2025 CYBERSECURITY ATTACKS PLAYBOOKS

👉Prepared by :-

🌐Mahesh Sarjerao Girhe🌐

👉Linkedln :-

https://www.linkedin.com/in/maheshgirhe7875

TABLE OF CONTENTS

AI-ENHANCED PHISHING ATTACKS PLAYBOOK

1. PREPARATION

- **Create and Maintain a List of:**
  - **Approved Email Communication Tools**:
    - Identify all sanctioned email systems and ensure monitoring for unauthorised usage. o **Key User Groups**:
    - Executives, finance teams and high-value targets (HVTs) vulnerable to phishing attempts. o **Common Indicators of AI-Enhanced Emails**:
    - Abnormal linguistic patterns, overly personalised messages or AIgenerated content.
- **Email Templates**:
  - **Awareness Campaigns**:
    - Inform employees about AI-generated phishing tactics.
    - Provide guidance on recognising suspicious emails with examples. o **Internal Communication**:
    - Notify teams about the detection of AI-driven phishing campaigns.
  - **External Notifications**:
    - Alert partners or clients if they might be impacted by phishing targeting your organisation.
- **Ensure that:**
  - Email security solutions (e.g., DMARC, DKIM, SPF) are implemented and monitored.
  - Anti-phishing software detects:
    - Emails containing language indicative of AI tools (e.g., ChatGPT, Bard).
    - Highly personalised emails targeting HVTs.
    - Links leading to phishing sites hosted on compromised domains.
  - Multi-Factor Authentication (MFA) is enforced across all critical systems.
  - Training sessions on phishing simulations are conducted regularly.
- **Perform Fire Drills:**
  - Test the playbook with scenarios involving AI-driven phishing:
    - Highly personalised emails to HVTs.
    - Phishing links mimicking login portals.
  - Validate detection and response times.

    - Ensure escalation paths are updated.
- **Review Threat Intelligence:**
    - Monitor trends in AI-driven phishing attacks. ○ Review intelligence on compromised accounts or exploited platforms. ○ Analyse phishing sites for generative AI usage patterns.
- **Asset Inventory**:
    - Maintain a list of:
        - HVTs and their associated email accounts.
        - Domains used for corporate communications.
        - Approved third-party tools and services integrated with email.

2. DETECT

- **MD1. Identify Threat Indicators**:
    - **Alerts**:
        - **SIEM**:
        - Unusual email activity (e.g., multiple failed login attempts).
        - Sudden spikes in email traffic from external domains.
        - **Email Security Solutions**:
        - Flagged suspicious emails containing generative AI markers.
        - **Network Monitoring**:
        - Links leading to known phishing sites or credential harvesting.
    - **Notifications**:
        - Employees reporting phishing emails.
        - External vendors or clients flagging suspicious communication.
- **MD2. Identify Risk Factors**:
    - **Common Risks**:
        - Credential theft via fake login portals.
        - Deployment of malicious attachments (e.g., macros, Trojans).
    - **Company-Specific Risks**:
        - Potential financial losses or reputational damage. ▪ Exposure of proprietary data.
- **MD3. Data Collection**:
    - **Email Headers**:
        - Analyse metadata for spoofed addresses or unusual sending patterns. ○ **Attachments**:
        - Inspect for malicious macros or payloads. ○ **URLs**:
        - Validate links for phishing or C2 activity.
- **MD4. Categorise**:
    - Types of AI-Enhanced Phishing:
        - **Spear Phishing**: Highly personalised messages.
        - **Whaling**: Targeting executives with realistic-looking requests.

- **Business Email Compromise (BEC)**: Impersonating trusted entities.

- **MD5. Is it an Advanced Attack?**
  - If the attack uses deepfake audio or AI-enhanced emails:
    - Escalate to senior analysts or Incident Response Team (IRT).
- **MD6. Triage**:
  - Assess the impact:
    - Compromised accounts or credentials. ▪ Spread to other employees or clients.
- **MD7. Is it a False Positive?**
  - Document and close if verified as false. ○ If true, escalate and move to the **Analyse** phase.

3. ANALYSE

- **MA1. Verify**: ○ Cross-check phishing email details with reported IOCs.
- **MA2. Identify IOCs**:
  - Use tools like VirusTotal, URLScan or PhishTank to analyse:
    - URLs.
    - Email attachments. ▪ Sender domains.
- **MA3. Extract IOCs**:
  - Inspect logs for:
    - IPs or domains associated with phishing links. ▪ Sender email spoofing techniques.
- **MA4. Submit to Partners**: ○ Share IOCs with security vendors for signature updates.
- **MA5. Scan Enterprise**: ○ Search for affected users and suspicious email activity.

4. CONTAIN / ERADICATE

- **MC1. Contain**:
  - Quarantine phishing emails.
  - Lock compromised accounts and enforce MFA reset.
- **MC2. Eradicate**:
  - Remove phishing links from email servers.
  - Terminate malicious processes initiated via compromised accounts.
- **MC3. Validate**:
  - Ensure no residual phishing emails remain.
  - Confirm removal of all malicious artifacts.

5. RECOVER

- **MR1. Restore Operations**:

    - Re-enable affected accounts with secure credentials. o Educate impacted users on recognising phishing attempts.

6. LESSONS LEARNT

- **Conduct a Post-Incident Review**:
    - Improve detection strategies for AI-enhanced phishing. o Update the playbook with new tactics and response measures.
    - Enhance employee awareness and training based on the attack vector.

ADVANCED RANSOMWARE CAMPAIGNS PLAYBOOK

1. PREPARATION

- **Create and Maintain a List of**:
    - **Critical Assets**:
        - Identify high-value systems (e.g., financial servers, executive devices, databases).
        - Maintain a list of sensitive data repositories. o **Backup Systems**:
        - Ensure backups are performed regularly and stored securely offline.
    - **Key Executives and High-Value Targets (HVTs)**:
        - Identify individuals most likely to be targeted.
- **Email Templates**:
    - **Internal Communication**:
        - Notify employees of suspicious file downloads or ransomware activity.
        - Provide instructions for reporting suspicious behavior.
    - **External Notifications**:
        - Inform partners or vendors if they might be affected by the attack.
- **Ensure That**:
    - Endpoint Detection and Response (EDR) and antivirus tools are:
        - Configured to detect ransomware activities (e.g., file encryption, unusual process creation).
        - Updated regularly to include signatures for the latest ransomware variants. o Privileged Access Management (PAM) solutions enforce:
        - Least privilege access for all employees.
        - Time-bound access for administrative tasks.
    - Network segmentation restricts lateral movement across critical systems. o Multi-Factor Authentication (MFA) is enforced for all critical systems and VPNs.
- **Perform Fire Drills**:
    - Test playbook functionality quarterly.
    - Validate detection and response against scenarios like:
        - Rapid file encryption on shared drives.
        - Ransomware targeting HVTs.
    - Ensure escalation paths and contact lists are up to date.
- **Review Threat Intelligence**:
    - Monitor trends in ransomware campaigns (e.g., double extortion methods). o Investigate ransomware variants targeting your industry.
    - Review Indicators of Compromise (IOCs) from recent attacks.

- **Asset Inventory**:
  - Maintain an up-to-date inventory of:
    - Critical systems and their owners.
    - Backup systems and processes.
    - Tools used for file encryption or decryption.

2. DETECT

- **MD1. Identify Threat Indicators**:
  - **Alerts**:
    - **SIEM**:
    - Sudden spike in file encryption activities.
    - Anomalous file deletion or modification. ▪ **EDR**:
    - Processes mimicking ransomware behavior (e.g., high CPU usage, file renaming).
    - **Network Monitoring**:
    - Data exfiltration to external servers.
    - Connections to known ransomware command-and-control (C2) servers.
  - **Notifications**:
    - Users reporting:
    - Files with unusual extensions.
    - Ransom notes displayed on their devices.
- **MD2. Identify Risk Factors**:
  - **Common Risks**:
    - Data encryption leading to operational downtime.
    - Stolen data leaked online.
  - **Company-Specific Risks**:
    - Reputational damage if sensitive executive data is leaked. ▪ Financial losses from downtime or ransom payments.
- **MD3. Data Collection**:
  - **Process Analysis**:
    - Inspect processes encrypting large volumes of files. o **Network Traffic**:
    - Analyse outbound connections to C2 domains or IPs.
  - **Host Analysis**:
    - Examine encrypted files for common ransomware extensions.
- **MD4. Categorise**:
  - Types of Ransomware Attacks:
    - **Encryption**: Files locked with a ransom note.
    - **Exfiltration**: Sensitive data stolen and threatened to be leaked.
    - **Hybrid**: Encryption combined with exfiltration (double extortion).

- **MD5. Is it an Advanced Attack?**
  - If the attack targets HVTs or involves sophisticated tactics:
    - Escalate to Incident Response Team (IRT) and notify senior management.
- **MD6. Triage**:
  - Assess the scope of impact:
    - Number of affected hosts.
    - Potential exfiltration of sensitive data.
- **MD7. Is it a False Positive?**
  - Document and close if verified false. o If true, escalate and proceed to **Analyse**.

3. ANALYSE

- **MA1. Verify**:
  - Cross-check encryption behaviors with known ransomware signatures.
- **MA2. Identify IOCs**:
  - Use tools like VirusTotal, Any.Run and Hybrid Analysis to analyse:
    - Encrypted files.
    - Malicious executables. ▪ C2 domains or IPs.
- **MA3. Extract IOCs**:
  - Collect evidence from affected hosts:
    - Ransom notes.
    - Encryption keys (if visible).
    - Files modified during the attack.
- **MA4. Submit to Partners**:
  - Share samples with cybersecurity vendors for analysis and signature creation.
- **MA5. Scan Enterprise**:
  - Search for IOCs across the network and endpoints.
  - Ensure no lateral movement or additional infections.

4. CONTAIN / ERADICATE

- **MC1. Contain Affected Hosts**:
  - Isolate compromised systems using EDR solutions.
  - Block C2 domains and IPs at the firewall.
- **MC2. Eradicate**:
  - Terminate ransomware processes.
  - Delete malicious executables and artifacts.
- **MC3. Validate**:

    - Ensure all encrypted files and ransomware artifacts are removed. o Perform a network-wide scan to confirm no additional threats.

---

5. RECOVER

- **MR1. Restore Operations**:
    - Restore data from secure backups. o Reimage compromised systems. o Rotate credentials and enforce MFA on all accounts.

6. LESSONS LEARNT

- **Conduct a Post-Incident Review**:
    - Assess how ransomware bypassed existing defenses.
    - Enhance detection and response strategies for future attacks. o Update the playbook to include new IOCs and tactics observed during the incident.

SUPPLY CHAIN COMPROMISES PLAYBOOK

1. PREPARATION

- **Create and Maintain a Vendor Inventory**:
  - Identify all third-party vendors, partners and service providers.
  - Classify vendors by risk level based on the access they have to your systems.
- **Conduct Vendor Risk Assessments**:
  - Evaluate vendors' security postures regularly using:
    - Security questionnaires.
    - Vulnerability assessments or penetration tests.
  - Review vendors' compliance with standards (e.g., ISO 27001, SOC 2).
- **Implement Security Controls**:
  - **Access Management**:
    - Enforce least-privilege access for all vendor accounts.
    - Regularly audit and rotate credentials.
  - **Network Segmentation**:
    - Restrict third-party access to specific systems.
    - Use virtual private networks (VPNs) or zero-trust models for remote vendor access. o **Monitoring**:
    - Set up dedicated logging and monitoring for vendor activities.
- **Incident Response Preparation**:
  - Create tailored response plans for supply chain compromises.
  - Establish clear communication protocols with vendors during incidents. o Include clauses in contracts requiring vendors to notify you of breaches promptly.

2. DETECT

- **MD1. Identify Threat Indicators**:
  - **SIEM Alerts**:
    - Suspicious access patterns from vendor accounts.
    - Unauthorised access attempts to sensitive systems by third-party accounts. o **Endpoint Protection**:
    - Malware or tools used for lateral movement originating from thirdparty systems. o **Network Monitoring**:
    - Anomalous data transfers to vendor networks or external IPs.
- **MD2. Identify Risk Factors**:
  - **Common Risks**:
    - Exploited software updates from a vendor.
    - Compromised vendor credentials.

    - **Company-Specific Risks**:
        - Loss of sensitive customer or operational data.
        - Disruption of critical systems reliant on third-party software.
- **MD3. Data Collection**:
    - **Account Analysis**:
        - Investigate vendor account activity.
    - **Network Analysis**:
        - Review traffic patterns between your network and vendor systems. o **Log Analysis**:
        - Check for unusual activity correlated with vendor-related accounts or IPs.
- **MD4. Categorise**:
    - Types of Supply Chain Attacks:
        - **Software Exploitation**:
        - Malicious updates or patches from vendors.
        - **Credential Abuse**:
        - Stolen or compromised vendor credentials used for unauthorised access.
        - **Physical Device Compromise**:
        - Hardware shipped with malware or backdoors.
- **MD5. Is it an Advanced Attack?**
    - If the attack involves advanced persistence mechanisms or highly sensitive systems, escalate to senior incident response teams and threat intelligence analysts.
- **MD6. Triage**:
    - Assess the scope of impact:
        - Systems affected by the vendor's compromise. ▪ Data potentially exfiltrated or modified.
- **MD7. Is it a False Positive?**
    - If verified false, document and close the alert. o If true, proceed to **Analyse**.

