BUILDING A SOC FROM SCRATCH: STRATEGIES AND TEAM ESTABLISHMENT

BY IZZMIER IZZUDDIN

STEP-BY-STEP GUIDE TO BUILDING A SOC STRATEGIES AND TEAM ESTABLISHMENT

1. INITIAL ASSESSMENT AND PLANNING

1.1 Understand Organisational Needs

- **Objective**: Ensure the company's IT and technological ecosystem is safeguarded against internal and external threats.
- **Engage Stakeholders**: Facilitate discussions with key personnel, including executives, IT staff and security teams, to gain insights into:
    - Business Priorities:
        - Identify critical assets like customer data, intellectual property or operational systems that require protection.
        - Align SOC goals with business continuity and revenue generation objectives.
    - Compliance Requirements:
        - Map out regulations applicable to the organisation, such as:
            - GDPR (General Data Protection Regulation).
            - ISO 27001 (Information Security Management).
            - PCI-DSS (Payment Card Industry Data Security Standard).
            - Understand audit and reporting requirements for compliance.
- **Example Scenario**: You are tasked with setting up a SOC for a medium-sized e-commerce business, "Izzmier E-Commerce." During stakeholder meetings:
    - Business Priority:
        - Executives express concern about customer payment data being stolen, impacting revenue and reputation.
        - The development team highlights the importance of uptime for their web application to avoid losing customers.
    - Compliance Requirement:

        - The business must comply with PCI-DSS since it processes credit card payments.

        - The compliance officer mentions that recent audits flagged a lack of real-time logging and monitoring as a critical issue.

- **Action Steps**:

    - Prioritise protection of payment gateways, customer databases and the e-commerce platform.

    - Plan to integrate real-time monitoring to meet compliance and business objectives.

1.2 Assess Existing Security Posture

- **Inventory the Current Security Stack**:

    - Catalogue tools and solutions already in use, such as:

        - Antivirus: McAfee, Symantec.

        - Firewalls: Palo Alto, Fortinet.

        - Switches: Cisco, Juniper.

        - Endpoint Detection and Response (EDR): CrowdStrike, SentinelOne.

        - Microsoft Defender for Endpoint and Cloud.

        - SD-WAN: Secure remote access and site-to-site connectivity solutions.

- **Conduct a Gap Analysis**:

    - Current Threat Detection Capability:

        - Identify what threats the current tools can and cannot detect.

        - Pinpoint any tools with overlapping or redundant functionality.

    - Alert Management:

        - Evaluate if alerts are consolidated in a SIEM or scattered across individual devices.

        - Review the quality of alerts—are they actionable or prone to false positives?
    - **Proactive vs Reactive Posture**:
        - Determine whether incidents are being detected proactively (through monitoring) or reactively (post-breach).
        - Example: Look at recent incidents to assess the time taken to detect and respond.
    - **Skills Assessment**:
        - Review the security team's expertise. Are they equipped to handle the tools and processes in place?
- **Example Scenario**: You audit Izzmier E-Commerce's current security tools:
    - Inventory Findings:
        - Antivirus: McAfee Endpoint Security is installed but not integrated with a central alerting system.
        - Firewall: Fortinet is in place, but logs are stored locally without a SIEM.
        - Endpoint Security: Using CrowdStrike Falcon for detection but limited to laptops; mobile devices are unprotected.
        - Microsoft Defender is enabled on all systems but generates numerous low-priority alerts.
    - Gap Analysis:
        - Missing tools for cloud monitoring, despite hosting the e-commerce website on AWS.
        - Alerts are siloed across tools—firewall logs are not analysed in real-time, leading to delays in detecting lateral movement.
        - Most incidents detected are reactive. For example, a ransomware attack was discovered only after a critical server was encrypted.
- **Action Steps**:
    - Consolidate all logs into a SIEM like Splunk or Microsoft Sentinel.

    - Expand endpoint protection to include mobile devices.
    - Implement a cloud-native monitoring tool like AWS GuardDuty for visibility into cloud activity.

1.3 Define the Scope of the SOC

- **Assets to Monitor**:
    - Specify the range of systems and data the SOC will oversee, including:
        - Servers: Both on-premises and cloud-hosted systems.
        - Endpoints: Laptops, desktops, mobile devices and IoT.
        - Network Devices: Routers, switches, firewalls and load balancers.
        - Databases: Both SQL and NoSQL, on-premises and cloud-based.
        - Applications: Mission-critical and business-critical software.
- **Threats to Detect**:
    - Establish priorities for detecting specific threats, such as:
        - Malware, ransomware, phishing attempts.
        - Insider threats, including unauthorised access or privilege misuse.
        - Advanced Persistent Threats (APTs).
        - Data exfiltration and other forms of unauthorised data access.
- **Expected Outcomes**:
    - Define measurable outcomes for SOC success:
        - Reduce Mean Time to Detect (MTTD): The time taken to identify an incident.
        - Reduce Mean Time to Respond (MTTR): The time taken to mitigate and resolve an incident.
    - Develop KPIs (Key Performance Indicators) to track SOC effectiveness.
- **Example Scenario**: For Izzmier E-Commerce, you define the following scope:
    - Assets to Monitor:

        - Servers: Protect the on-prem ERP system and AWS-hosted web servers.

