INTERVIEW PREPARATION FOR COMMON TECHNICAL TOPICS WITH QUESTIONS AND ANSWERS

BY IZZMIER IZZUDDIN

COMMON TOPICS

Incident Response

- Incident response involves managing and mitigating the impact of a cybersecurity incident.
- Steps in Incident Response

    1. **Preparation**
       Develop policies, procedures and playbooks. Ensure tools and communication channels are in place.
    2. **Detection and Analysis**
       Identify signs of an incident using monitoring tools (SIEM, IDS/IPS). Analyse the data to confirm the incident.
    3. **Containment**
       Implement short-term and long-term containment strategies to limit the spread (e.g., isolating affected systems).
    4. **Eradication**
       Remove the cause of the incident (e.g., malware removal, patching vulnerabilities).
    5. **Recovery**
       Restore systems to normal operations while monitoring for signs of weakness or further compromise.
    6. **Lessons Learned**
       Conduct a post-incident review to identify areas for improvement.

2. Network Security

- **Firewalls**
  Understand the difference between types of firewalls (e.g., stateful, stateless, next-generation firewalls) and how they control incoming and outgoing network traffic.
- **VPNs (Virtual Private Networks)**
  Familiarise yourself with VPN protocols (e.g., IPsec, SSL/TLS) and their roles in securing remote access.
- **IDS/IPS (Intrusion Detection/Prevention Systems)**
  Know how these systems detect and respond to suspicious activities on a network. Understand the difference between signature-based and anomaly-based detection.

- **Network Segmentation**
  Learn how to divide a network into segments to limit lateral movement by attackers and improve security control.

3. Log Analysis and SIEM (Security Information and Event Management)

- **Log Analysis**
  Learn to analyse logs from various sources (e.g., firewalls, IDS/IPS, servers, applications) to detect malicious activity or anomalies.
- **SIEM Tools**
  Familiarise yourself with tools like Splunk, QRadar and AlienVault. Understand how to create correlation rules to detect patterns of attack (e.g., brute force attempts, lateral movement).

4. Threat Intelligence

- **Gathering Intelligence**
  Understand open-source (OSINT), internal (collected from within the organisation) and third-party (commercial threat feeds) sources.
- **Analysing Intelligence**
  Learn how to analyse threat intelligence data for actionable insights. Familiarise yourself with frameworks like the MITRE ATT&CK framework for mapping adversary tactics and techniques.
- **Applying Intelligence**
  Use threat intelligence to enhance security measures (e.g., updating firewall rules, improving detection capabilities).

5. Vulnerability Management

- **Vulnerability Scanning**
  Understand the use of tools like Nessus, Qualys and OpenVAS for automated vulnerability scanning.
- **Prioritisation**
  Learn to prioritise vulnerabilities based on risk factors such as CVSS score, exploit availability, asset criticality and the organisation's risk appetite.
- **Remediation**
  Understand patch management, configuration management and how to work with development teams to fix vulnerabilities.

6. Endpoint Security

- **Endpoint Protection Tools**
  Familiarise yourself with tools like antivirus/anti-malware solutions, Endpoint Detection and Response (EDR) and advanced threat protection platforms.
- **Strategies for Endpoint Security**
  Understand the importance of maintaining secure configurations, patch management, application whitelisting and user education to prevent endpoint compromise.

EXAMPLE QUESTIONS & ANSWERS

INCIDENT RESPONSE

1. **Question:** What are the steps involved in an incident response process and how do you detect an incident?

Answer: The incident response process generally involves six steps: Preparation, Detection and Analysis, Containment, Eradication, Recovery and Lessons Learned. To detect an incident, we use monitoring tools like SIEMs, IDS/IPS, antivirus alerts and network traffic analysis. Logs from different systems are analysed to identify any anomalies or indicators of compromise (IoCs), such as unusual login attempts, file integrity changes or unexpected outbound connections.

2. **Question:** How would you contain a malware outbreak in an enterprise environment?