3. ANALYSE

- **MA1. Verify**:
    - Confirm the vendor has been compromised using:
        - Threat intelligence feeds.
        - Public disclosures or notifications from the vendor.
- **MA2. Identify IOCs**:
    - Collect indicators associated with the vendor compromise, such as:
        - Malicious domains or IPs.
        - Hashes of compromised software files or malware.
- **MA3. Investigate Affected Systems**:

    - Review impacted systems for signs of compromise originating from vendorrelated activity.
- **MA4. Collaborate**:
    - Contact the vendor for additional details and updates. o Share findings and IOCs with internal teams and industry peers, if appropriate.
- **MA5. Scan Enterprise**: o Search for IOCs across the network, endpoints and critical systems.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat**:
    - Disable or restrict vendor accounts showing signs of compromise. o Block malicious IPs, domains or file hashes linked to the vendor compromise.
    - Isolate affected systems from the network.
- **MC2. Eradicate**:
    - Remove malicious files, malware or compromised software updates.
    - Patch vulnerabilities exploited during the attack.
- **MC3. Validate**:
    - Confirm no further unauthorised access or malicious activity is detected.

5. RECOVER

- **MR1. Restore Operations**:
    - Re-enable vendor access only after the issue has been resolved and additional controls are implemented.
    - Update affected systems and software with clean versions. o Notify internal teams and external stakeholders about the resolution.

6. LESSONS LEARNT • **Conduct a Post-Incident Review**:

    - Evaluate how the vendor compromise occurred and how it propagated into your environment.
    - Update vendor risk management policies and incident response plans based on the findings.
    - Strengthen monitoring and controls for vendor-related activities.

ZERO-DAY EXPLOITS PLAYBOOK

1. PREPARATION

- **Vulnerability Management**:

    - Maintain an up-to-date inventory of all software and hardware, including versions and patch status. ○ Monitor trusted vulnerability databases (e.g., CVE, NVD) and vendor advisories for emerging threats.
- **Threat Intelligence**:
    - Subscribe to feeds from vendors, government agencies and cybersecurity firms specialising in zero-day vulnerabilities. ○ Collaborate with information-sharing communities (e.g., ISACs) to gain early awareness.
- **Hardening Systems**:
    - Disable unused services and features. ○ Enforce strict application controls using tools like AppLocker or Software Restriction Policies.
    - Implement robust EDR/XDR solutions for anomaly detection.
- **Network Segmentation and Access Control**:
    - Segregate critical systems from general networks.
    - Enforce least-privilege access policies.
- **Incident Response Drills**:
    - Simulate zero-day scenarios to test detection and response capabilities.
    - Validate escalation paths and cross-team collaboration.
- **Vendor Communication**:
    - Establish direct lines of communication with software and hardware vendors for emergency patching guidance.
- **Document Security Policies**:
    - Ensure incident response, vulnerability management and patch management policies are comprehensive and regularly updated.

2. DETECT

- **MD1. Identify Threat Indicators**:
    - **SIEM Alerts**:
        - Anomalous application behaviors, such as unexpected service crashes or unusual privilege escalations. ○ **EDR/XDR Logs**:
        - Detection of code execution in unusual memory regions.
        - Indicators of exploitation, such as buffer overflows or heap sprays.
    - **Network Monitoring**:
        - Sudden spikes in outbound traffic or unusual connections to unfamiliar IPs/domains. ○ **Application Logs**:
        - Errors or anomalies indicating exploitation attempts.
- **MD2. Identify Risk Factors**:
    - **Common Risks**:
        - Data exfiltration and espionage.
        - Lateral movement to other systems. ○ **Company-Specific Risks**:
        - Disruption to business-critical operations.
        - Regulatory fines and reputational damage.

- **MD3. Data Collection**:
    - **Endpoint Analysis**:
        - Identify suspicious processes, memory dumps or injected code. o **Network Analysis**:
        - Collect traffic data related to suspected C2 communications.
    - **Log Analysis**:
        - Review system logs for anomalies around the time of suspected exploitation.
- **MD4. Categorise**:
    - Types of Zero-Day Attacks:
        - **Remote Code Execution (RCE)**: Exploits allowing arbitrary code execution.
        - **Privilege Escalation**: Gaining unauthorised system-level access. ▪ **Information Disclosure**: Exploits revealing sensitive data.
- **MD5. Is it an Advanced Attack?**
    - If sophisticated techniques such as obfuscation or multi-stage payloads are observed:
        - Escalate to threat intelligence and hunting teams. ▪ Notify senior leadership.
- **MD6. Triage**:
    - Assess scope and impact:
        - Identify affected systems, data compromised and potential lateral movement.
- **MD7. Is it a False Positive?**
    - Validate with additional analysis. If false, close the incident and document findings.

3. ANALYSE

- **MA1. Verify**:
    - Confirm the vulnerability exploited matches behaviors observed.
- **MA2. Identify IOCs**:
    - Gather and validate:
        - Exploit payloads or scripts.
        - Domains, IPs and hashes linked to the attack.
- **MA3. Forensic Analysis**:
    - Examine impacted systems for:
        - Exploited files or memory artifacts.
        - Evidence of persistence mechanisms.
- **MA4. Collaborate**:
    - Share findings with vendors and security communities to assist in patch development.

- **MA5. Enterprise-Wide Scan**:
    - Search for IOCs across systems and networks to ensure no further compromises.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat**:
    - Isolate affected systems to prevent lateral movement. ○ Block known malicious IPs, domains and hashes using network security tools.
- **MC2. Eradicate**:
    - Remove malware or persistence mechanisms.
    - Apply interim mitigations (e.g., disable vulnerable features).
- **MC3. Validate Remediation**:
    - Confirm no residual exploitation or IOCs remain active.

5. RECOVER

- **MR1. Restore Operations**:
    - Rebuild affected systems from secure backups.
    - Reapply patches or configurations once available.
- **MR2. Monitor**: ○ Keep systems under enhanced observation for recurring activity.

6. LESSONS LEARNT

- **Conduct Post-Incident Review**:
    - Analyse the attack's lifecycle, including how the zero-day was exploited and mitigated.
    - Update policies and playbooks to strengthen defenses against future zeroday exploits.
    - Improve threat intelligence sharing and vendor collaboration.

AI-POWERED MALWARE PLAYBOOK

1. PREPARATION

- **AI-Specific Threat Intelligence**:
    - Monitor industry reports and research on emerging AI-powered malware trends. ○ Participate in forums and information-sharing platforms to stay informed about the latest tactics.
- **Advanced Security Solutions**:

    - Deploy AI/ML-enhanced EDR and NDR tools capable of detecting adaptive and evolving malware. o Use behavior-based analysis to identify anomalies rather than relying solely on signatures.
- **System Hardening**:
    - Limit execution of unknown applications using application whitelisting.
    - Enforce strict privilege controls and disable unnecessary AI-enabled features in software.
- **Incident Response Enhancements**:
    - Train response teams on AI-powered malware scenarios, including its potential evasion tactics. o Establish playbooks for detecting and mitigating polymorphic or evolving threats.
- **Data Protection and Encryption**:
    - Encrypt sensitive data to limit exposure in case of a breach.
    - Regularly back up critical systems and store backups offline.
- **Threat Simulation Drills**:
    - Simulate AI-powered malware attacks to test detection and response effectiveness. o Validate escalation paths and update playbooks based on lessons learned.

2. DETECT

- **MD1. Identify Threat Indicators**:
    - **Behavioral Anomalies**:
        - Unusual system or network activity patterns that adapt over time.
    - **EDR Alerts**:
        - Rapid changes in malware signatures or behaviors, indicating potential adaptation. o **NDR Tools**:
        - Detection of evolving C2 communications using encrypted or covert channels. o **System Logs**:
        - Unexpected changes in process behavior or privilege escalation attempts.
- **MD2. Identify Risk Factors**:
    - **Common Risks**:
        - Data exfiltration via adaptive methods.
        - Persistent threats leveraging AI to avoid detection. o **Company-Specific Risks**:
        - Brand damage from prolonged malware presence.
        - Operational disruptions due to adaptive malware targeting critical systems.
- **MD3. Data Collection**:
    - **Endpoint Analysis**:

        - Capture and analyse malware samples using sandboxes or forensic tools. ○ **Network Analysis**:
        - Inspect traffic patterns for signs of AI-driven communication techniques (e.g., dynamic DNS, steganography). ○ **Memory Dumps**:
        - Look for signs of AI-enabled decision-making processes in malware payloads.
- **MD4. Categorise**:
    - Types of AI-Powered Malware:
        - **Polymorphic Malware**: Frequently changes its code to evade detection.
        - **Self-Learning Malware**: Adapts based on environment and security configurations.
        - **Steganographic Malware**: Uses AI to embed malicious code within benign files.
- **MD5. Is it an Advanced Attack?**
    - Escalate to senior analysts if malware demonstrates:
        - Adaptive communication techniques.
        - AI-driven decision-making capabilities.
- **MD6. Triage**:
    - Assess the malware's impact:
        - Systems affected, data compromised and potential for lateral movement.
- **MD7. Is it a False Positive?**
    - Validate alerts with threat intelligence and additional analysis.

3. ANALYSE

- **MA1. Verify**:
    - Confirm adaptive behaviors through sandbox testing or manual analysis.
- **MA2. Identify IOCs**:
    - Gather and validate:
        - Malware hashes, C2 domains and suspicious IPs.
        - Indicators of adaptive techniques (e.g., dynamic payload modifications).
- **MA3. Reverse Engineer**:
    - Use tools like Ghidra or IDA Pro to dissect AI-powered malware and understand its decision-making processes.
- **MA4. Collaborate**: ○ Share findings with vendors and threat intelligence communities.
- **MA5. Scan Enterprise**:

- Search for IOCs across endpoints, logs and network traffic to detect further infections.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat**:
  - Isolate infected systems. ○ Block malicious domains, IPs and communication patterns using firewall or DNS filtering.
- **MC2. Eradicate**:
  - Terminate malicious processes and remove associated files.
  - Implement stricter execution policies to prevent re-infection.
- **MC3. Validate Remediation**:
  - Scan all systems to ensure no traces of malware remain.

5. RECOVER

- **MR1. Restore Operations**:
  - Rebuild affected systems from clean backups.
  - Reassess security controls to prevent recurrence.
- **MR2. Enhanced Monitoring**:
  - Increase vigilance for evolving threats using AI/ML-based security solutions.

6. LESSONS LEARNT

- **Post-Incident Review**:
  - Analyse the malware's AI capabilities and the effectiveness of the response.
    - Update detection and response playbooks with findings.
  - Enhance training for security teams on handling AI-powered threats.

DEEPFAKE SOCIAL ENGINEERING PLAYBOOK

1. PREPARATION • **Training and Awareness**:

- Conduct regular employee training on identifying deepfake threats, including examples of audio and video manipulation. ○ Emphasise verification procedures, such as multi-channel communication (e.g., confirming requests via phone if received by email).

- **Security Policies**:
  - Mandate strict authentication protocols for sensitive requests, such as dual approval for financial transactions.
  - Enforce the use of secure communication channels for official interactions.

- **Technology Solutions**:
    - Implement deepfake detection tools and AI-based fraud monitoring solutions.
    - Use biometric authentication systems that are resistant to manipulation.
- **Incident Response Enhancements**:
    - Prepare response templates for potential deepfake incidents, such as public communication or employee alerts.
    - Create a decision tree for escalating suspected deepfake threats.
- **Threat Intelligence**:
    - Monitor advancements in deepfake technologies and track their use in cyberattacks.
    - Share intelligence on observed techniques with industry peers and threatsharing platforms.
- **Pretext Simulation Drills**:
    - Conduct phishing simulations involving potential deepfake scenarios to test employee response.

2. DETECT

- **MD1. Identify Threat Indicators**:
    - **Audio or Video Irregularities**:
        - Delayed or unnatural lip-syncing, inconsistent voice tonality or artifacts in video feeds. o **Suspicious Requests**:
        - Uncharacteristic urgency in requests from high-level executives.
    - **Behavioral Red Flags**:
        - Unusual phrasing or deviations from normal communication patterns.
- **MD2. Verify Authenticity**:
    - Confirm via secondary communication methods (e.g., direct phone calls or face-to-face confirmation). o Use tools like Sensity or Microsoft Video Authenticator to validate audio or video authenticity.
- **MD3. Data Collection**:
    - **Metadata Analysis**:
        - Review email headers, timestamps and file properties for anomalies. o **Network Logs**:
        - Check for external access to video conferencing or audio systems.
- **MD4. Categorise**:
    - Types of Deepfake Attacks:
        - **Impersonation**: High-level executives requesting sensitive actions.
        - **Blackmail**: Threats involving manipulated audio/video content. ▪ **Social Engineering**: Manipulated audio to deceive employees.
- **MD5. Is it a Sophisticated Threat?**

  - If the deepfake bypasses detection tools or uses advanced methods, escalate to senior analysts.
- **MD6. Triage**:
  - Assess the impact:
    - Determine if any sensitive information has been divulged. ▪ Identify targeted individuals and the scope of the attack.
- **MD7. Is it a False Positive?**
  - If proven legitimate, document the findings and close the incident.

