familiar With Basic IT Concepts**

- Basic networking (IP addresses, subnets, DNS), operating system fundamentals and understanding of firewalls, proxies and intrusion detection systems (IDS/IPS) will be useful.
- Have examples of how you might spot anomalies or recognise normal traffic patterns vs. potential threats.

5. **Show Interest In Continuous Learning**
    - Mention any courses, labs or practice exercises you've done on platforms like TryHackMe, Cybrary or Hack The Box.
    - Emphasise your enthusiasm for staying updated on cybersecurity news and trends.

Interview Tips For L2 Cybersecurity Analyst Roles

1. **Demonstrate Analytical And Investigative Skills**
    - L2 analysts dig deeper into incidents, so be ready to showcase your experience with root cause analysis and advanced threat detection.
    - Explain how you analyse suspicious activities or artifacts to identify the scope and potential impact of an incident.
2. **Showcase Experience With Advanced Threat Intelligence And Tools**
    - Discuss any experience with malware analysis, threat hunting or sandboxing tools.
    - Explain how you utilise OSINT tools (like VirusTotal) to investigate indicators of compromise (IoCs) and understand threat actor motives and tactics.
3. **Emphasise Incident Response And Remediation Expertise**
    - Discuss specific incidents you've handled (if possible) and walk through the full lifecycle of your response.
    - Be familiar with forensics, containment and recovery strategies and how you've worked with other teams to mitigate threats and implement long-term protections.
4. **Advanced Networking And Security Protocols**

- Expect questions on TCP/IP, ports, protocols and encryption methods relevant to securing data.
- Show understanding of security controls, compliance frameworks (e.g., NIST, ISO) and how they inform your approach to incident handling.

5. **Situational And Behavioral Scenarios**
    - For example: How would you handle a scenario where a high-severity alert is raised and the initial investigation shows signs of a breach?
    - Be ready to articulate your problem-solving process, communication with stakeholders and any preventative measures you'd recommend.

SIMULATED INTERVIEW FOR AN L1 CYBERSECURITY ANALYST

General Knowledge

I: Could you explain what the main responsibilities of an L1 cybersecurity analyst are?

C: Certainly. An L1 cybersecurity analyst is responsible for monitoring security alerts, triaging incidents and identifying potential security threats. They usually respond to low- to moderate-severity alerts and escalate serious incidents to higher-level analysts. The L1 role also involves using SIEM tools to track, document and report on suspicious activity. Essentially, the goal is to quickly identify and address potential security issues to minimise impact on the organisation.

I: Next, could you tell me what a SIEM tool is and why it's important for cybersecurity monitoring?

C: A SIEM (Security Information and Event Management) tool is a system that aggregates and analyses log data from different network devices, applications and servers. It's important because it helps security teams detect suspicious patterns, unusual behaviors and potential threats in real-time. SIEM tools allow analysts to view and manage alerts in one place, making it easier to monitor and respond to potential security incidents.

I: Do you know some common SIEM tools used in the industry?

C: Yes, some popular SIEM tools are Splunk, IBM QRadar, ArcSight and LogRhythm. Each tool has different features and capabilities, but they all provide centralised logging, monitoring and analysis.

Technical Knowledge

I: Could you explain the difference between a firewall and an IDS (Intrusion Detection System)?

C: Of course. A firewall acts as a barrier between an internal network and the internet, filtering incoming and outgoing traffic based on predefined security rules. Its primary function is to block unauthorised access while allowing legitimate traffic. An IDS, on the other hand, is designed to monitor network traffic for suspicious activities or known threats and alert security teams when it detects potentially malicious behavior. Unlike firewalls, IDS doesn't block traffic but simply detects and logs it.

I: What would you say is the role of DNS in network communication?

C: DNS or Domain Name System, translates human-readable domain names like "example.com" into IP addresses that computers use to identify each other on a network. It's essential because it allows users to access websites with domain names rather than having to remember IP addresses. In terms of security, DNS can also be leveraged to detect and block malicious domains.

I: What are the main differences between TCP and UDP?

C: TCP or Transmission Control Protocol, is a connection-oriented protocol, meaning it establishes a connection before data is transmitted, ensuring reliable delivery. It's often used for applications where data integrity is crucial, like web browsing or email. UDP or User Datagram Protocol, is a connectionless protocol, which means it doesn't establish a connection and doesn't guarantee delivery, making it faster but less reliable. UDP is often used in real-time applications like video streaming or online gaming, where speed is more important than reliability.