Answer: Containment involves isolating affected systems to prevent the spread of malware. We can implement both short-term and long-term containment strategies. In the short term, disconnect the affected systems from the network, disable user accounts if needed and apply network segmentation. In the long term, patch vulnerabilities, enhance security policies and ensure proper system backups and restore points.

NETWORK SECURITY

3. **Question:** Can you explain the difference between stateful and stateless firewalls?

Answer: A stateful firewall monitors the state of active connections and makes decisions based on the context of the traffic (e.g., allowing a response packet for an established connection). A stateless firewall, on the other hand, makes decisions based solely on predefined rules (like IP addresses, ports) for each incoming packet without considering the state of the connection.

4. **Question:** How do IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) differ in terms of functionality?

Answer: An IDS is a monitoring system that detects and alerts on potential intrusions or malicious activities. It does not take action to prevent the activity. An IPS, however, can detect malicious activity and actively prevent it by blocking traffic, dropping packets or resetting connections.

LOG ANALYSIS AND SIEM

5. **Question:** What are some key log sources that you would monitor in a SIEM and why?

Answer: Key log sources in a SIEM include

- **Firewall logs**
  To detect unauthorised access attempts or suspicious traffic patterns.
- **IDS/IPS logs**
  To identify known attack signatures or anomalous behaviour.
- **Authentication logs (e.g., Active Directory)**
  To detect brute-force attacks, unauthorised logins or privilege escalations.
- **Application logs**
  To monitor for application-layer attacks such as SQL injection or XSS. These logs help in correlating events across different parts of the network to detect potential security incidents.

6. **Question:** How would you create a correlation rule in a SIEM to detect a brute-force attack?

Answer: A correlation rule for detecting a brute-force attack could involve setting a threshold for failed login attempts from a single IP or user within a short time frame (e.g., 10 failed attempts within 5 minutes). If the threshold is exceeded, the SIEM generates an alert. The rule could also include exceptions for known or trusted IP addresses.

THREAT INTELLIGENCE

7. **Question:** What types of threat intelligence do you use and how do you apply it in your organisation?

Answer: Threat intelligence can be classified into strategic, tactical, operational and technical. Strategic intelligence is high-level information about threats and trends, tactical intelligence involves specific techniques or TTPs (Tactics, Techniques and Procedures) of adversaries, operational intelligence provides information about specific threats to an organisation and technical intelligence includes IOCs (Indicators of Compromise) like IP addresses or hashes. In our organisation, we use threat intelligence to update firewall rules, create new detection signatures in SIEM and inform incident response plans.

8. **Question:** How do you utilise the MITRE ATT&CK framework for threat hunting?

Answer: The MITRE ATT&CK framework provides a comprehensive matrix of adversary tactics and techniques that can be used to map detected activities to known attack patterns. During threat hunting, I use the framework to hypothesis potential attack scenarios, identify gaps in our detection capabilities and improve our SIEM correlation rules and alerts.

VULNERABILITY MANAGEMENT

9. **Question:** What is your approach to prioritising vulnerabilities for remediation?

Answer: Vulnerabilities are prioritised based on several factors: CVSS scores, exploit availability, the criticality of the affected systems, potential impact and the business context. For example, a high-severity vulnerability on an internet-facing server would take precedence over a low-severity vulnerability on an internal machine. We also consider mitigating controls in place and use risk-based vulnerability management to align remediation efforts with the organisation's risk appetite.

10. **Question:** What steps do you take after discovering a critical vulnerability in a production system?

Answer: After discovering a critical vulnerability, immediate steps include

- Assessing the impact of the vulnerability on the production environment.
- Applying patches or temporary mitigations (e.g., disabling vulnerable features, adding firewall rules).
- Testing the patches in a controlled environment before deployment to production.
- Monitoring for signs of exploitation and ensuring proper logging and alerts.
- Documenting the process and updating the vulnerability management policy.

ENDPOINT SECURITY

11. **Question:** How would you secure endpoints in a distributed work environment?