3. ANALYSE

- **MA1. Verify Incident Scope**:
  - Cross-check logs, emails and communications to determine the attack vector.
- **MA2. Identify IOCs**:
  - Validate suspicious files or communications using tools like VirusTotal or Maltego.
- **MA3. Reverse Engineer**:
  - Analyse deepfake audio/video using forensic tools to understand the source and methods used.
- **MA4. Collaborate**: o Share findings with security vendors and intelligence-sharing networks.
- **MA5. Scan Enterprise**: o Search for signs of similar deepfake attempts across the organisation.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat**:
  - Block communication from identified sources (e.g., spoofed emails or phone numbers).
  - Temporarily disable affected accounts or communication channels.
- **MC2. Eradicate**:
  - Remove or block malicious files and revoke any unauthorised access.
  - Strengthen affected protocols and processes to prevent reoccurrence.
- **MC3. Validate**:
  - Ensure all traces of the attack are mitigated. o Test deepfake detection tools to confirm proper functioning.

5. RECOVER • **MR1. Restore Confidence**:

  - Notify affected parties of resolved threats and ensure transparent communication.

    - Provide updated training and guidelines to employees.
- **MR2. Technology Updates**:
    - Upgrade detection tools and reinforce authentication mechanisms.

6. LESSONS LEARNT

- **Post-Incident Review**:
    - Analyse the effectiveness of deepfake detection and response. o Update training materials and playbooks with lessons learned. o Identify gaps in processes and deploy solutions to address them.

QUANTUM COMPUTING THREATS PLAYBOOK

1. PREPARATION • **Understand Quantum Risks**:

o Train security teams on quantum computing and its potential impact on cryptography. o Evaluate the organisation’s cryptographic landscape to identify vulnerabilities to quantum decryption.

- **Cryptographic Inventory**:
    - Maintain a comprehensive list of encryption methods and keys in use. o Identify legacy cryptographic protocols (e.g., RSA, ECC) that are vulnerable to quantum attacks.
- **Adopt Quantum-Resistant Cryptography**:
    - Transition to quantum-safe algorithms as recommended by NIST's PostQuantum Cryptography (PQC) standards. o Begin hybrid implementations combining classical and quantum-resistant cryptography to ease the transition.
- **Secure Communication Channels**:
    - Deploy secure key exchange mechanisms resistant to quantum threats (e.g., lattice-based cryptography). o Implement forward secrecy for encrypted communications to prevent future decryption.
- **Vendor Assessment**:
    - Collaborate with vendors to ensure they are adopting quantum-safe technologies.
    - Require third-party vendors to disclose their cryptographic practices.
- **Scenario Simulations**:
    - Conduct tabletop exercises simulating quantum decryption threats, focusing on data breaches and cryptographic failures.
- **Threat Intelligence Monitoring**:

    - Track advancements in quantum computing capabilities and monitor industry trends.
    - Watch for early indicators of potential quantum decryption tools.
- **Data Classification and Prioritisation**:
    - Identify and categorise sensitive data based on its exposure risk and encryption strength.

2. DETECT

- **MD1. Identify Indicators of Compromise (IOCs)**:
    - **Cryptographic Failures**:
        - Sudden decryption of encrypted files or traffic.
        - Unauthorised access to encrypted databases.
    - **Anomalous Network Activity**:
        - Increased computational power in network communications indicating potential quantum decryption attempts.
- **MD2. Monitor for Quantum Tools**:
    - Observe for emerging tools or platforms leveraging quantum computing for cryptographic analysis.
- **MD3. Data Collection**:
    - **Encryption Logs**:
        - Review logs for anomalies in encryption and decryption operations.
    - **Network Traffic**:
        - Monitor for brute-force decryption attempts on encrypted communications.
- **MD4. Categorise Quantum Threats**:
    - Identify threats as:
        - **Cryptographic Attacks**: Breaking current encryption.
        - **Data Harvesting**: Storing encrypted data for future quantum decryption.
- **MD5. Is it a Quantum Threat?**
    - Confirm with advanced analysis tools if anomalous activity suggests quantum decryption.
- **MD6. Triage**:
    - Assess the scope of the threat:
        - Data at risk.
        - Affected systems.
        - Potential long-term impact.
- **MD7. Is it a False Positive?**
    - If confirmed as false, document findings and close the case. If true, escalate to senior analysts.

3. ANALYSE

- **MA1. Verify Incident Scope**:
  - Cross-check logs, encryption protocols and threat intelligence sources.
- **MA2. Identify IOCs**:
  - Use tools like Wireshark, Seek and Maltego to analyse network traffic and cryptographic anomalies.
- **MA3. Reverse Engineer**:
  - Investigate the methods used in suspected quantum-based attacks to determine the cryptographic weaknesses exploited.
- **MA4. Collaborate**:
  - Share findings with government agencies, industry peers and cryptographic standard bodies.
- **MA5. Enterprise Scan**:
  - Search systems for similar vulnerabilities and potential data harvesting activities.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat**:
  - Disable vulnerable cryptographic protocols on affected systems.
  - Isolate compromised networks and assets.
- **MC2. Mitigation**:
  - Apply immediate patches or upgrades to affected cryptographic tools.
  - Re-encrypt sensitive data with quantum-safe algorithms.
- **MC3. Validate**:
  - Verify the integrity of systems and data after containment. o Conduct penetration testing to ensure vulnerabilities are addressed.

5. RECOVER • **MR1. Restore Operations**:

  - Reintegrate systems into the production environment after thorough validation.
  - Restore data from secure, quantum-safe backups if necessary.
- **MR2. Strengthen Defenses**:
  - Accelerate the transition to post-quantum cryptographic standards. o Implement quantum-resilient key management systems.

6. LESSONS LEARNT

- **Post-Incident Review**:

    - Evaluate the effectiveness of quantum-resilient preparations and response efforts. o Identify areas for improvement in encryption practices and incident response processes. o Update the playbook with new insights and ensure alignment with evolving quantum-safe standards.

IoT VULNERABILITIES PLAYBOOK

1. PREPARATION

- **Inventory and Asset Management**:
    - Maintain an up-to-date inventory of all IoT devices within the network, including their make, model, firmware version and purpose.
    - Categorise devices based on criticality and sensitivity of data they handle.
- **IoT Security Policies**:
    - Establish IoT-specific security policies, such as requiring strong, unique passwords and disabling unused features. o Implement network segmentation to isolate IoT devices from critical infrastructure.
- **Firmware and Patch Management**:
    - Regularly update IoT device firmware and apply patches provided by manufacturers.
- **Secure Configuration**:
    - Disable default credentials and unnecessary services. o Enable secure communication protocols (e.g., TLS) and disable unsecured protocols (e.g., Telnet).
- **Monitoring and Logging**:
    - Enable logging on IoT devices to track activity and identify anomalies.
    - Integrate IoT logs with SIEM for centralised monitoring.
- **Threat Intelligence**: o Stay updated on vulnerabilities and attack trends affecting IoT devices.
- **Employee Awareness**:
    - Train employees to recognise and report suspicious IoT-related activities or device malfunctions.

2. DETECT

- **MD1. Identify Indicators of Compromise (IOCs)**:
    - **Unusual Network Traffic**:
        - Unexpected traffic originating from IoT devices, especially to unfamiliar IP addresses. o **Device Behavior**:

        - Sudden reboots, unresponsive devices or unauthorised configuration changes. o **Credential Abuse**:
        - Multiple failed login attempts, indicating potential brute-force attacks.
- **MD2. Monitor for Exploitation**:
    - Use intrusion detection systems (IDS) to monitor network activity for known IoT attack patterns.
- **MD3. Data Collection**:
    - **Device Logs**: Review logs for anomalous commands or unauthorised access attempts.
    - **Network Traffic Analysis**: Use tools like Wireshark or Seek to analyse traffic from IoT devices.
- **MD4. Categorise Threats**:
    - Determine if the anomaly is related to:
        - Botnet activity (e.g., DDoS attacks).
        - Unauthorised data access or exfiltration. ▪ Malware infection.
- **MD5. Validate IOCs**:
    - Cross-reference suspicious activity with threat intelligence sources.

3. ANALYSE

- **MA1. Scope the Incident**:
    - Identify affected devices, compromised data and the potential impact on operations.
- **MA2. Identify Exploitation Method**:
    - Investigate how the vulnerability was exploited (e.g., outdated firmware, weak credentials).
- **MA3. Reverse Engineer Attacks**:
    - Analyse malware or exploit payloads using tools like IDA Pro or Cuckoo Sandbox to understand their behavior.
- **MA4. Collaboration**:
    - Share findings with the IoT device manufacturer and peers in the industry for coordinated mitigation efforts.
- **MA5. Broader Analysis**: o Scan for similar vulnerabilities across all IoT devices within the network.

4. CONTAIN / ERADICATE • **MC1. Isolate Compromised Devices**:

    - Disconnect affected IoT devices from the network to prevent further spread of the attack.
- **MC2. Apply Fixes**:
    - Patch vulnerabilities or upgrade firmware for affected devices.

    - Reset devices to factory settings if necessary and reconfigure securely.
- **MC3. Strengthen Defenses**:
    - Change device passwords and enforce multi-factor authentication (MFA) where possible.
    - Block known malicious IPs or domains in network firewalls.
- **MC4. Verify Containment**:
    - Monitor the network to ensure no residual malicious activity.

5. RECOVER • **MR1. Restore Normal Operations**:

    - Reinstate affected devices into the network only after thorough validation and testing.
    - Recover any compromised data from secure backups.
- **MR2. Enhance IoT Security**:
    - Implement additional security measures, such as device-specific firewalls or access controls. o Regularly review and update IoT security policies.

6. LESSONS LEARNT

- **Post-Incident Review**:
    - Document the incident, including root cause, timeline, response efforts and outcomes.
    - Identify gaps in IoT security practices and update the playbook accordingly.
- **Future Mitigation**:
    - Collaborate with IoT manufacturers to address systemic vulnerabilities.
    - Deploy automated tools for continuous IoT vulnerability scanning.

INSIDER THREATS PLAYBOOK

1. PREPARATION • **Access Management**:

    - Enforce least privilege principles: limit access to sensitive data and systems to only those who need it.
    - Implement role-based access controls (RBAC).
- **Policies and Training**:
    - Establish clear policies on acceptable use, data handling and incident reporting.
    - Conduct regular security awareness training, emphasising the risks of insider threats.
- **Monitoring and Logging**:

  - Deploy user activity monitoring tools (e.g., User Behavior Analytics - UBA). o Enable detailed logging for critical systems, including file access, email activity and network connections.
- **Background Checks**:
  - Conduct thorough pre-employment screenings for employees and contractors.
- **Incident Response Preparation**:
  - Predefine response protocols for suspected insider threats, including escalation paths and containment strategies.
  - Maintain an up-to-date list of internal and external stakeholders for rapid communication.
- **Threat Intelligence**:
  - Monitor industry-specific trends and tactics used in insider threat cases.

2. DETECT

- **MD1. Identify Indicators of Insider Threats**:
  - **Anomalous Behavior**:
    - Unusual access patterns, such as accessing systems or data outside of work hours.
    - Attempts to access data or systems beyond the user's role or need.
  - **Performance Issues**:
    - Increased complaints about system performance, indicating potential data exfiltration. o **Behavioral Changes**:
    - Sudden changes in employee behavior, such as disengagement or unexplained absences.
- **MD2. Monitoring Tools**:
  - UBA systems for detecting deviations from normal user behavior.
  - DLP (Data Loss Prevention) tools to monitor for sensitive data exfiltration.
- **MD3. Data Collection**:
  - Analyse:
    - Logs from file servers, email systems and cloud applications.
    - USB and removable media usage logs.
  - Correlate activity using SIEM to identify patterns of abuse or negligence.
- **MD4. Categorise Threats**:
  - **Types of Insider Threats**:
    - Malicious: Intentional actions to harm the organisation.
    - Negligent: Unintentional actions compromising security (e.g., accidental data exposure).
    - Compromised: Employees coerced by external actors.

3. ANALYSE

- **MA1. Scope the Incident**:
    - Identify the affected systems, data accessed and whether the insider acted maliciously or negligently.
- **MA2. Examine Logs and Activities**:
    - Review logs to pinpoint unauthorised or suspicious activities.
    - Analyse email communications for signs of data sharing or external coordination.
- **MA3. Verify Intent**:
    - Interview employees or contractors to understand the context of their actions. o Cross-check their activities against established access policies and permissions.
- **MA4. Collaboration**:
    - Work with HR, legal and management teams to determine intent and appropriate next steps.