I: Could you explain what a DDoS attack is?

C: A DDoS or Distributed Denial of Service attack, is an attempt to disrupt normal traffic to a server, service or network by overwhelming it with a flood of internet traffic. Attackers use multiple compromised devices to send large amounts of requests simultaneously, making the target unavailable to legitimate users. The goal is to exhaust resources, causing downtime or degraded performance.

Scenario-Based Questions

I: Imagine you're monitoring alerts in the SIEM and notice an unusual spike in failed login attempts from a single IP address. How would you handle this?

C: First, I'd investigate the IP address by checking its location, reputation and history in the SIEM to see if it's known for malicious activity. I'd also check if the attempts are targeting a specific account or system. If I confirm it's suspicious, I'd escalate it as a potential brute force attack, document my findings and follow the incident response procedures, such as blocking the IP address if authorised and informing the client or higher-level analysts if needed.

I: What would you do if you received an alert for a phishing email?

C: For a phishing alert, I'd start by verifying the email details, such as the sender's address, message contents and any attachments or links. I'd try to determine if it was flagged correctly. If I confirm it's a phishing email, I'd document it, report it to the relevant

department and work on containing it by notifying affected users and removing the email from the system, if possible. I'd also advise users to avoid interacting with similar emails and provide recommendations on how to recognise phishing attempts in the future.

I: Let's say a user reports their system is running slowly and they suspect malware. How would you investigate?

C: I'd first run a preliminary check of system logs and recent activities on the user's machine, looking for signs of suspicious processes or connections. I'd also check for unusual software installations, high CPU usage and network traffic. If I find indicators of malware, I'd isolate the machine from the network, perform a malware scan and escalate the issue if advanced analysis is needed. Once I confirm it's clear, I'd restore it following our procedures.

Wrap-Up and Additional Questions

C: Could you share more about the typical day-to-day responsibilities for an L1 analyst here? Also, are there training opportunities to progress to an L2 role?

I: Absolutely. Day-to-day, you'll be monitoring alerts in the SIEM, analysing and categorising them and escalating incidents as needed. We emphasise teamwork and learning, so there will be plenty of guidance from senior analysts and we offer periodic training to help with skill development and certification support. Advancement to an L2 role is definitely possible with time and proven performance.

SIMULATED FOR AN L2 CYBERSECURITY ANALYST

General Knowledge

I: Could you explain the role of an L2 analyst and how it differs from an L1 analyst?

C: Of course. An L2 analyst goes beyond the initial alert monitoring and triaging tasks of an L1. L2 analysts handle more in-depth investigations, respond to escalated incidents and carry out threat hunting to proactively detect risks. They analyse logs, conduct root cause analyses and work on remediating incidents to prevent recurrence. L2 analysts may also work on tuning detection rules to reduce false positives and improve detection accuracy.

I: Could you also explain what threat hunting is and why it's essential for an L2 role?

C: Threat hunting is the process of proactively searching for signs of malicious activity or hidden threats within a network that may have evaded existing defenses. It's essential for an L2 role because it allows us to identify and mitigate advanced persistent threats (APTs) and other subtle attacks that don't trigger standard alerts. Threat hunting enables us to stay one step ahead of attackers by identifying patterns or anomalies that indicate malicious activity.

I: Can you describe the cyber kill chain and its relevance in incident response?

C: Certainly. The cyber kill chain is a model that outlines the stages of a cyber attack, from initial reconnaissance to data exfiltration. The stages typically include Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command and Control and Actions on Objectives. Understanding the kill chain helps in identifying the attacker's progression and allows us to disrupt or mitigate an attack at various stages. By identifying where an attack is in the kill chain, we can tailor our response efforts to stop the adversary before they achieve their goals.

Technical Knowledge

I: Can you explain what a DNS tunneling attack is and how it might be detected?

C: A DNS tunneling attack uses the DNS protocol to tunnel unauthorised data in and out of a network. Attackers use DNS requests and responses to bypass traditional security controls by embedding data within the payload of DNS queries. This type of attack is challenging to detect because DNS traffic is often allowed through firewalls. Detection methods include monitoring DNS traffic for unusual patterns, such as large amounts of DNS queries, high entropy in DNS request strings or anomalous domain names that don't fit normal patterns.