Answer: Securing endpoints in a distributed environment involves a multi-layered approach

- Deploying Endpoint Detection and Response (EDR) tools for real-time monitoring and response.
- Implementing antivirus and anti-malware solutions with regular updates.
- Ensuring regular patch management for operating systems and applications.
- Using encryption to protect sensitive data on devices.
- Enforcing multi-factor authentication (MFA) and strong password policies.
- Training users on security best practices and phishing awareness.

12. **Question:** What is an EDR solution and how does it differ from traditional antivirus software?

Answer: An EDR (Endpoint Detection and Response) solution provides continuous monitoring and response to advanced threats on endpoints. Unlike traditional antivirus software that relies on signature-based detection, EDR uses behavioural analysis, machine learning and threat intelligence to detect and respond to suspicious activities, even if they are zero-day threats or fileless malware.

INTERVIEW SIMULATION QUESTIONS (INTERVIEWER) & ANSWERS (CANDIDATE)

INCIDENT RESPONSE

1. **Interviewer:** Can you walk me through the steps you would take to handle a ransomware incident in an organisation?

Candidate: Certainly. Handling a ransomware incident involves the following steps

I. **Preparation**
Ensure that we have an incident response plan in place and that everyone knows their role. Backup systems should be verified regularly and cybersecurity awareness training should be ongoing.

II. **Detection and Analysis**
Use SIEM, EDR tools and monitoring systems to detect signs of ransomware, such as unusual file extensions, high CPU usage or unexpected processes. Analyse these alerts to determine the ransomware type and its entry point.

III. **Containment**
Immediately isolate infected machines from the network to prevent the ransomware from spreading. Use network segmentation to isolate critical systems and prevent lateral movement.

IV. **Eradication**
Identify the malicious files and processes, remove them using antivirus or EDR tools and eliminate the root cause by patching vulnerabilities that were exploited.

V. **Recovery**
Restore affected systems from clean backups and carefully monitor the restored systems to ensure no remnants of the ransomware remain.

VI. **Lessons Learned**
Conduct a post-incident review to identify weaknesses, improve response plans and update security measures. It's essential to document the entire process to improve future responses.

2. **Interviewer:** That’s a solid overview. How would you handle communication with stakeholders during such an incident?

Candidate: Communication is crucial. We need to keep stakeholders informed about the incident's status without causing unnecessary panic. I would coordinate with the PR team to prepare a statement for public release, ensure that internal communications

are clear and factual and maintain regular updates with senior management and affected users. If necessary, law enforcement should be involved.

NETWORK SECURITY

3. **Interviewer:** How would you differentiate between a stateful firewall and an IDS?

Candidate: A stateful firewall monitors the state of active connections and decides whether to allow or block traffic based on the state of the connection, along with predefined rules. It is particularly effective for defending against unauthorised access or maintaining a secure connection state.

An Intrusion Detection System (IDS), on the other hand, is a passive monitoring device that detects potential intrusions or malicious activities by analysing traffic against known attack patterns or anomalies. Unlike a firewall, an IDS does not block traffic; it only generates alerts for further investigation.

4. **Interviewer:** Good. If you discovered that an internal user is sending large amounts of data to an unknown external IP, how would you proceed?

Candidate: I would first analyse the firewall logs and IDS/IPS alerts to gather more information about the data being sent, including the source and destination IP addresses, ports used and the amount of data transferred. Next, I would check the endpoint involved for signs of compromise, such as unusual processes or file changes. If necessary, I would contain the threat by blocking the connection at the firewall level, isolating the endpoint from the network and conducting a deeper forensic analysis to understand the root cause.

LOG ANALYSIS AND SIEM

5. **Interviewer:** What steps would you take to analyse a potential brute-force attack detected by your SIEM?

Candidate: I would take the following steps

I. **Identify and Correlate Events**
Start by reviewing the SIEM alert to understand the scope, such as the number of failed login attempts, the source IP and the affected accounts.

II. **Cross-Check Logs**
Correlate logs from different sources like Active Directory, VPN and application logs to identify the pattern of failed and successful login attempts from the same source IP or different IPs to the same account.