4. CONTAIN / ERADICATE • MC1. Contain Insider Actions:

- Immediately revoke or restrict the individual's access to systems and sensitive data.
- Temporarily isolate affected systems to prevent further damage or data exfiltration.

- **MC2. Investigate and Remediate**:
    - If the threat was negligent, provide retraining and implement stricter controls.
    - If malicious, involve legal and law enforcement teams to pursue necessary actions.
- **MC3. Validate Security**:
    - Perform a comprehensive audit to ensure no residual threats exist.
    - Update access permissions and monitor systems for similar behavior.

5. RECOVER

- **MR1. Resume Normal Operations**:
    - Reinstate affected systems after thorough validation.
    - If applicable, restore deleted or compromised data from backups.
- **MR2. Strengthen Defenses**:
    - Refine access controls and enforce stricter monitoring policies. o Deploy additional security tools, such as advanced DLP or identity management solutions.

6. LESSONS LEARNT

- **Post-Incident Review**:
  - Document the incident’s timeline, root cause and resolution.
  - Identify process and policy gaps that allowed the incident to occur.
- **Enhance Security Posture**:
  - Update insider threat detection tools and policies based on findings.
  - Schedule additional security awareness training, focusing on insider threats.
- **Proactive Threat Hunting**:
  - Regularly review activity logs and access patterns to identify potential insider threats early.

CLOUD SECURITY MISCONFIGURATIONS PLAYBOOK

1. PREPARATION

- **Cloud Security Policies**:
  - Define clear policies for configuring and managing cloud services. o Enforce compliance with industry standards like CIS Benchmarks for cloud security.
- **Access Controls**:
  - Implement role-based access control (RBAC) and the principle of least privilege.
  - Use Multi-Factor Authentication (MFA) for accessing cloud resources.
- **Configuration Management**:
  - Use Infrastructure as Code (IaC) tools like Terraform or CloudFormation to manage configurations.
  - Maintain an inventory of cloud resources and their configurations.
- **Monitoring and Logging**:
  - Enable logging and monitoring features, such as AWS CloudTrail, Azure Monitor or Google Cloud Logging.
  - Use centralised SIEM solutions to analyse cloud activity logs.
- **Training and Awareness**:
  - Provide regular training for cloud administrators to ensure they understand best practices and common pitfalls.
- **Automated Security Tools**:
  - Deploy tools like AWS Config, Azure Security Center or Prisma Cloud for continuous configuration assessments.

2. DETECT

- **MD1. Identify Indicators of Misconfigurations**:

  - **Open Access Issues**:
    - Publicly accessible storage buckets (e.g., AWS S3, Azure Blob).
    - Over-permissive IAM roles allowing unintended actions. o **Unencrypted Data**:
    - Sensitive data stored without encryption at rest or in transit.
  - **Audit Failures**:
    - Logs or alerts indicating suspicious activity or changes to configurations.
- **MD2. Monitor Key Areas**:
  - Storage buckets, databases and virtual machines for public exposure. o Network configurations, such as overly permissive security group rules.
  - Access logs for unusual or unauthorised activities.
- **MD3. Utilise Automated Tools**:
  - Cloud-native tools like AWS Trusted Advisor, Azure Defender or Google Security Command Center.
  - Third-party tools like Tenable, Qualys or Wiz for broader cloud misconfiguration detection.

3. ANALYSE

- **MA1. Scope the Misconfiguration**:
  - Identify which resources are affected and the potential data exposed.
  - Determine the root cause, such as human error, lack of oversight or flawed automation scripts.
- **MA2. Assess Impact**:
  - Quantify the data exposed and the risk to the organisation.
  - Identify whether the misconfiguration has been exploited (e.g., unauthorised access or data downloads).
- **MA3. Validate Logs and Alerts**:
  - Review logs to confirm unauthorised access attempts or changes to configurations.
  - Correlate with threat intelligence to assess the likelihood of exploitation.
- **MA4. Engage Relevant Teams**:
  - Coordinate with cloud administrators, security teams and legal/compliance teams as needed.

4. CONTAIN / ERADICATE • MC1. Secure Misconfigured Resources:

  - Immediately correct the misconfiguration (e.g., make the storage bucket private or restrict overly permissive IAM roles).
  - Revoke unauthorised access or over-permissive credentials.
- **MC2. Validate Security Controls**:

    - Enable encryption for sensitive data at rest and in transit.
    - Update network security group rules to minimise exposure.
- **MC3. Conduct Forensic Analysis**:
    - Analyse logs for signs of exploitation during the period of misconfiguration.
    - Capture any evidence of unauthorised access or data theft for further investigation.

5. RECOVER • **MR1. Restore Configurations**:

    - Ensure all affected resources are securely reconfigured following best practices.
    - Use automated tools to validate configuration compliance.
- **MR2. Notify Stakeholders**:
    - Inform affected parties, such as clients or regulators, if sensitive data was exposed.
    - Provide transparency about the steps taken to resolve the issue.
- **MR3. Conduct Post-Incident Testing**:
    - Perform penetration tests or red-team exercises to validate the security of the cloud environment.

6. LESSONS LEARNT

- **Post-Incident Review**:
    - Document the incident, including root cause analysis and resolution steps.
    - Share findings with stakeholders and incorporate lessons into training.
- **Strengthen Configuration Management**:
    - Use automated CI/CD pipelines to deploy secure configurations.
    - Regularly audit cloud configurations for compliance and vulnerabilities.
- **Enhance Monitoring and Response**:
    - Set up alerts for common misconfigurations and unauthorised activities. o Train incident response teams on cloud-specific threats and resolutions.

ADVANCED PERSISTENT THREATS (APTs) PLAYBOOK

1. PREPARATION

- **APTs Awareness and Training**:
  - Provide regular training for employees on recognising signs of APT activity, including spear-phishing attempts and unusual behavior. o Conduct workshops to educate IT staff about APT tactics, techniques and procedures (TTPs).
- **Network Segmentation**:
  - Implement strong segmentation to limit the movement of APT actors within the network.
  - Ensure that sensitive data and critical systems are isolated from the general network.
- **Endpoint Detection and Response (EDR) Implementation**:
  - Ensure that EDR tools are in place on all endpoints to monitor for advanced, subtle APT indicators (e.g., living-off-the-land techniques, credential dumping). o Configure alerts for unusual user or process behaviors indicative of an APT attack (e.g., large-scale data movement, lateral movement).
- **Threat Intelligence Feeds**:
  - Integrate global and industry-specific threat intelligence feeds to stay up-todate on the latest APT tactics and tools. o Share and receive threat intelligence with trusted partners and government entities for a broader understanding of emerging threats.
- **Incident Response Plan**:
  - Develop a detailed incident response plan specifically for APTs, including coordination between different teams (e.g., IT, legal, public relations).
  - Designate a response team that specialises in handling advanced attacks and ensure that all team members are familiar with the playbook.
- **Red Team Exercises**:
  - Conduct simulated APT scenarios to test the organisation's readiness and identify gaps in detection and response capabilities.

2. DETECT

- **MD1. Identify Indicators of Compromise (IOCs)**:
  - **SIEM Alerts**:
    - Unusual authentication attempts or login patterns (e.g., failed logins followed by successful logins).
    - Suspicious lateral movement or privilege escalation.

        - Evidence of tools commonly used in APT campaigns (e.g., Mimikatz, Cobalt Strike).
    - **Network Traffic Anomalies**:
        - Communication with known APT infrastructure (e.g., C2 servers, command-and-control domains).
        - Unusual outbound traffic or data exfiltration patterns.
    - **File Integrity Monitoring**:
        - Detection of new or altered files, especially in sensitive directories. ▪ Changes to critical system configurations or registry settings.
- **MD2. Identify Threat Actor TTPs**:
    - Review MITRE ATT&CK framework for known APT techniques and tactics used by specific threat actor groups. ○ Monitor for behavior indicative of known APT groups, including spearphishing emails, use of legitimate administrative tools for malicious purposes and living-off-the-land techniques.
- **MD3. Monitor for Low-and-Slow Attacks**:
    - APTs often operate slowly and stealthily to avoid detection. Set up monitoring for long-term, low-frequency activity (e.g., incremental data exfiltration). ○ Look for irregularities over extended periods, such as dormant backdoors that activate later or slow data gathering.

3. ANALYSE

- **MA1. Confirm IOC Matches**:
    - **IOC Validation**:
        - Use tools like VirusTotal, Hybrid Analysis and Threatminer to validate IOCs (IPs, hashes, domains) against known databases.
        - Cross-check network traffic, file hashes and suspicious domain names against threat intelligence sources.
- **MA2. Evaluate the Scope of the Attack**:
    - Identify which systems or users are affected. Look for signs of lateral movement or other compromised accounts that indicate a broader breach. ○ Conduct forensic analysis of endpoint activity to map out attacker behavior and identify tools used.
- **MA3. Correlate with Threat Intelligence**:
    - Compare attack patterns with known APT groups and their historical activity (e.g., APT28, APT29, Cozy Bear, Charming Kitten). ○ Analyse metadata, TTPs and known techniques to identify potential attribution to a specific threat actor group.
- **MA4. Perform Root Cause Analysis**:
    - Determine the initial entry point (e.g., spear-phishing email, exploit of an unpatched vulnerability) and how the attacker gained access to the network.

    - Identify any vulnerabilities or gaps in security that were exploited, such as unpatched systems or weak access controls.

- **MA5. Escalate if Necessary**:
    - If the attack appears to be part of a broader APT campaign, escalate to a specialised incident response team, threat hunting team or external experts.
    - Notify law enforcement if the attack is determined to be state-sponsored or part of a larger geopolitical threat.

4. CONTAIN / ERADICATE • MC1. Isolate Compromised

Systems:

- Use EDR tools to isolate infected machines and prevent further lateral movement within the network.
- Block or contain traffic to C2 servers and known malicious IP addresses.

- **MC2. Terminate Malicious Processes**:
    - Identify and terminate active malware or backdoor processes. Use memory analysis to track and kill hidden processes or payloads.
    - Revoke any compromised credentials and reset administrative passwords.
- **MC3. Remove Persistence Mechanisms**:
    - Check for and remove any persistence mechanisms used by the attacker (e.g., scheduled tasks, registry keys or backdoor user accounts). ○ Ensure that no traces of the attack are left behind in the form of hidden files, malware or modifications to system settings.
- **MC4. Strengthen Security Posture**:
    - Patch vulnerabilities exploited during the attack and harden systems to prevent further compromises. ○ Ensure that multi-factor authentication (MFA) is enabled for all critical access points.

5. RECOVER • MR1. Restore Systems and Data:

- Reimage infected systems and restore data from secure backups to ensure no malicious remnants remain. ○ Validate that the recovery process does not reintroduce any malware or vulnerabilities.

- **MR2. Test for Re-entry**:
    - Conduct penetration tests or red-team exercises to verify that the APT group cannot re-enter the network using the same methods.
    - Validate that all system and network defenses are functioning as intended.
- **MR3. Communicate with Stakeholders**:
    - Notify internal and external stakeholders, including clients, vendors and regulators, if sensitive data was exfiltrated or compromised. ○ Provide

updates on the status of the investigation and any preventive measures taken to address the APT.

6. LESSONS LEARNT • **Post-Incident Review**:

- Conduct a thorough review of the attack, identifying strengths and weaknesses in the detection, containment and eradication processes.
- Update incident response plans and security controls based on lessons learned.

- **Improve Detection Capabilities**:
  - Enhance detection mechanisms for low-and-slow APT activity, including better network traffic analysis and file integrity monitoring.
  - Implement advanced behavior analytics tools to detect anomalies associated with APT TTPs.
- **Collaborate with Industry Peers**:
  - Share findings with industry peers and threat intelligence communities to better understand emerging APT tactics and tools.
  - Contribute to threat intelligence feeds and collaborate with law enforcement when necessary.
- **Update Security Infrastructure**:
  - Invest in next-gen endpoint protection, threat hunting capabilities and continuous monitoring systems to proactively detect future APTs.
  - Increase training efforts to raise awareness about APTs across the organisation.

CREDENTIAL STUFFING ATTACKS PLAYBOOK

1. PREPARATION • **Password Hygiene and**

Policies:

- Enforce strong password policies, requiring complex, unique passwords for all user accounts.
- Educate users about the dangers of reusing passwords across multiple sites and encourage the use of password managers.

- **Multi-Factor Authentication (MFA)**:
  - Require MFA for all critical systems and applications, especially for administrative accounts and accounts containing sensitive data.
  - Configure MFA methods that are resistant to bypassing, such as hardware tokens or mobile app-based authenticators.
- **Monitoring and Detection Setup**:
  - Implement robust account login monitoring using SIEM solutions to track failed login attempts, especially from unusual IP addresses or locations.
  -

Set up thresholds for failed login attempts and configure alerts for abnormal spikes in login failures.