I: Can you describe what MITRE ATT&CK is and how it's useful for an L2 analyst?

C: The MITRE ATT&CK framework is a knowledge base of tactics, techniques and procedures (TTPs) that attackers use in various stages of a cyber attack. It's beneficial for L2 analysts because it provides a structured approach to understanding adversarial behaviors and helps map out how an attacker might compromise a network. By referencing MITRE ATT&CK, we can identify gaps in our detection capabilities, prioritise threats based on techniques observed and plan more effective defenses and response strategies.

I: How would you differentiate between an IOC (Indicator of Compromise) and a TTP?

C: An IOC is an observable piece of data that indicates potential malicious activity, like IP addresses, domain names or file hashes associated with known threats. TTPs, on the other hand, refer to the specific actions or methodologies used by attackers, like spear-phishing or credential dumping. While IOCs are individual signs of a compromise, TTPs describe the attacker's overall strategy and behavior, making them more useful for understanding an adversary's long-term objectives and improving detection capabilities.

Scenario-Based Questions

I: Imagine you receive an alert indicating multiple failed login attempts followed by a successful login from an unusual location. What steps would you take?

C: First, I'd start by verifying the details in the alert and checking if the unusual login location matches any known VPN usage or travel records for the user. I'd review recent login history for this user to establish a baseline and determine if this pattern is truly abnormal. If it seems suspicious, I'd investigate further by checking for additional indicators, such as unusual file access or data transfers. I would then reach out to the user to confirm if they were responsible for the login. If the activity remains unverified, I'd escalate the case and potentially lock the account as a precautionary measure, depending on the organisation's response policy.

I: What would you do if you discovered ransomware on one of the company's servers?

C: My first priority would be to contain the infection by isolating the affected server to prevent the ransomware from spreading. I'd also immediately inform the incident response team and relevant stakeholders. Once the server is contained, I'd conduct an analysis to determine how the ransomware entered the system and which files or systems have been impacted. If backups are available, I'd work on restoring the affected files. Additionally, I'd perform a root cause analysis to identify and address any vulnerabilities exploited by the

ransomware, such as unpatched software or weak credentials and implement preventive measures to minimise future risk.

I: Suppose you see unusual outbound traffic to a suspicious IP address. How would you investigate it?

C: I'd start by identifying the origin of the traffic within our network, including the specific device and process responsible. I'd check recent logs from that device for any suspicious processes or unauthorised software. I'd also use threat intelligence sources or OSINT tools to gather information on the suspicious IP address, verifying if it's associated with known malicious activities. If I find indicators of compromise, I'd escalate the case, isolate the device and start an in-depth investigation into the incident to determine the scope and potential impact.

Wrap-Up and Additional Questions

C: Could you share more about the security team's structure and any upcoming projects that an L2 analyst would be involved in?

I: Sure! Our team is structured into three levels, with L1 analysts focusing on monitoring and triaging, L2 on in-depth investigations and escalations and L3 handling threat intelligence and forensic analysis. Currently, we're working on enhancing our threat detection by tuning our SIEM rules and L2 analysts are crucial for identifying gaps and refining our alert logic. We're also implementing regular threat-hunting sessions, where L2 analysts will play an active role.

CYBERSECURITY ANALYST INTERVIEW SIMULATION

General Knowledge

I: Can you explain the CIA triad and its importance in cybersecurity?

C: The CIA triad stands for Confidentiality, Integrity and Availability. It's a foundational model for cybersecurity.

- Confidentiality ensures sensitive information is accessible only to authorised individuals.
- Integrity guarantees that data is accurate and hasn't been tampered with.
- Availability ensures that information and systems are accessible when needed. Together, these principles guide the implementation of security measures to protect systems and data.

I: What's the difference between vulnerability, threat and risk?

C: A vulnerability is a weakness in a system, such as outdated software. A threat is a potential event or actor that can exploit the vulnerability, like a cybercriminal or malware. Risk is the likelihood and impact of the threat exploiting the vulnerability, considering the business context.

I: Can you describe the difference between IDS and IPS?