III. **Check for Indicators of Compromise**
Look for other indicators, such as unexpected user agent strings, anomalous

access times or geographical locations that don't match the user's usual behaviour.

IV. **Create a Correlation Rule**
If it's a legitimate attack, I would create a correlation rule to trigger alerts for similar future events. For example, the rule could alert if there are more than 5 failed login attempts followed by a successful login within 10 minutes.

V. **Respond**
If confirmed as a brute-force attack, block the offending IP address, notify affected users and potentially force a password reset.

6. **Interviewer:** Can you give an example of a correlation rule you would set up to detect suspicious activity in a SIEM?

Candidate: Sure. One example is a rule to detect possible lateral movement within the network. The rule could be: If there are successful logins from a user account to multiple systems within a short period (e.g., 10 different systems within 5 minutes), generate an alert. This could indicate a compromised account being used to move laterally through the network.

THREAT INTELLIGENCE

7. **Interviewer:** How do you integrate threat intelligence into a security program?

Candidate: Threat intelligence is integrated by leveraging strategic, tactical, operational and technical intelligence to inform various aspects of security operations

I. **Updating Detection Rules**
Use intelligence feeds to update SIEM and IDS/IPS detection rules with the latest IOCs (Indicators of Compromise).

II. **Threat Hunting**
Use the MITRE ATT&CK framework to align threat intelligence with potential adversary tactics, techniques and procedures (TTPs), guiding threat hunters to focus on specific areas.

III. **Vulnerability Management**
Prioritise patching based on intelligence regarding active exploits in the wild.

IV. **Incident Response**
Develop playbooks for incident response based on specific threat actor profiles or threat types.

V. **Training and Awareness**
Educate staff about current threats and how to recognise them.

8. **Interviewer:** Can you provide a specific example of how you've used threat intelligence to prevent an attack?

Candidate: Sure. We received intelligence about a new malware strain targeting our industry, including IOCs such as IP addresses and file hashes. We immediately updated our SIEM with these IOCs to monitor for any suspicious activity. When our SIEM detected a connection attempt to one of the malicious IPs from an internal host, we isolated the machine, investigated the issue and discovered a phishing email as the initial attack vector. By acting quickly, we prevented a potential compromise.

VULNERABILITY MANAGEMENT

9. **Interviewer:** Walk me through your approach to vulnerability management in an enterprise environment.

Candidate: The approach includes

I. **Regular Scanning**
Use tools like Nessus or Qualys to perform regular scans of all assets to detect vulnerabilities.

II. **Risk-Based Prioritisation**
Prioritise vulnerabilities based on CVSS scores, exploit availability, asset criticality and potential business impact. For example, a critical vulnerability on an internet-facing server would be prioritised higher than one on an internal server.

III. **Remediation**
Apply patches, configurations or other mitigations to remediate vulnerabilities. For systems that cannot be immediately patched, implement compensating controls.

IV. **Verification**
Conduct follow-up scans to ensure vulnerabilities have been effectively mitigated.

V. **Continuous Improvement**
Review the vulnerability management process regularly, incorporating feedback and lessons learned to improve future cycles.

10. **Interviewer:** How would you handle a zero-day vulnerability for which no patch is available?

Candidate: For a zero-day vulnerability, I would implement compensating controls such as network segmentation, firewall rules or disabling the vulnerable service if possible. Additionally, I would monitor closely for any indicators of compromise

associated with the vulnerability and collaborate with the security community and vendors for updates and potential workarounds.

ENDPOINT SECURITY

11. **Interviewer:** How do you approach securing endpoints in an organisation where employees work remotely?

Candidate: Securing remote endpoints requires a multi-faceted approach

1. **Endpoint Detection and Response (EDR)**
   Deploy EDR solutions to monitor endpoints for suspicious activities and enable rapid response to potential threats.
2. **Patch Management**
   Ensure all operating systems and applications are regularly updated with the latest security patches.
3. **Data Encryption**
   Use full-disk encryption and encrypt sensitive data in transit and at rest.
4. **MFA and VPN**
   Enforce multi-factor authentication (MFA) and require VPN access for remote connections to the corporate network.
5. **Security Awareness**
   Regularly train users on recognising phishing attacks and following security best practices.