- **Rate Limiting and CAPTCHA**:
    - Enable rate limiting to restrict the number of login attempts within a specific time frame, preventing attackers from brute-forcing credentials. ○ Implement CAPTCHA challenges on login pages to thwart automated login attempts.
- **Threat Intelligence Feeds**:
    - Subscribe to breach notification services and threat intelligence feeds that provide data on compromised credentials and known botnet IP addresses. ○ Regularly update blacklists to block IP addresses associated with known attack sources.
- **Red Team and Penetration Testing**:
    - Conduct regular penetration tests to simulate credential stuffing attacks and identify weaknesses in authentication systems.
    - Test the effectiveness of MFA, rate limiting and CAPTCHA systems against real-world credential stuffing tactics.

2. DETECT

- **MD1. Monitor Failed Login Attempts**:
    - **SIEM Alerts**:
        - Alert on unusually high numbers of failed login attempts from the same IP address or geographical region.
        - Track failed login attempts that match usernames or email addresses across different platforms.
        - Watch for repeated login failures from various IP addresses attempting to access a single account.
- **MD2. Detect Abnormal IP Addresses and Geographies**:
    - Use geolocation data to identify logins from unexpected regions, especially when an account typically logs in from a different location. ○ Detect the use of proxy or VPN services to mask the true origin of login attempts.
- **MD3. Recognise Credential Reuse**:
    - Cross-reference login attempts with known compromised password databases (e.g., HaveIBeenPwned) to identify if an account is using a stolen password combination. ○ Set up alerts when accounts show a pattern of matching credentials that have appeared in previous breaches.
- **MD4. Analyse Account Lockouts and Suspicious Activity**:
    - Trigger alerts for account lockouts after a predefined number of failed login attempts. ○ Monitor for accounts that are locked after repeated failed login attempts, indicating potential automated attacks.

3. ANALYSE

- **MA1. Confirm Indicators of Credential Stuffing**:
  - **IOCs**:
    - Numerous login attempts with different combinations of usernames and passwords within a short period.
    - Login attempts from known bad IP addresses or proxies.
  - Validate failed login attempts against breached credential databases (e.g., checking if login attempts match known leaked credentials).
- **MA2. Investigate Suspicious Accounts**:
  - Review login history and behaviors for accounts experiencing high failure rates. Look for patterns indicating they are targets of credential stuffing.
  - Examine account activities after successful logins from unauthorised sources to determine if any unusual actions or access occurred.
- **MA3. Review CAPTCHA or Rate Limiting Efficacy**:
  - Verify that CAPTCHA or rate limiting is being correctly triggered after a threshold number of failed login attempts. o Check if the attacks are bypassing rate-limiting mechanisms or CAPTCHA challenges (e.g., through botnets or CAPTCHA solving services).
- **MA4. Correlate with Threat Intelligence**:
  - Cross-reference observed attack patterns (e.g., IP addresses, behavior) with known credential stuffing campaigns. o Analyse trends in attack attempts based on recent data from threat intelligence sources.
- **MA5. Assess the Impact of the Attack**:
  - Determine if any accounts were successfully compromised and identify the scope of the breach. o Evaluate any exfiltration of data or other malicious activity linked to the attack.

4. CONTAIN / ERADICATE • MC1. Block

Malicious IP Addresses:

o Use firewall rules or SIEM to automatically block IP addresses exhibiting suspicious activity, such as high rates of failed login attempts. o Add known botnet IP addresses and proxy servers to the blocklist to prevent further login attempts.

- **MC2. Implement Account Lockouts and Reset Credentials**:
  - Lock out accounts that are under attack and reset their passwords to prevent unauthorised access.
  - Notify affected users to change their passwords and enforce strong authentication measures.
- **MC3. Enforce Multi-Factor Authentication (MFA)**:

    - Immediately enforce MFA for all user accounts, especially for those potentially compromised during the attack. ○ Implement additional layers of authentication for accounts that were targeted or affected.
- **MC4. Strengthen Authentication Systems**:
    - Tighten rate-limiting mechanisms and CAPTCHA rules to prevent automated login attempts. ○ Implement bot detection tools that use machine learning to detect automated login behavior.
- **MC5. Disable Stolen Credentials**:
    - If possible, disable accounts that are suspected to be using stolen credentials to prevent further unauthorised access.
    - Use breach notification services to identify and protect other accounts that may be impacted by the same stolen credentials.

5. RECOVER • **MR1. Restore Access for**

Legitimate Users:

○ Ensure that legitimate users can regain access to their accounts by resetting their credentials and enabling MFA. ○ Provide support for users who are locked out or unable to access their accounts.

- **MR2. Investigate Data Breach Impact**:
    - If data was accessed or exfiltrated, conduct a detailed investigation to determine the scope of the breach.
    - Notify users if their data was compromised and provide them with necessary steps to secure their accounts.
- **MR3. Perform Root Cause Analysis**:
    - Assess how the credential stuffing attack bypassed current security measures (e.g., weak rate limiting or inadequate CAPTCHA).
    - Analyse logs, review attack patterns and identify areas for improvement in the authentication system.
- **MR4. Test Recovery Procedures**:
    - Ensure that all security measures are functional after the attack, including account lockout systems, CAPTCHA and rate limiting. ○ Verify that no accounts remain compromised and that all systems are secure before restoring full access.

6. LESSONS LEARNED • **Post-Incident**

Review:

○ Hold a meeting with relevant stakeholders (security, IT, user support) to review the response to the credential stuffing attack. ○ Identify areas where response time could be improved and whether detection capabilities need to be enhanced.

- **Improve Detection and Prevention Mechanisms**:
  - Update and improve rate-limiting rules to ensure they trigger faster and more effectively for login attempts. ○ Enhance CAPTCHA and bot-detection mechanisms to prevent further automation-based attacks.
- **Update Password and Authentication Policies**:
  - Consider implementing passwordless authentication methods or requiring stronger passwords for high-value accounts. ○ Enforce stronger password policies and more frequent password changes, especially for users with access to critical systems.
- **Increase User Awareness and Education**:
  - Continue educating users on the risks of credential stuffing and the importance of using strong, unique passwords for each service. ○ Provide guidance on setting up MFA and encourage its use across all accounts.

FILELESS MALWARE PLAYBOOK

1. PREPARATION

- **Create and Maintain a List of** ○ All software and applications approved for use in the organisation.
    - Helps detect unauthorised tools and prevent misuse.
  - Users with access to tools that can execute code in memory (e.g., PowerShell, WMI, scripts).
- **Email Templates** ○ Notify employees about suspicious script activities or memory-based attacks. ○ Communicate with internal teams regarding proactive measures (e.g., disabling macros by default).
  - Notify external vendors if vulnerabilities in their products are exploited.
- **Ensure that:**
  - Endpoint Detection and Response (EDR) solutions are capable of monitoring script activities.
  - Detection exists for unusual behaviours like:
    - PowerShell commands without files.
    - Processes launching from memory.
    - Usage of tools like MSHTA, BITSAdmin or CertUtil.
  - Network segmentation limits critical systems' exposure.
- **Perform Firedrill** ○ Validate Playbook functionality upon publication and annually.
  - Test scenarios like:
    - Memory-only attacks.

        - Exploitation of trusted processes like PowerShell or WMI.
    - Ensure escalation paths and contact lists are up to date.
- **Review Threat Intelligence**
    - Investigate trends in fileless malware attacks.
    - Analyse new tactics targeting the sector and brands.
    - Monitor CVEs exploited by attackers for fileless methods.
- **Asset Inventory**
    - Maintain a list of:
        - Endpoints, servers and network ranges.
        - Software used in the environment (version details).
        - Owners and pre-authorised actions.
    - Include tools that allow memory execution (e.g., scripting frameworks).

2. DETECT

MD1. Identify Threat Indicators

- **Alerts**
    - SIEM
        - Anomalous PowerShell or WMI activity.
        - Memory injections.
    - EDR
        - Detection of unsigned or obfuscated scripts.
    - DNS logs
        - Connections to command-and-control (C2) domains.
    - Network monitoring tools
        - Unusual traffic patterns.
- **Notifications**
    - Internal users reporting performance issues or crashes.
    - External vendors reporting vulnerabilities or suspicious activity.

MD2. Identify Risk Factors

- **Common Risks**
    - Credential theft.
    - Network traversal and lateral movement.
    - Data exfiltration.
- **Company-Specific Risks**
    - Reputational damage from breaches.
    - Financial impact from service disruption or regulatory penalties.

MD3. Data Collection

- **Processes**
    - Analyse processes that triggered detections (e.g., powershell.exe, wmic.exe).
    - Identify parent-child process relationships.
- **Memory Analysis**
    - Capture memory dumps to identify scripts or commands executed.
- **Network**

  - Identify domains, IPs or ports involved in C2 communications.

MD4. Categorise

- **Types of Fileless Attacks** ○ Memory-only malware. ○ Living-off-the-land binaries (LOLBins). ○ Script-based attacks (e.g., PowerShell, VBScript). ○ Malicious WMI scripts.

MD5. Is it an Advanced Attack?

- If the attack uses obfuscated scripts or advanced memory manipulation:
  - Escalate to the Threat Hunting team. ○ Notify senior analysts.

MD6. Triage

- **Determine Impact and Scope** ○ Affected hosts. ○ Any lateral movement.
  - Potential data exfiltration.

MD7. Is it a False Positive?

- Document and close if false.
- If true: escalate and proceed to Analyse phase.

3. ANALYSE

MA1. Verify

- Double-check logs for unusual behaviours (e.g., script execution, network anomalies).

MA2. Identify IOCs

- Use tools like VirusTotal, Hybrid Analysis and URLScan to validate:
  - Scripts. ○ Domains. ○ IPs.

MA3. Extract IOCs

- Analyse captured memory for: ○ Scripts or commands.
  - Injected processes.
- Analyse network connections for C2 communications.

MA4. Submit to Partners

- Provide samples to security vendors if novel techniques are observed.

MA5. Scan Enterprise

- Update endpoint rules to detect similar behaviours.
- Search endpoints for IOCs and review network traffic for lateral movement.

4. CONTAIN / ERADICATE

MC1. Contain Affected Hosts

- Use EDR to isolate affected systems.
- Block suspicious domains and IPs.
- Blackhole DNS for identified C2 domains.

MC2. Eradicate

- Terminate malicious processes.
- Remove any registry modifications or scripts left by the malware.

MC3. Validate

- Ensure all IOCs are removed.
- Rescan systems and networks for residual traces.

5. RECOVER MR1. Restore Operations

- Reimage affected systems.
- Restore data from secure backups.

6. LESSONS LEARNT

- Conduct a post-incident review to enhance:
  - Detection capabilities.
  - Response strategies.
- Update Playbook based on findings.

ROGUE ACCESS POINT (ROGUE AP) ATTACK PLAYBOOK

1. PREPARATION

- **Create and Maintain a List of** ○ Authorised access points, including:
    - SSIDs.
    - MAC addresses.
    - Locations.
  - Employee devices allowed to connect to Wi-Fi.

- **Email Templates** ○ Notify employees about suspicious Wi-Fi networks.
  - Communicate with IT teams about identifying rogue devices.
- **Tools and Equipment** ○ Wireless Intrusion Prevention Systems (WIPS) configured to detect and block unauthorised access points.
  - Wi-Fi heatmaps to identify areas vulnerable to rogue AP placement.
- **Ensure that:**
  - Access points are secured with strong encryption (e.g., WPA3). ○ MAC filtering is implemented for additional security.
  - Network segmentation is in place to limit access for connected devices.
- **Perform Firedrill** ○ Validate the playbook annually by simulating:
    - The detection of a rogue AP. ▪ Mitigation scenarios.
- **Review Threat Intelligence** ○ Monitor trends in Wi-Fi-based attacks. ○ Stay updated on vulnerabilities in wireless protocols or devices.

2. DETECT

MD1. Identify Threat Indicators

- **Alerts** ○ WIPS/Network Monitoring Tools ▪ Detection of unauthorised SSIDs.
    - MAC address spoofing attempts. ○ SIEM
    - Anomalous device connections.
    - Unusual traffic patterns associated with new devices.
- **Notifications** ○ Employees reporting suspicious Wi-Fi networks. ○ External alerts from vendors or service providers about Wi-Fi-related vulnerabilities.

MD2. Identify Risk Factors

- **Common Risks**
  - Credential theft via rogue AP. ○ Man-in-the-middle (MITM) attacks.
  - Malware injection.
- **Company-Specific Risks** ○ Sensitive data interception from employees. ○ Potential exposure of corporate assets to external attackers.

MD3. Data Collection

- **Wireless Scans** ○ Use tools like Aircrack-ng, Kismet or enterprise WIPS to detect rogue APs.
  - Look for:
    - SSIDs mimicking legitimate networks. ▪ Unfamiliar MAC addresses.
- **Logs**

    - Analyse Wi-Fi logs for devices connecting to suspicious networks.
- **Device Behaviour** o Identify devices exhibiting abnormal traffic patterns or excessive beacon frames.

MD4. Categorise

- **Types of Rogue APs** o Personal hotspots set up by employees.
    - Malicious APs set up by attackers to intercept traffic. o Misconfigured legitimate APs.

MD5. Is it an Advanced Attack?

- Indicators of advanced attacks include:
    - Rogue APs configured to use encryption identical to corporate APs. o Targeted MITM activities or credential theft.