C: An Intrusion Detection System (IDS) monitors network traffic for suspicious activity and alerts administrators but doesn't take action. An Intrusion Prevention System (IPS) goes a step further by actively blocking or mitigating identified threats in real-time.

Technical Knowledge

I: Can you explain how a SIEM tool works?

C: A SIEM (Security Information and Event Management) tool aggregates and analyses log data from multiple sources like firewalls, servers and applications. It identifies patterns, correlates events and generates alerts for potential security incidents. Analysts use it to monitor, investigate and respond to threats effectively.

I: How would you investigate a malware infection in a corporate environment?

C: I would start by isolating the affected device to contain the malware. Then, I'd analyse logs to identify the source and entry point, such as phishing emails or drive-by downloads.

Using tools like antivirus or sandboxing, I'd assess the malware's behaviour. Finally, I'd remediate by removing the malware, patching vulnerabilities and updating policies or controls to prevent recurrence.

I: Could you explain what lateral movement is and how to detect it?

C: Lateral movement occurs when an attacker gains access to one system and moves across the network to access additional resources. It's often part of a larger attack like ransomware. Detection involves monitoring for unusual access patterns, excessive account privileges or abnormal traffic between internal systems. Tools like UEBA (User and Entity Behaviour Analytics) and network monitoring solutions can help identify lateral movement.

Scenario-Based Questions

I: Suppose you detect multiple failed login attempts followed by a successful login from a suspicious IP address. What steps would you take?

C: I'd start by verifying the user's activity and location. I'd check if the IP address matches known VPNs or legitimate usage. If not, I'd investigate logs for signs of brute force attempts or credential compromise. I'd lock the account and contact the user for verification. Simultaneously, I'd search for additional signs of compromise, such as unusual data access or file downloads.

I: Your team identifies a zero-day vulnerability affecting critical systems. What actions would you take?

C: First, I'd assess the vulnerability's impact on our environment by identifying affected systems. Next, I'd implement temporary mitigations, such as disabling affected services or increasing monitoring. I'd also ensure relevant stakeholders are informed and work with vendors for patches or updates. Once a patch is available, I'd test it in a controlled environment before deploying it organisation-wide.

I: What would you do if you notice data being exfiltrated from a secure server?

C: I'd immediately isolate the server and block the suspicious outbound connections. I'd review logs to identify the source of the exfiltration and investigate how the attacker gained access. If possible, I'd recover the stolen data and notify the incident response team and management. After containment, I'd conduct a thorough root cause analysis and update security controls to prevent future breaches.

Wrap-Up and Additional Questions

C: Could you share more about the types of incidents the team typically handles and any upcoming projects I might contribute to if hired?

I: Our team handles incidents ranging from phishing to advanced persistent threats. We're also working on improving our detection rules and integrating new threat intelligence feeds. Lately, we've been focusing on proactive threat hunting and enhancing our incident response procedures.

SCENARIO-BASED QUESTIONS

Incident Response Scenarios

Question: You notice multiple failed login attempts followed by a successful login from an unusual IP address. What steps would you take to investigate and respond?

- First, I'd verify the login details, including timestamps, IP addresses and geolocation, by pulling logs from the SIEM and checking login records.
- If the IP address is unusual, I'd cross-reference it with known threat intelligence sources.
- I'd check for any account changes made and assess if sensitive data was accessed.
- If suspicious, I'd reset the password, notify the user and increase monitoring on the account.

Question: A user reports their computer is behaving strangely, with frequent pop-ups and performance issues. How would you investigate and remediate this issue?

- I'd first isolate the machine from the network to prevent lateral spread.
- Next, I'd perform a malware scan and analyse logs for indicators of compromise (IOCs).
- After identifying and removing malware, I'd apply any necessary patches or updates and educate the user on security practices.

Question: An employee reports receiving a phishing email and you suspect other employees may have received the same email. How would you handle this situation?

- I'd examine the email headers and payload to confirm it's phishing.
- Then, I'd search for similar emails in our email security solution to see if others received it.
- If widespread, I'd notify staff about the phishing email, update filtering rules and conduct a post-incident review.

Question: You detect large amounts of data being transferred to an external IP address outside business hours. How would you investigate and respond?

- I'd analyse data transfer logs to confirm if sensitive data was involved and locate the user or process responsible.