12. **Interviewer:** Can you explain the difference between an antivirus and an EDR solution?

Candidate: Antivirus solutions primarily focus on signature-based detection to identify known malware and viruses. They are often effective against well-known threats but can miss zero-day or sophisticated attacks.

EDR (Endpoint Detection and Response), on the other hand, provides advanced detection capabilities through behavioural analysis, machine learning and threat intelligence. EDRs can detect fileless malware, unknown threats and lateral movements. They also offer response capabilities, such as isolating infected endpoints and performing forensic analysis.

INTERVIEW SIMULATION QUESTIONS (INTERVIEWER) & ANSWERS (CANDIDATE) - SCENARIO-BASED

Scenario 1: Your organisation's SIEM system has triggered an alert for suspicious outbound traffic from an internal server that is supposed to host only internal web applications. The alert indicates that the server is communicating with a known malicious IP address associated with data exfiltration activities. Upon initial investigation, you notice that a large amount of data has been transferred over the last few hours to this IP.

1. **Interviewer:** You've received an alert from the SIEM about suspicious outbound traffic from an internal server. This server is meant only to host internal applications, but it appears to be communicating with a known malicious IP linked to data exfiltration. Upon further inspection, you notice a significant amount of data transfer to this IP over the past few hours. How would you handle this situation?

Candidate: First, I would categorises this as a potential data exfiltration incident, which is a high-priority issue. Here's the step-by-step process I would follow

I. **Containment**
My immediate action would be to isolate the affected server from the network to prevent further data loss. I would use network controls, such as firewall rules or network access control (NAC) solutions, to block all outbound traffic from the compromised server.

II. **Identification and Analysis**

- I would start by reviewing the SIEM logs to gather detailed information about the suspicious activity, such as the time of the initial connection to the malicious IP, the volume of data transferred and the protocol used.
- Next, I would analyse other logs, including firewall, proxy and endpoint logs, to determine if there were any other signs of compromise, such as unusual login activities, process executions or unexpected outbound connections from other servers or endpoints.
- I would also check for any relevant IOCs (Indicators of Compromise) and TTPs (Tactics, Techniques and Procedures) associated with this IP address or the specific malware family, if identified, using threat intelligence feeds.

III. **Forensic Investigation**

- Conduct a forensic analysis on the compromised server. This would involve capturing a memory dump and disk image to analyse any

malicious processes, malware artifacts or signs of lateral movement within the environment.

- I would look for any evidence of command and control (C2) communication, unauthorised access or data staging for exfiltration.

IV. Eradication

- Once the root cause, such as malware or a vulnerability, is identified, I would work to remove the threat. This could involve removing malware, applying patches or modifying configurations to close any exploited vulnerabilities.
- I would also scan other systems for similar artifacts to ensure that the attack is contained and hasn't spread.

V. Recovery

- Restore the affected server from a known good backup, if available and monitor closely for any signs of reinfection or residual compromise.
- Reconnect the server to the network only after ensuring it is clean and securing the environment.

VI. Post-Incident Analysis and Reporting

- Conduct a lessons-learned session with all relevant teams to understand how the incident occurred, what could have been done better and any gaps in the existing security posture.
- Update detection and response playbooks, SIEM rules and firewall rules to prevent similar incidents in the future.

VII. Communication with Stakeholders

- Throughout this process, I would keep all relevant stakeholders informed, including the IT team, management and legal and compliance teams. If there's a potential for regulatory impact or data breach notification, I would involve the legal and compliance teams immediately.

2. **Interviewer:** That's a comprehensive approach. How would you determine if any sensitive data was exfiltrated?

Candidate: To determine if sensitive data was exfiltrated, I would

I. Examine Data Transferred

Analyse the network logs and any captured packets to identify the type and volume of data that was transferred to the malicious IP. I would focus on any files or databases accessed during the time frame of the alert.