MD6. Triage

- **Determine Impact and Scope** o Number of devices connected to the rogue AP.
    - Potential data intercepted or manipulated.

MD7. Is it a False Positive?

- Document and close if false (e.g., an employee’s personal hotspot).
- If true: escalate and proceed to Analyse phase.

3. ANALYSE

MA1. Verify

- Confirm the rogue AP's existence using multiple tools (e.g., Wi-Fi heatmaps and scanners).

MA2. Identify IOCs

- Identify key indicators such as:
    - Unauthorised SSID names. o MAC addresses spoofing legitimate APs. o Devices connecting to both legitimate and rogue networks.

MA3. Extract IOCs

- Record all:
    - SSIDs, BSSIDs and channels used by the rogue AP. o Associated devices and their activities.

MA4. Submit to Partners

- Share findings with network device vendors if advanced techniques are involved.

MA5. Scan Enterprise

- Verify that no other rogue APs are present in the environment.

4. CONTAIN / ERADICATE

MC1. Contain the Rogue AP

- Use WIPS or manual tools to deauthenticate rogue AP connections.
- Physically locate and disable the rogue AP if possible.

MC2. Eradicate

- Block rogue AP MAC addresses on the network.
- Identify and address vulnerabilities exploited to set up the rogue AP.

MC3. Validate

- Confirm the rogue AP is no longer broadcasting or accessible.
- Rescan the area for any signs of additional rogue devices.

5. RECOVER

MR1. Restore Operations

- Educate users to avoid connecting to unverified networks.
- Strengthen Wi-Fi security policies.

6. LESSONS LEARNT

- Review the incident and identify:
  - Gaps in detection or response.
  - Weaknesses in current Wi-Fi security measures.
- Update the playbook and security protocols based on findings.

SQL INJECTION ATTACK PLAYBOOK

1. PREPARATION

- **Security Controls** ○ Implement input validation and sanitisation for web applications.
  - Use prepared statements or parameterised queries in database interactions.
  - Apply Web Application Firewall (WAF) rules to detect and block injection patterns.
- **Asset Inventory** ○ Maintain an up-to-date list of all databases and web applications, including endpoints handling user inputs.
- **Access Controls** ○ Ensure least privilege access for database users.
  - Regularly review and rotate database credentials.
- **Monitoring Tools** ○ Configure SIEM tools to monitor:
    - Database logs for anomalous queries.
    - Unauthorised changes to data.
  - Set up alerts for suspicious URL patterns or payloads detected in HTTP traffic.
- **Incident Drills** ○ Simulate SQL injection scenarios to test detection and response procedures.

2. DETECT

MD1. Identify Threat Indicators

- **Alerts** ○ WAF: Detection of common SQL injection payloads like ' OR '1'='1 or UNION SELECT.
  - SIEM: Unusual database queries, such as:
    - DROP TABLE commands.
    - Mass exfiltration of sensitive data. ▪ Queries from unauthorised IPs.
- **Logs**
  - Web server logs: Unusual query strings in GET/POST requests.
  - Database logs:
    - Queries executed outside normal application patterns. ▪ Login attempts using non-application accounts.

MD2. Identify Risk Factors

- **Common Risks**
  - Data theft or unauthorised modifications.
  - Database corruption or deletion.
  - Privilege escalation in the database.

- **Company-Specific Risks** ○ Compromise of sensitive customer data (e.g., PII).
    - ○ Breach of compliance standards (e.g., GDPR, HIPAA).

MD3. Data Collection

- **Payload Analysis** ○ Examine malicious inputs submitted via web forms, URLs or APIs.
    - ○ Review WAF logs for blocked or allowed suspicious requests.
- **Database Queries** ○ Correlate suspicious input with the database queries executed during the same timeframe.

MD4. Categorise

- **Injection Types** ○ Error-Based SQL Injection (visible database errors). ○ Union-Based SQL Injection (data exfiltration via UNION SELECT). ○ Blind SQL Injection (true/false payloads with no direct error feedback).

MD5. Is it an Advanced Attack?

- Advanced indicators:
    - ○ Use of out-of-band (OOB) channels to exfiltrate data (e.g., DNS). ○ Automated tools like SQLmap detected in logs.
    - ○ Cross-database queries targeting linked servers.

MD6. Triage

- **Assess Impact** ○ Severity of data accessed or modified.
    - ○ Whether the attacker achieved code execution or database control.
- **Prioritisation** ○ High-priority if sensitive data was accessed or database availability is at risk.

MD7. Is it a False Positive?

- **Validation** ○ Cross-check suspicious activity with developers. ○ Confirm anomalies in database or web server logs.

- **Resolution** ○ Document and close if a false positive.

3. ANALYSE

MA1. Verify

- Confirm SQL injection by:

  - Reproducing the malicious payload in a secure test environment. o Checking application responses and database logs.

MA2. Identify IOCs

- Common indicators include:
  - Exploited input fields (e.g., login forms, search boxes). o Suspicious query patterns in database logs.

MA3. Extract IOCs

- Document malicious payloads, IP addresses and timestamps.

MA4. Submit to Partners

- Share findings with WAF vendors or database administrators.

MA5. Scan Enterprise

- Perform web application vulnerability scans to identify other SQL injection risks.

4. CONTAIN / ERADICATE

MC1. Contain the Threat

- Block offending IPs at the firewall or WAF.
- Disable compromised application endpoints temporarily.

MC2. Eradicate the Root Cause

- Patch the vulnerable web application.
- Implement stricter input validation and sanitisation.
- Apply updates to WAF rules to block similar payloads.

MC3. Validate

- Test the application to confirm that SQL injection is no longer exploitable.

5. RECOVER

MR1. Restore Operations

- Restore corrupted or deleted data from backups.
- Reactivate application endpoints after testing.

6. LESSONS LEARNT • Review the attack vector and determine how it was missed during development or testing.

- Strengthen application security by adopting secure coding practices.
- Update the playbook and train developers and analysts to handle similar incidents.

STEGANOGRAPHY-BASED DATA EXFILTRATION PLAYBOOK

1. PREPARATION

- **Security Controls** ○ Monitor outbound data traffic for anomalies in file formats and sises. ○ Use DLP (Data Loss Prevention) tools to scan file content for hidden payloads.
    - ○ Implement strict access controls on sensitive files and databases.
- **Employee Awareness**
    - ○ Train employees to recognise signs of steganography, such as modified image or audio files.
- **Policies** ○ Restrict unnecessary use of multimedia files for transferring sensitive data. ○ Enforce the use of encryption and file integrity checks for sensitive data transfers.
- **Threat Intelligence** ○ Gather intelligence on known steganography tools like Steghide, OpenStego and Outguess.

2. DETECT

MD1. Identify Threat Indicators • Anomalous Network Activity ○ Increased outbound traffic of seemingly innocuous files (e.g., JPG, PNG, MP3). ○ Files with unusual patterns, such as higher-than-expected sises or irregular metadata.

- **System Logs**
    - ○ Tools like exiftool or strings being executed on critical systems.
    - ○ Usage of uncommon commands to interact with multimedia files.
- **User Behaviour** ○ Sudden increase in file downloads or uploads by an employee. ○ Access to steganography-related tools or websites.

MD2. Identify Risk Factors

- **Common Risks**
    - ○ Exfiltration of intellectual property or sensitive customer data.
    - ○ Stealthy distribution of malicious payloads embedded in files.
- **Company-Specific Risks** ○ Leakage of proprietary research, trade secrets or classified designs.

MD3. Data Collection • File Analysis ○ Extract metadata and check for anomalies (e.g., timestamps, editing history).

- ○ Use steganalysis tools to examine files for hidden data.
- **Network Traffic** ○ Capture and analyse outbound traffic for suspicious file transfers.
    - ○ Look for encrypted payloads disguised in multimedia file uploads.

MD4. Categorise

- **Steganography Type** ○ Image-based: Data hidden in image pixel values (e.g., LSB embedding).
  - Audio-based: Hidden data in inaudible frequencies or audio noise. ○ Video-based: Modifications to frame data or metadata.

MD5. Is it an Advanced Attack?

- Advanced indicators include:
  - Use of custom or unknown steganography tools. ○ Encrypted or obfuscated payloads requiring specialised decoding techniques.

MD6. Triage

- **Assess Impact**
  - Severity of the data exfiltrated and its potential misuse.
- **Prioritisation** ○ High-priority if sensitive data or critical intellectual property is leaked.

MD7. Is it a False Positive?

- **Validation** ○ Compare the suspicious files to legitimate versions. ○ Verify user actions and network logs.

3. ANALYSE

MA1. Verify

- Use steganalysis tools like StegSpy, StegExpose or custom scripts to confirm hidden data.
- Decode payloads using the identified tool or method.

MA2. Identify IOCs

- Indicators include:
  - Modified multimedia files. ○ Specific tools or scripts executed.
  - Network destinations for exfiltration.

MA3. Extract IOCs

- Document the tools, techniques and destinations used in the attack.

MA4. Submit to Partners

- Share findings with threat intelligence teams or law enforcement if necessary.

MA5. Scan Enterprise

- Search for other suspicious files or tools within the network.

4. CONTAIN / ERADICATE

MC1. Contain the Threat

- Isolate the system or user account involved in the attack.
- Block outbound communications to the identified destinations.

MC2. Eradicate the Root Cause

- Remove the steganography tools and suspicious files from systems.
- Patch vulnerabilities exploited to introduce steganography tools. **MC3.**

Validate

- Conduct a thorough scan to confirm no hidden payloads remain.

5. RECOVER

MR1. Restore Operations

- Re-enable affected systems after remediation.
- Restore any corrupted or altered data from backups.

6. LESSONS LEARNT

- Review the incident to identify gaps in detection and response.
- Update security policies to prevent misuse of multimedia files.
- Enhance employee training on the risks of steganography.

CACHE POISONING ATTACK PLAYBOOK

1. PREPARATION

- **Security Controls** o Enforce cache validation policies, such as requiring strong ETags or LastModified headers. o Use HTTPS with proper certificate validation to prevent man-in-the-middle attacks.
    - o Enable Content Security Policies (CSP) to limit the impact of poisoned content.
- **System Hardening**
    - o Configure caching layers (e.g., CDNs, proxies) to verify upstream responses.
    - o Disable caching for user-specific or sensitive data.
- **Threat Intelligence** o Stay updated on vulnerabilities in caching systems and applications.

2. DETECT

MD1. Identify Threat Indicators

- **Network Activity** o Suspicious or malformed cache-control headers in HTTP responses. o High frequency of cache misses followed by unexpected hits serving incorrect data.
- **User Behaviour** o Increased reports of users seeing outdated, malicious or irrelevant content.
- **Application Logs** o Unusual request patterns targeting cacheable resources. o Exploitation attempts on specific endpoints using query parameters or fragments.

MD2. Identify Risk Factors

- **Common Risks**
    - o Distribution of malicious scripts, phishing pages or redirects to users.
    - o Tarnished reputation due to users receiving compromised content.
- **Company-Specific Risks** o Poisoning of public-facing resources like product pages or login forms.

MD3. Data Collection

- **Log Analysis** o Examine web server logs for suspicious GET/POST requests.
    - o Analyse responses from cache servers for manipulated headers or payloads.
- **Traffic Capture** o Monitor traffic to detect altered content in HTTP responses.
    - o Verify cache key collisions caused by manipulated requests.

MD4. Categorise

- **Type of Cache Poisoning** ○ HTTP Header Injection: Manipulating headers like Content-Type or CacheControl.
    - Query String Poisoning: Exploiting improper cache key validation. ○ CDN Cache Misconfiguration: Leveraging incorrect caching rules in a CDN.

MD5. Is it an Advanced Attack?

- Indicators of advanced attacks:
    - Use of zero-day exploits targeting caching layers. ○ Highly customised payloads affecting specific user groups or geographies.

MD6. Triage

- **Assess Impact**
    - Severity of poisoned content and its potential reach.
- **Prioritisation** ○ High-priority if sensitive or widely accessed content is compromised.

MD7. Is it a False Positive?

- **Validation** ○ Compare cached responses with the original content from the origin server.

3. ANALYSE MA1. Verify

- Use tools like curl or web debugging proxies to fetch and validate cached content.
- Identify discrepancies between cached and source data.

MA2. Identify IOCs

- Indicators include:
    - Unexpected headers or payloads in cached responses. ○ Suspicious query strings causing unexpected cache hits.

MA3. Extract IOCs

- Document compromised URLs, query parameters or headers.

MA4. Submit to Partners

- Share IOCs with CDN or caching service providers to update their security rules.

MA5. Scan Enterprise

- Search for similar vulnerabilities across other endpoints or caching layers.

4. CONTAIN / ERADICATE

MC1. Contain the Threat

- Purge the cache to remove poisoned content.
- Temporarily disable caching on affected resources.

MC2. Eradicate the Root Cause

- Patch vulnerabilities in the web application or caching configuration.
- Fix improper cache key validation mechanisms.

MC3. Validate

- Ensure updated cache configurations prevent recurrence.

5. RECOVER

MR1. Restore Operations

- Resume caching with updated policies and configurations.
- Reassure users by publicly addressing the incident and its resolution.