- If confirmed, I'd block the IP, isolate affected systems and report the incident to appropriate stakeholders.
- Finally, I'd conduct a root-cause analysis to prevent similar incidents.

Question: An endpoint in the network has been flagged for unusual behaviour, including communicating with a known malicious domain. What actions would you take?

- I'd isolate the endpoint, examine logs and identify processes connecting to the malicious domain.
- I'd then perform a malware scan, remove any threats and block further communication with the malicious domain.
- Finally, I'd enhance security measures and review network logs for any lateral movement.

Question: Your organisation becomes aware of a zero-day vulnerability in software critical to operations. What steps would you take to protect the organisation while waiting for a vendor patch?

- Until a patch is released, I'd limit access to the vulnerable software, apply any workarounds and set up additional monitoring.
- I'd check with the vendor for any temporary mitigations and monitor threat intel for updates on active exploits.

Threat Detection And Analysis Scenarios

Question: Your SIEM alerts you to an unusually high volume of traffic between internal servers. What would you do next?

- I'd use the SIEM to correlate events and identify if this traffic is expected or indicates malicious activity.
- If malicious, I'd isolate affected systems, check for abnormal processes and investigate network connections.

Question: You're reviewing a list of SIEM alerts and suspect some are false positives. How would you validate and reduce the occurrence of false positives?

- I'd examine event logs to verify if the alerts align with known legitimate behavior.

- I'd fine-tune the SIEM rules, remove unnecessary alerts and ensure filters minimise future false positives.

Question: A workstation triggers an alert for possible ransomware activity. How would you investigate, contain and mitigate the threat?

- I'd isolate the workstation immediately and analyse logs for any malicious activity.
- After confirming ransomware, I'd scan connected systems, ensure backups are secure and initiate a post-incident analysis.

Question: A user account with no administrative privileges suddenly attempts to modify critical system files. What steps would you take?

- I'd investigate recent changes, check if the user credentials were compromised and confirm if sensitive files were accessed or modified.
- I'd reset account credentials if needed, review policies and monitor for further unusual activities.

Question: Your company's web application is experiencing a Distributed Denial of Service (DDoS) attack. How would you handle the situation?

- I'd reach out to our ISP or hosting provider for traffic mitigation and use rate-limiting controls on our infrastructure.
- I'd analyse traffic patterns for source identification and block malicious IPs and finally, assess the attack's impact on business continuity.

Vulnerability Management Scenarios

Question: During a routine scan, you find several systems running outdated software. How would you prioritise remediation?

- I'd prioritise systems with the most critical business impact, determine patch availability and schedule updates.
- High-risk systems would be patched first and I'd monitor for potential exploitation attempts.

Question: A critical security patch has been released, but applying it requires downtime. How would you manage the patching process to minimise risk and impact?

- I'd coordinate with IT to schedule patching during non-peak hours and deploy patches in a test environment before full rollout.
- I'd document the process and update our vulnerability management tracking system.

Question: You discover several devices on the network that are not documented or managed. How would you address this?

- I'd scan the network to identify these assets, gather information on their purpose and enforce inventory tracking policies.
- If unauthorised, I'd isolate the assets and investigate any potential security gaps.

Policy And Compliance Scenarios

Question: You discover a user with access to sensitive data they don't need for their job. How would you handle this situation?

- I'd investigate the user's access history, consult with their manager and revoke any unnecessary access.
- I'd implement a review process to prevent similar access violations.

Question: An employee uses a personal device to access corporate resources and you suspect it may be compromised. What actions would you take?

- I'd work with IT to run a malware scan on the device and ensure it complies with company policy.
- I'd also reinforce BYOD policies with the employee and discuss mobile device management solutions.

Question: An internal audit identifies non-compliance with a critical security policy. How would you address the issue and ensure compliance?

- I'd assess the non-compliance risk, establish corrective actions and work with departments to address the issue.
- Finally, I'd schedule a follow-up review to ensure sustained compliance.

Proactive Security Scenarios

Question: You receive threat intelligence about an ongoing attack campaign targeting your industry. What steps would you take to protect your organisation proactively?

- I'd review the threat intelligence and map it to our current environment, identifying high-risk assets.
- I'd share relevant threat intelligence with SOC team members and deploy security measures accordingly.