II. **Review Server Logs**
Check the server access logs for any files accessed, modified or copied around the time of the suspicious activity.

III. **File Integrity Monitoring**
If we have file integrity monitoring (FIM) in place, I would review logs for any unauthorised or unusual changes to files that contain sensitive information.

IV. **Compare Against Known Data Inventory**
Compare the accessed or transferred data against our data inventory and classification policy to assess the sensitivity and impact of the data potentially exfiltrated.

V. **Engage DLP Tools**
Utilise any Data Loss Prevention (DLP) tools in place to identify if sensitive data, such as PII, intellectual property or financial data, was involved.

VI. **Coordinate with Data Owners**
Engage with data owners and relevant teams to validate the findings and assess the full impact.

3. **Interviewer:** Great response. How would you improve the detection and prevention of such incidents in the future?

Candidate:

I. **Enhance Monitoring**
I would review and enhance SIEM rules to detect unusual outbound connections, large data transfers and abnormal server behaviours.

II. **Deploy Network Segmentation**
Implement stricter network segmentation to limit which servers can communicate with the internet, especially for servers that are supposed to be internal-only.

III. **Implement Data Anomaly Detection**
Deploy anomaly detection mechanisms to identify abnormal data flows or network connections.

IV. **Regular Threat Intelligence Updates**
Regularly update threat intelligence feeds and use them to fine-tune detection mechanisms.

V. **Security Awareness Training**
Conduct training to educate employees about phishing and other common attack vectors that could lead to initial compromise.

VI. Regular Penetration Testing

Perform regular penetration testing and vulnerability assessments to identify weaknesses before attackers can exploit them.

Scenario 2: Your organisation has deployed a new web-based application accessible to customers over the internet. Shortly after its deployment, multiple customers report receiving phishing emails that appear to be coming from your organisation. The emails contain personal information about the customers, leading you to believe there may be a data breach or compromise of the new application.

1. **Interviewer:** We've recently deployed a new web-based application for our customers. However, soon after its release, customers started reporting phishing emails that seem to be sent from our organisation. These emails contain specific personal information about the customers. What steps would you take to investigate this potential data breach or compromise?

Candidate: Given the situation, this seems like a serious security incident involving potential data leakage or compromise. Here's how I would approach this

I. **Initial Assessment and Triage**

- First, I would classify this as a potential data breach with a high impact and high urgency. I would immediately inform key stakeholders, including the incident response team, management and legal/compliance teams.
- I would check for any recent security alerts, vulnerabilities or anomalies reported in the new web application and identify whether any of them could have contributed to the data compromise.

II. **Containment**

- Before diving into the investigation, I would implement immediate containment measures, such as temporarily taking the application offline or blocking certain functionalities (e.g., user registration or sensitive data access) to prevent further data exposure.

III. **Data Collection and Investigation**

- **Log Analysis**
  I would begin by collecting logs from the web server, application server and database to look for signs of suspicious activity, such as SQL injection attempts, unusual error messages or unexpected API calls.
- **Review Recent Changes**
  Examine recent code changes, configuration settings or updates to the application to identify any potential vulnerabilities or misconfigurations.
- **Analyse Phishing Emails**
  Gather samples of the phishing emails reported by customers and analyse the headers, content and links to determine if they are being sent from our infrastructure or if it's a case of email spoofing.

- **Access Patterns**
  Review access logs to identify unusual patterns, such as high volumes of data access or export operations tied to a single user or IP address.
- **Threat Intelligence**
  Utilise threat intelligence feeds to see if this type of attack is being reported elsewhere, potentially indicating a wider campaign.

IV. Identify the Root Cause

- If the logs indicate that attackers were able to exploit a vulnerability in the application (such as SQL injection or a misconfigured API), I would escalate this to the development and operations teams to address the vulnerability immediately.
- If it appears that customer data was extracted due to a weak access control mechanism, I would focus on tightening these controls.