6. LESSONS LEARNT

- Conduct a post-incident review to identify the attack vector and missed controls.
- Update cache configurations and implement stricter validation policies.
- Train developers and IT teams on secure caching practices.

HOMOGRAPH ATTACK PLAYBOOK

1. PREPARATION

- **Security Controls** ○ Enable Unicode-aware phishing protection in web browsers. ○ Implement strict domain registration monitoring for typosquatting or homograph domains.
    - ○ Use a secure DNS resolver that blocks known malicious domains.
- **User Awareness** ○ Educate users about homograph attacks and the importance of verifying URLs before interacting.
    - ○ Regularly remind users to avoid clicking unknown or suspicious links.

- **Technology Setup** ○ Configure email filters to flag or block messages with deceptive URLs. ○ Deploy endpoint protection tools to detect and block access to suspicious domains.

2. DETECT

MD1. Identify Threat Indicators

- **Network Indicators** ○ Requests to domains containing Unicode characters that mimic legitimate ones. ○ DNS lookups for newly registered or suspicious domains with slight visual differences.
- **User Reports** ○ Complaints about being redirected to unexpected or malicious sites after clicking links.
- **Email Indicators** ○ Phishing emails containing links to homograph domains. ○ Presence of Punycode URLs (e.g., http://xn--example-dk3a.com).

MD2. Identify Risk Factors

- **Common Risks**
    - Credential theft through phishing sites mimicking legitimate login portals.
    - Malicious downloads served from lookalike domains.
- **Company-Specific Risks** ○ Brand impersonation resulting in reputational damage. ○ Financial fraud targeting customers or employees.

MD3. Data Collection

- **Log Analysis** ○ Check DNS, proxy and web server logs for unusual domain names or requests.
    - Search for traffic directed toward domains containing visually deceptive characters.
- **Email Analysis** ○ Investigate flagged emails for links leading to homograph domains.
- **Threat Intelligence** ○ Leverage databases of known malicious homograph domains.

MD4. Categorise

- **Attack Vectors** ○ Phishing: Mimicking login pages or financial websites.
    - Malware Distribution: Serving malicious payloads via lookalike domains.
    - Brand Abuse: Using homograph domains to impersonate company assets.

MD5. Is it an Advanced Attack?

- Advanced indicators:

    - Use of dynamic DNS or bulletproof hosting to avoid detection. ○ Targeted campaigns against high-value individuals (e.g., spear phishing).

MD6. Triage

- **Assess Impact** ○ Identify users or systems interacting with the malicious domain.
    - Evaluate the potential data exposure or financial loss.
- **Prioritisation** ○ High-priority if sensitive data is at risk or if a significant number of users are targeted.

MD7. Is it a False Positive?

- Verify whether the domain is legitimately owned or a registered homograph.

3. ANALYSE

MA1. Verify

- Use WHOIS and threat intelligence tools to identify the domain’s registration details.
- Access the domain via a sandbox to validate its content and purpose.

MA2. Identify IOCs

- Extract domain names, IP addresses and Punycode representations as indicators.

MA3. Extract IOCs

- Collect and document malicious domain details, phishing page screenshots and associated IPs.

MA4. Submit to Partners

- Share IOCs with DNS providers, threat intelligence platforms and browser vendors.

MA5. Scan Enterprise

- Identify other instances of interaction with the homograph domain across the network.

4. CONTAIN / ERADICATE

MC1. Contain the Threat

- Block access to the homograph domain via DNS and proxy.

- Remove any cached links or emails containing the malicious URLs.

MC2. Eradicate the Root Cause

- Shut down the malicious domain by contacting the registrar or hosting provider.
- Strengthen email filters to detect similar threats in the future.

MC3. Validate

- Confirm that the malicious domain is inaccessible across the organisation.

5. RECOVER

MR1. Restore Operations

- Notify affected users about the incident and advise them to change any exposed credentials.
- Conduct a security review of processes that failed to block the threat.

6. LESSONS LEARNT

- Conduct a retrospective analysis to improve monitoring and detection of homograph domains.
- Update training programs to raise awareness about the attack method.
- Regularly monitor for domain impersonation attempts involving the company’s brand.

DENIAL-OF-SERVICE (DoS) ATTACK PLAYBOOK

1. PREPARATION

- **Security Controls** ○ Deploy a Web Application Firewall (WAF) to filter and block malicious traffic. ○ Set rate-limiting policies on servers and APIs to handle traffic spikes.
  - Enable DDoS protection services (e.g., Cloudflare, AWS Shield).
- **Incident Response Setup** ○ Establish a DoS response team with clear roles and responsibilities.
  - Maintain updated network diagrams and asset inventories.
- **User Awareness** ○ Train staff to recognise symptoms of DoS attacks, such as sudden system unavailability.

2. DETECT

MD1. Identify Threat Indicators

- **Network Indicators** ○ Sudden spikes in inbound traffic, particularly from a single source or range.
  - Multiple repeated requests to a single endpoint.
  - Saturation of network bandwidth or server resources.
- **System Indicators** ○ High CPU or memory utilisation on affected systems. ○ Increased response times or timeouts for legitimate users.

MD2. Identify Risk Factors

- **Common Risks**
  - Temporary unavailability of critical services or websites.
  - Financial loss due to service downtime.
- **Company-Specific Risks** ○ Disruption to customer-facing applications, damaging brand reputation. ○ Potential exploitation of service downtime for follow-up attacks.

MD3. Data Collection

- **Log Analysis** ○ Review firewall, router and server logs for abnormal traffic patterns.
  - Identify traffic sources, protocols and frequency of requests.
- **Traffic Analysis** ○ Use network monitoring tools (e.g., Wireshark, SolarWinds) to analyse packet flow.

MD4. Categorise

- **Attack Vectors** ○ TCP SYN Flood: Exploiting handshake requests to exhaust server resources.
    - UDP Flood: Overloading servers with high volumes of UDP packets. ○ HTTP GET/POST Flood: Bombarding web applications with HTTP requests.

MD5. Is it an Advanced Attack?

- **Indicators of Advanced Attacks** ○ Large-scale Distributed Denial-of-Service (DDoS) involving botnets. ○ Use of spoofed IP addresses to evade detection. ○ Layer 7 (application layer) attacks designed to bypass traditional defences.

MD6. Triage

- **Assess Impact**
    - Identify the systems and services affected by the attack.
    - Evaluate the downtime duration and business impact.
- **Prioritisation** ○ High-priority if critical services are down or if the attack affects a large user base.

MD7. Is it a False Positive?

- Compare traffic patterns to historical data to rule out legitimate traffic spikes.

3. ANALYSE MA1. Verify

- Confirm the attack by cross-referencing logs, traffic analysis and user reports.

MA2. Identify IOCs

- Extract attacker IP addresses, payload patterns and unusual traffic volumes.

MA3. Extract IOCs

- Document the attack's characteristics, including protocol type and source details.

MA4. Submit to Partners

- Share IOCs with your ISP and security service providers for mitigation assistance.

MA5. Scan Enterprise

- Investigate whether internal systems contributed to the attack (e.g., compromised devices).

4. CONTAIN / ERADICATE

MC1. Contain the Threat

- Implement rate-limiting rules on affected endpoints.
- Block malicious IP addresses or ranges at the firewall level.
- Redirect traffic through a DDoS mitigation service.

MC2. Eradicate the Root Cause

- Patch and harden exposed services to prevent abuse.
- Disable unused network services that could be exploited.

MC3. Validate

- Verify that legitimate traffic can access the service and malicious traffic is blocked.

5. RECOVER

MR1. Restore Operations

- Gradually lift rate limits or restrictions to normalise service delivery.
- Monitor traffic to ensure there is no resurgence of malicious activity.

MR2. Post-Incident Recovery

- Communicate with affected users, explaining the downtime and corrective measures.
- Perform a comprehensive system health check.

6. LESSONS LEARNT

- Conduct a post-mortem analysis to identify gaps in detection and mitigation.
- Update playbooks and implement additional controls based on the attack vector.
- Regularly test the response to simulated DoS attacks to improve readiness.

MALWARE ATTACK PLAYBOOK

1. PREPARATION • **Security Controls** ○ Deploy Endpoint Detection and Response (EDR) solutions for continuous monitoring and response.

    - Ensure antivirus and anti-malware tools are updated across all endpoints.
    - Implement application whitelisting to block unauthorised software execution.
    - Use network segmentation to minimise malware spread.

    - Enforce least privilege for users and applications to limit damage.
- **Asset Inventory** ○ Maintain a detailed inventory of all critical systems and software.
    - Identify systems prone to malware attacks (e.g., email servers, endpoints).
- **Access Controls** ○ Enforce multi-factor authentication (MFA) for remote and privileged access.
    - Regularly audit access permissions and revoke unnecessary rights.
- **Monitoring Tools** ○ Configure SIEM tools to monitor:
        - Anomalous file changes (e.g., sudden encryption of files).
        - Execution of unusual processes or scripts. ▪ Traffic to known malicious IPs/domains.
- **Incident Drills** ○ Simulate malware infection scenarios (e.g., ransomware, trojans) to test detection and containment plans. ○ Train employees to recognise phishing emails and malicious links.

2. DETECT

- **MD1. Identify Threat Indicators** ○ **Alerts**
        - EDR: Detection of suspicious file executions or privilege escalations. ▪ SIEM: Unusual network connections (e.g., C2 traffic).
    - **Logs**
        - Endpoint logs: New or unusual file executions (e.g., .exe, .dll or PowerShell scripts).
        - Network logs: Large data transfers to unknown IPs or domains.
- **MD2. Identify Risk Factors** ○ **Common Risks**
        - Data exfiltration or loss.
        - Lateral movement across the network.
        - Disruption of operations via ransomware.
    - **Company-Specific Risks**
        - Breach of intellectual property or proprietary data.
        - Impact on compliance with standards like GDPR, HIPAA.
- **MD3. Data Collection** ○ Analyse malicious files for hashes and behavior. ○ Review logs for the initial infection vector (e.g., phishing email, compromised website).
- **MD4. Categorise** ○ Malware Types:
        - Ransomware (encrypting files for ransom).
        - Spyware (stealing sensitive data).
        - Worms (spreading without user action).
    - Delivery Methods:
        - Email attachments, malicious links or removable media.
- **MD5. Is it an Advanced Attack?**

  - Advanced indicators:
    - Use of zero-day exploits.
    - Sophisticated obfuscation techniques in malware.
    - Presence of advanced persistent threat (APT) groups.
- **MD6. Triage** ○ Assess the malware's impact on critical systems and data.
  - Prioritise based on potential data theft or business disruption.
- **MD7. Is it a False Positive?**
  - Validate suspicious activity against known legitimate processes.
  - Cross-reference with threat intelligence sources for confirmation.

3. ANALYSE

- **MA1. Verify** ○ Reproduce malware activity in a sandbox environment.
  - Analyse application logs and system behaviors.
- **MA2. Identify IOCs** ○ File hashes (e.g., MD5, SHA256). ○ C2 server IPs or domains.
  - Registry changes or system configurations modified.
- **MA3. Extract IOCs** ○ Document infected files, URLs and attack timestamps.
- **MA4. Submit to Partners** ○ Share findings with antivirus vendors and threat intelligence partners.
- **MA5. Scan Enterprise** ○ Perform a full malware scan across endpoints, servers and networks.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat**
  - Isolate infected systems by disconnecting them from the network.
  - Block malicious domains and IPs via firewalls or DNS filtering.
- **MC2. Eradicate the Root Cause** ○ Remove malware using updated antivirus or EDR tools.
  - Patch vulnerabilities exploited by the malware.
- **MC3. Validate** ○ Perform post-removal scans to ensure no malware remnants remain.

5. RECOVER

- **MR1. Restore Operations** ○ Recover files and systems from secure, verified backups.
  - Reactivate systems only after thorough testing.
- **MR2. Communicate**

    - ○ Notify stakeholders of recovery status and any required actions.

6. LESSONS LEARNT

- Review infection vector and assess why security controls failed.
- Strengthen employee training programs to improve phishing detection.
- Update the playbook with new IOCs and remediation strategies.
- Evaluate the effectiveness of tools used and identify gaps.

PHISHING ATTACK PLAYBOOK

1. PREPARATION

- **Security Controls** ○ Deploy email filtering solutions to detect and block phishing emails. ○ Enable domain-based email authentication (e.g., SPF, DKIM, DMARC). ○ Use anti-phishing browser extensions and tools for employees.
    - ○ Regularly update email clients and security software.
- **Asset Inventory** ○ Maintain an inventory of business-critical email accounts and systems.
    - ○ Identify high-value targets (e.g., executives, HR and finance personnel).
- **Access Controls** ○ Enforce MFA for all email accounts, especially for privileged users.
    - ○ Regularly audit and update access permissions for sensitive data.
- **Monitoring Tools** ○ Configure SIEM tools to monitor:
        - ▪ Unusual email login locations.
        - ▪ Sudden email forwarding rule changes.
        - ▪ Suspicious email activity, such as mass outbound emails.
- **Incident Drills** ○ Simulate phishing attacks (e.g., spear-phishing exercises) to assess employee awareness. ○ Train employees to recognise phishing indicators, such as mismatched domains and suspicious links.