Question: A USB drive is found in the office parking lot. An employee brings it in and plugs it into their workstation. What would you do?

- I'd isolate the workstation, retrieve the USB and scan it in a secure environment.
- I'd inform staff of the risks and implement a policy to prevent unauthorised USB device usage.

Question: Your team suspects an APT group is targeting your organisation. What steps would you take to investigate and mitigate potential risks?

- I'd analyse logs for unusual activity and look for lateral movement indicators.
- I'd increase security controls on critical assets and regularly update the team on the investigation.

Log And Forensics Scenarios

Question: You are reviewing firewall logs and notice repeated attempts to access an internal server from an external IP address. What would be your next steps?

- I'd inspect firewall logs for repeated access attempts and match them against known threat intelligence.
- I'd block any IPs involved in suspicious activities and investigate if other systems were targeted.

Question: A user's machine has been compromised and critical files have been deleted. How would you recover and analyse the data?

- I'd isolate the machine, attempt file recovery using backup solutions and analyse logs to understand the attacker's actions.
- Finally, I'd strengthen backup processes and access controls.

Question: After a security incident, you're tasked with building a timeline of events. What tools and techniques would you use?

- I'd gather data from logs, EDR solutions and employee reports, analysing timestamps to create an event sequence.
- I'd use forensic tools like FTK Imager to assist in compiling an accurate timeline.

Cloud Security Scenarios

Question: You find that sensitive files in your organisation's cloud storage are accessible to the public. What would you do?

- I'd immediately change permissions to restrict access, then check for any unauthorised access to sensitive files.
- I'd run a security scan on all cloud resources to ensure proper configurations and implement ongoing monitoring.

Question: Your cloud provider's logs show unusual activity in the admin console. How would you investigate?

- I'd review logs to verify unauthorised actions, monitor other privileged accounts and set up alerts for any additional unusual activity.
- If needed, I'd reset admin credentials and enable multifactor authentication.

Question: An employee is using an unauthorised SaaS application for work purposes. How would you address the risks involved?

- I'd communicate with the employee to understand their requirements, propose approved tools and restrict unapproved applications.
- I'd work with IT to monitor and control access to SaaS applications moving forward.

Phishing And Social Engineering Scenarios

Question: A staff member receives an email from an address that appears to belong to the CEO, requesting a wire transfer. What actions would you take?

- I'd verify the sender's email and analyse email headers to confirm if it's a spoof.

- I'd educate employees on the impersonation attempt and strengthen email authentication policies (e.g., SPF, DKIM).

Question: A visitor without a badge follows an employee into a restricted area. How would you respond to this physical security breach?

- I'd review CCTV footage, document the incident and reinforce physical security training with employees.
- I'd evaluate access controls and consult security to implement stricter badge policies.

Question: An employee posts sensitive company information on their social media account. What actions would you take to mitigate the risk?

- I'd reach out to the employee, explain the importance of not sharing sensitive information and request removal of the post.
- I'd review the social media policy with employees to prevent future incidents.

Other Real-World Scenarios

Question: Your organisation's vendor notifies you of a data breach affecting their systems. How would you respond to minimise the impact on your organisation?

- I'd assess the data exposure impact, request the vendor's investigation results and strengthen access controls for the vendor.
- I'd notify impacted stakeholders and initiate a risk review for other third-party integrations.

Question: An IoT device in your network is flagged for a critical vulnerability. What steps would you take to secure it?

- I'd update the IoT device firmware and, if possible, isolate it to a segmented network.
- I'd apply additional security measures like regular vulnerability scans on IoT devices.

Question: A disgruntled employee with access to sensitive data is suspected of leaking information. How would you investigate?

- I'd audit the employee's access, monitor for unusual activity and conduct interviews if needed.

- I'd review access controls for similar roles and educate employees on data handling practices.

Question: You discover user accounts for employees who left the company months ago are still active. What would you do?

- I'd remove inactive accounts, confirm removal with relevant departments and update the offboarding policy to prevent recurrence.

Question: A software update from a trusted vendor is found to include malicious code. How would you manage the risk?

- I'd isolate systems using the updated software, perform a security scan and consult with the vendor on remediation steps.
- I'd evaluate other software vendors for similar risks and increase monitoring for compromised assets.