V. Eradication and Remediation

- Based on the root cause, I would work with the development team to patch vulnerabilities, update configurations and implement additional security controls, such as web application firewalls (WAF) and rate-limiting.
- Ensure that compromised customer data is no longer accessible and that any backdoors or malware placed by attackers are removed.

VI. Notification and Communication

- If a breach is confirmed, coordinate with the legal and compliance teams to determine if any regulatory notifications are required (e.g., GDPR, CCPA).
- Communicate with affected customers to inform them of the breach, advising them to be cautious of phishing attempts and offering guidance on protective measures (e.g., changing passwords, monitoring accounts).

VII. Recovery

- Once the application is secured and all vulnerabilities are remediated, bring the application back online.
- Monitor closely for any signs of continued malicious activity or attempts to exploit the same or similar vulnerabilities.

VIII. Post-Incident Review and Improvement

- Conduct a post-incident review with all relevant teams to analyse the timeline, response actions and any gaps identified during the incident.
- Update security policies, incident response plans and user training programs to address these gaps and prevent similar incidents in the future.
- Implement additional preventive measures, such as code reviews, automated security testing and continuous monitoring.

2. **Interviewer:** You've covered the investigation and response thoroughly. How would you improve our organisation's ability to detect such incidents earlier?

Candidate:

I. **Enhance Monitoring and Alerts**
Set up more granular monitoring and alerts for anomalous activities, such as unusual data access patterns, spikes in data transfer and repeated failed login attempts.

II. **Implement Stronger Access Controls**
Ensure role-based access control (RBAC) is properly implemented and consider integrating multi-factor authentication (MFA) for administrative and customer accounts.

III. **Regular Vulnerability Assessments and Penetration Testing**
Conduct regular vulnerability scans and penetration tests on all web applications, particularly after any code changes, to identify weaknesses proactively.

IV. **Phishing Awareness Programs**
Implement an ongoing phishing awareness program to educate both employees and customers about recognising and reporting phishing attempts.

V. **Integrate Threat Intelligence**
Utilise threat intelligence platforms to keep abreast of emerging threats that could affect our applications and systems, enabling us to adjust defences proactively.

3. **Interviewer:** Good points! If a vulnerability was discovered in the new application, how would you communicate this internally and to our customers?

Candidate:

- **Internal Communication**
I would use a structured incident report to communicate the vulnerability details, its impact and the steps being taken to remediate it to all relevant

internal stakeholders, including development, IT, compliance and management teams.

- **Customer Communication**
  I would collaborate with the legal, compliance and public relations teams to craft a transparent message to affected customers. This message would include what was discovered, the steps taken to mitigate the issue, any potential impact on them and what actions they should take, like updating passwords or being vigilant against phishing emails.

Scenario 3: Your organisation is conducting a routine vulnerability assessment of its internal network and discovers several high-severity vulnerabilities on critical servers. These vulnerabilities include unpatched software, default credentials and open ports that should be closed. You also notice that one of the critical servers is directly exposed to the internet, which increases the risk significantly.

1. **Interviewer:** During a routine vulnerability assessment, we identified several high-severity vulnerabilities on critical servers, such as unpatched software, default credentials and open ports that should be closed. One of these servers is also exposed to the internet, which is a significant risk. How would you prioritise and mitigate these vulnerabilities?

Candidate: First, I'd recognise this as a critical situation that requires immediate action due to the high risk associated with the vulnerabilities and the exposed server. Here's the approach I'd take to address these issues

I. Prioritisation of Vulnerabilities

- I'd prioritise the vulnerabilities based on their risk and impact using a risk matrix approach. Vulnerabilities that are exposed to the internet, such as those on the exposed server, would be addressed first because they have the highest potential for exploitation.
- Next, I would categorise the vulnerabilities by their type and severity
  - **Critical (Exposed Server with Default Credentials)**
    Immediate attention is needed as this poses a significant risk of unauthorised access.
  - **High (Unpatched Software)**
    These vulnerabilities are likely to be exploited, especially if they are known to have active exploits.
  - **Medium (Open Ports)**
    Ports that are not needed or not well-protected should be closed to reduce the attack surface.