2. DETECT

- **MD1. Identify Threat Indicators** ○ **Alerts**
        - ▪ Email gateway: Detection of malicious attachments or links. ▪ SIEM: Login attempts from unusual locations or devices.
    - ○ **Logs**
        - ▪ Email server logs:
        - ▪ Emails containing suspicious links or attachments.
        - ▪ Anomalies in sent or received email volumes.
        - ▪ User reports: Suspicious emails forwarded to the security team.

- **MD2. Identify Risk Factors** ○ **Common Risks**
    - Credential theft via phishing pages.
    - Data exfiltration or unauthorised access to accounts. ○

  Company-Specific Risks
    - Financial fraud through compromised accounts.
    - Breach of sensitive customer or employee data.
- **MD3. Data Collection** ○ Analyse email headers for sender IPs and domains.
    - Inspect URLs for signs of phishing (e.g., typosquatting, shortened links).
    - Retrieve user activity logs for suspicious actions after clicking links.
- **MD4. Categorise** ○ Phishing Types:
    - **Spear Phishing:** Targeted at specific individuals or departments.
    - **Whaling:** Targeting executives or high-profile employees. ▪ **Clone Phishing:** Mimicking legitimate emails.
- **MD5. Is it an Advanced Attack?**
    - Advanced indicators:
        - Use of compromised legitimate email accounts.
        - Sophisticated phishing kits with evasion techniques.
        - Multi-stage attacks involving malware or additional phishing.
- **MD6. Triage**
    - Prioritise incidents involving:
        - High-value accounts (e.g., executives, finance). ▪ Access to sensitive data or financial systems.
- **MD7. Is it a False Positive?**
    - Validate suspicious emails by cross-referencing with legitimate communications. ○ Confirm with users if unusual activities (e.g., new email rules) were intentional.

3. ANALYSE • MA1. Verify ○ Reproduce email actions in a secure environment (e.g., opening links in isolated browsers).

- Check for phishing indicators in the email's content, attachments and URLs.
- **MA2. Identify IOCs** ○ Common indicators include:
    - Phishing domains or URLs.
    - Email sender addresses and IPs.
    - Malicious attachments (e.g., .exe, .xlsm).
- **MA3. Extract IOCs** ○ Document all malicious indicators, including timestamps and user interactions.
- **MA4. Submit to Partners** ○ Share phishing indicators with email security vendors and threat intelligence providers.

- **MA5. Scan Enterprise** ○ Check other users for emails from the same sender or with similar indicators.
    - Monitor for additional login attempts or suspicious activities linked to phishing.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat** ○ Block phishing domains and sender IPs at the email gateway. ○ Quarantine suspicious emails from all user inboxes.
    - Reset credentials for affected accounts immediately.
- **MC2. Eradicate the Root Cause** ○ Remove malicious email rules or auto-forwarding set by attackers.
    - Strengthen email authentication (e.g., SPF, DKIM, DMARC).
- **MC3. Validate** ○ Conduct phishing tests to ensure users recognise similar future threats. ○ Review logs to confirm no residual malicious activity.

5. RECOVER

- **MR1. Restore Operations** ○ Re-enable affected accounts and email services after thorough checks.
    - Notify impacted users about the steps taken and additional precautions.
- **MR2. Communicate**
    - Inform stakeholders of the incident resolution and preventive measures implemented.

6. LESSONS LEARNT

- Review how the phishing email bypassed existing security controls.
- Update employee training programs with lessons from the incident.
- Strengthen detection and response procedures for email-based threats.
- Update the playbook with new phishing tactics and IOCs.

WATERING HOLE ATTACK PLAYBOOK

1. PREPARATION • **Security Controls** ○ Deploy robust web filtering solutions to prevent access to malicious websites.

- Conduct regular security assessments of websites frequently visited by employees.
- Use endpoint protection with real-time detection for malicious web content.
- Ensure browsers, plugins and operating systems are up to date with the latest security patches.

- **Asset Inventory** ○ Identify and document commonly visited websites critical for business operations.
  - Maintain an up-to-date inventory of employee devices and software.
- **Access Controls** ○ Limit administrative privileges to reduce the impact of compromise.
  - Enforce network segmentation to isolate critical systems.
- **Monitoring Tools** ○ Configure SIEM tools to monitor:
    - Outbound traffic to known or suspected malicious domains.
    - DNS requests for unusual or newly registered domains.
  - Deploy Intrusion Detection Systems (IDS) to detect exploit kits or malware payloads.
- **Incident Drills** ○ Simulate watering hole scenarios to test detection and response capabilities.
  - Train employees on safe browsing habits and recognising potential website compromises.

2. DETECT

- **MD1. Identify Threat Indicators** ○ **Alerts**
    - IDS/IPS: Detection of exploit kits in HTTP traffic.
    - SIEM: DNS lookups for malicious or newly registered domains.
    - Endpoint detection: Malware payloads downloaded from compromised websites.
  - **Logs**
    - Web proxy logs: Unusual traffic patterns to compromised sites. ▪ Browser activity logs: Sudden or unexpected redirects.
- **MD2. Identify Risk Factors** ○ **Common Risks**
    - Exploitation of unpatched vulnerabilities via malicious code.
    - Malware infections on employee devices.
    - Exfiltration of credentials or sensitive data.
  - **Company-Specific Risks**
    - Targeting websites frequently used by employees (e.g., industry forums, vendor portals).
    - Compromise of high-value devices or accounts.
- **MD3. Data Collection** ○ Analyse web traffic logs for connections to known watering hole sites. ○ Retrieve payloads delivered during the attack for analysis in a secure sandbox.
- **MD4. Categorise** ○ Watering Hole Variants:
    - **Browser Exploits:** Injected scripts that exploit browser vulnerabilities.
    - **Drive-By Downloads:** Automatic malware downloads without user interaction.
    - **Credential Theft:** Redirection to fake login pages.

- **MD5. Is it an Advanced Attack?**
  - Advanced indicators:
    - Use of zero-day browser or plugin exploits.
    - Targeting specific industries or companies.
    - Advanced malware with lateral movement capabilities.
- **MD6. Triage**
  - Prioritise incidents involving:
    - Access to internal systems or sensitive data. ▪ High-value or privileged user accounts.
- **MD7. Is it a False Positive?**
  - Validate flagged websites with threat intelligence feeds.
  - Confirm whether unusual activity was legitimate or benign.

3. ANALYSE

- **MA1. Verify** ○ Reproduce suspicious website interactions in a controlled test environment.
  - Examine scripts or embedded content for malicious code.
- **MA2. Identify IOCs** ○ Common indicators include:
    - Malicious JavaScript or HTML injections.
    - Malware payloads downloaded from compromised sites.
    - Suspicious IP addresses or domains hosting malicious content.
- **MA3. Extract IOCs** ○ Document malicious URLs, IP addresses, payloads and timestamps.
- **MA4. Submit to Partners**
  - Share findings with threat intelligence providers and affected website operators.
- **MA5. Scan Enterprise** ○ Check endpoints for malware infections linked to the watering hole site. ○ Conduct a vulnerability scan to identify unpatched systems.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat** ○ Block malicious domains and IP addresses in web filtering and firewalls.
  - Isolate infected devices from the network.
- **MC2. Eradicate the Root Cause** ○ Remove malware or malicious payloads from affected devices.
  - Apply patches for exploited vulnerabilities. ○ Work with website administrators to secure compromised watering hole sites.

- **MC3. Validate** ○ Verify that all IOCs have been mitigated and that systems are no longer vulnerable. ○ Conduct post-incident scans to confirm the absence of residual threats.

5. RECOVER

- **MR1. Restore Operations** ○ Reintegrate isolated devices after confirming they are clean.
    - Resume normal browsing activities with enhanced monitoring.
- **MR2. Communicate**
    - Notify affected employees and stakeholders about the incident and preventive measures.

6. LESSONS LEARNT

- Analyse how the watering hole site was compromised and how it targeted the company.
- Strengthen website monitoring practices and partnerships with frequently visited domains.
- Update security tools with new IOCs and rules to detect similar attacks.
- Train employees on updated safe browsing practices and phishing awareness.

ISLAND HOPPING ATTACK PLAYBOOK

1. PREPARATION

- **Security Controls** ○ Implement strict access controls for all third-party vendors and partners.
    - Conduct regular security audits of third-party systems connected to your network. ○ Apply network segmentation to minimise lateral movement from compromised third-party systems.
    - Use multi-factor authentication (MFA) for all external connections.
    - Monitor for supply chain and third-party risks with threat intelligence feeds.
- **Asset Inventory** ○ Maintain a detailed inventory of all third-party connections, systems and access levels.
    - Document business-critical assets and their dependencies on third-party systems.
- **Access Controls**
    - Enforce least privilege for all third-party accounts and regularly review access permissions.
    - Disable accounts immediately after contract termination or inactivity.
- **Monitoring Tools** ○ Configure SIEM tools to monitor:
        - Unusual activity in connections from third-party IPs.

    - Data exfiltration patterns or large data transfers.
    - Authentication attempts from unexpected locations or devices.
  - Deploy endpoint detection and response (EDR) to identify suspicious activity on devices accessing the network.
- **Incident Drills** ○ Simulate scenarios where a third-party vendor or partner is compromised to test detection and response.
  - Educate employees on recognising island hopping indicators, such as unusual partner system behavior.

2. DETECT

- **MD1. Identify Threat Indicators** ○ **Alerts**
    - SIEM: Anomalous access patterns from vendor systems.
    - IDS/IPS: Detection of unusual file transfers or privilege escalation attempts.
    - EDR: Signs of lateral movement originating from a trusted third-party connection.
  - **Logs**
    - VPN logs: Unexpected logins from third-party users.
    - Cloud platform logs: Sudden changes to access policies or unusual API calls.
- **MD2. Identify Risk Factors** ○ **Common Risks**
    - Lateral movement into sensitive systems.
    - Exfiltration of critical or sensitive data.
    - Deployment of ransomware or destructive malware.
  - **Company-Specific Risks**
    - Compromise of customer data through vendor relationships.
    - Disruption of operations due to compromised supply chain systems.
- **MD3. Data Collection** ○ Analyse network traffic for abnormal patterns between internal systems and third-party endpoints.
  - Investigate authentication logs for suspicious third-party account activity.
- **MD4. Categorise** ○ **Island Hopping Variants:**
    - **Supply Chain Exploits:** Compromising a vendor to infiltrate the organisation.
    - **Partner Pivoting:** Gaining access through compromised third-party accounts.
    - **Cloud Misconfigurations:** Exploiting third-party cloud integrations.
- **MD5. Is it an Advanced Attack?**
  - Advanced indicators:
    - Use of legitimate credentials stolen from third parties.
    - Sophisticated malware or tools for lateral movement.

        - Coordinated attacks targeting multiple organisations via the same vendor.
- **MD6. Triage**
    - Prioritise incidents involving:
        - High-value or sensitive data.
        - Connections to critical systems or infrastructure.
- **MD7. Is it a False Positive?**
    - Verify activity with the affected third party. ○ Validate alerts with cross-referenced logs from other monitoring tools.

3. ANALYSE • MA1. Verify ○ Reproduce suspicious activity in a sandbox environment to confirm malicious behavior.

- ○ Review third-party communications or logs for signs of compromise.
- **MA2. Identify IOCs** ○ Common indicators include:
    - Unusual login times or IP addresses associated with third-party accounts.
    - Suspicious API calls or system commands.
- **MA3. Extract IOCs** ○ Document malicious IPs, URLs, file hashes and compromised accounts.
- **MA4. Submit to Partners** ○ Share IOCs with affected third parties and relevant industry groups.
- **MA5. Scan Enterprise** ○ Conduct a comprehensive scan for lateral movement or malware within the network.
    - Audit permissions for all third-party accounts and connections.

4. CONTAIN / ERADICATE

- **MC1. Contain the Threat** ○ Disable compromised third-party accounts or connections.
    - Block malicious IPs and domains in firewalls and web filters.
- **MC2. Eradicate the Root Cause** ○ Work with the affected third party to remediate their systems.
    - Patch any vulnerabilities exploited in your environment.
    - Review and tighten network segmentation and access policies.
- **MC3. Validate** ○ Test connections and activity logs to ensure no further malicious activity.
    - Conduct red team exercises to confirm the effectiveness of mitigations.

5. RECOVER

- **MR1. Restore Operations**
    - Re-enable third-party access only after verifying the security of their systems.

    - Restore impacted systems or data from backups.
- **MR2. Communicate**
    - Notify stakeholders, including customers, partners and regulatory bodies if necessary.
    - Provide a detailed post-incident report.

6. LESSONS LEARNT

- Conduct a thorough post-incident review to understand how the third party was compromised.
- Update contracts and policies to enforce stricter cybersecurity requirements for vendors and partners.
- Enhance monitoring capabilities for third-party activity.
- Train employees and third-party users on cybersecurity best practices.