II. Immediate Containment Actions

- For the server exposed to the internet, I would immediately apply network segmentation or firewall rules to restrict access while we assess and remediate the vulnerabilities.
- I would work with the IT team to change any default credentials on all critical servers to strong, unique passwords and enforce multi-factor authentication where possible.

III. **Patch Management**

- I would coordinate with the IT and DevOps teams to apply patches for all high-severity vulnerabilities on the critical servers. This includes ensuring that all software and operating systems are updated to the latest versions.
- I would establish a phased patching approach for systems that are part of production environments to ensure minimal downtime and impact on business operations.

IV. **Configuration Management**

- Review and close any unnecessary open ports on the critical servers, particularly those exposed to the internet. I'd ensure that only required ports are open and where possible, limit access to specific IP ranges.
- Implement configuration changes based on security hardening guides, such as CIS Benchmarks, to further protect these servers.

V. **Perform Security Testing**

- After patching and configuration changes, I would conduct a follow-up vulnerability scan to verify that the vulnerabilities have been mitigated.
- I would also run a penetration test against the critical servers to ensure there are no remaining vulnerabilities that could be exploited.

VI. **Implement Continuous Monitoring**

- Set up continuous monitoring on critical servers for any signs of exploitation attempts, unauthorised access or unusual behaviour using SIEM and IDS/IPS tools.
- Ensure that alerts are configured for any failed login attempts or unexpected service restarts, which could indicate attempted exploitation.

VII. **Review Access Controls**

- Review user access controls and privilege levels to ensure the principle of least privilege is being followed. Reduce administrative privileges wherever possible and ensure only authorised personnel have access to critical servers.

VIII. **Documentation and Communication**

- Document the vulnerabilities identified, the remediation steps taken and any residual risks that might remain.

- Communicate the results and recommendations to management and stakeholders, including the need for regular vulnerability assessments and patch management processes.

IX. **Long-term Mitigation**

- Propose the implementation of an automated patch management system to ensure timely updates.
- Conduct regular security awareness training for IT staff and system administrators on the importance of maintaining secure configurations and password hygiene.

2. **Interviewer:** That's a good strategy. How would you ensure that such vulnerabilities are identified and mitigated earlier in the future?

Candidate:

I. **Implement a Robust Vulnerability Management Program**
Ensure regular vulnerability assessments and penetration testing are scheduled to proactively identify vulnerabilities before they can be exploited.

II. **Automated Patch Management**
Deploy an automated patch management system to keep software and systems up to date. This helps in applying patches as soon as they are available.

III. **Network Segmentation**
Review and enforce network segmentation to limit access to critical servers. Ensure that sensitive or critical systems are not directly exposed to the internet.

IV. **Continuous Monitoring and Threat Intelligence Integration**
Integrate threat intelligence feeds with the SIEM to automatically correlate and detect known vulnerabilities and threats, allowing for quicker response and remediation.

V. **Configuration Management and Hardening**
Implement a strict configuration management process, including baselining and regular reviews using tools like Ansible, Puppet or Chef for consistent security configurations.

VI. **Security Awareness Training**
Regularly train staff, particularly those managing critical servers, on security best practices and the importance of timely patching and remediation.

3. **Interviewer:** Good points. What steps would you take if the exposed server had already been compromised by an attacker?

Candidate:

1. **Incident Response Activation**
   Immediately activate the incident response plan and isolate the compromised server to prevent further spread or damage.

2. **Forensic Analysis**
   Perform a forensic analysis to determine the scope of the breach, the attacker's activities, the data accessed and any persistence mechanisms left behind by the attacker.

3. **Eradication and Recovery**
   Remove any malicious artifacts, backdoors or compromised accounts. Rebuild the server from a known good backup and ensure it is fully patched and configured securely before reintroducing it to the network.

4. **Review and Strengthen Security Posture**
   Conduct a post-incident review to identify gaps that allowed the compromise, update security policies and strengthen the overall security posture based on the lessons learned.