        - Endpoints: Include all employee laptops, desktops and mobile devices.

        - Applications: Monitor the e-commerce platform and payment gateway APIs for suspicious activity.

    - Threats to Detect:

        - Malware and ransomware targeting endpoints.

        - Brute-force login attempts on web servers.

        - Phishing campaigns targeting customer support employees.

        - Data exfiltration via unauthorised API access.

    - Expected Outcomes:

        - Reduce MTTD for phishing emails by setting up automated alerts for suspicious URLs in inbound emails.

        - Decrease MTTR for server compromises by automating playbooks in a SOAR platform like Palo Alto Cortex XSOAR.

- **Simulation**:

    - Threat Detected: An attacker launches a brute-force attack on the web application.

    - SOC Response:

        1. SIEM alerts the SOC about failed login attempts exceeding the defined threshold.

        2. Analysts investigate and identify the attacker’s IP address.

        3. The IP is blocked in the firewall and an automated alert is sent to the cloud security team to investigate potential additional breaches.

2. ESTABLISH FRAMEWORK AND GOVERNANCE

2.1 Choose a Security Framework

Key Frameworks Overview:

1. **NIST Cybersecurity Framework (CSF):**
   - Focuses on five core functions:
     - Identify: Understand critical assets, risks and vulnerabilities.
     - Protect: Implement safeguards like firewalls, access controls and encryption.
     - Detect: Develop capabilities for identifying incidents (e.g., SIEM, IDS).
     - Respond: Establish processes to mitigate the impact of incidents.
     - Recover: Build resilience and ensure continuity through backup and recovery plans.
2. **MITRE ATT&CK:**
   - Comprehensive matrix detailing adversary tactics and techniques.
   - Enables mapping SOC detection rules to known attack vectors.
   - Examples include:
     - Initial Access (T1190): Exploitation of public-facing applications.
     - Credential Dumping (T1003): Tools like Mimikatz targeting stored credentials.
3. **ISO 27001:**
   - Focuses on implementing an Information Security Management System (ISMS).
   - Ensures governance, risk management and continuous improvement.
   - Covers policies like access control, incident management and audit compliance.

Example Scenario: Aligning a Retail SOC

- Context: A retail company’s SOC must align with a security framework to combat increasing cyber threats targeting payment systems.
- Frameworks Chosen:
  - NIST CSF: For its end-to-end approach in defining and improving cybersecurity processes.
  - MITRE ATT&CK: To map detection rules and strengthen proactive threat hunting capabilities.

Implementation Steps:

1. NIST CSF Implementation:
   - Identify critical systems such as the payment gateway and customer database.
   - Implement multi-factor authentication (MFA) and encryption to protect assets.
   - Build workflows for responding to ransomware attacks, ensuring backups are secure and recovery plans are tested.
2. MITRE ATT&CK Integration:
   - Use the framework to analyse threats like “Credential Dumping” (T1003).
   - Develop SIEM rules to flag tools such as Mimikatz.
   - Analysts simulate scenarios like lateral movement using stolen credentials, enabling better detection strategies.

Simulation Example:

- Threat Detected: A SIEM alert identifies suspicious activity indicating an attempt to dump credentials on a Windows server.
- Action: Analysts consult MITRE ATT&CK to map the tactic to Credential Access (T1003).
- SOC Response:
  - Isolate the affected server.
  - Investigate the originating IP and associated accounts.

    - Follow the NIST CSF “Recover” function by restoring the server from backups and reinforcing security measures.

2.2 Develop Policies and Procedures

Core Components:

1. Incident Response Policies:
    - Define severity levels (e.g., Low, Medium, High, Critical).
    - Outline communication protocols for each severity level.
    - Include steps for forensic investigation, such as evidence preservation and chain of custody.
2. SOC Charter:
    - Outlines the mission, vision and scope of the SOC.
    - Helps align team objectives with business priorities.
    - Example Charter:
        - Vision: Provide 24/7 monitoring to proactively detect and mitigate threats.
        - Mission: Protect assets, ensure compliance and continuously improve incident response.

Example Scenario: Izzmier E-Commerce Incident Response Plan

- High Severity Incident Definition: Exfiltration of customer payment data.
- Escalation Procedures:
    - Notify the executive team within 30 minutes.
    - Engage forensic investigators within 1 hour.

Simulation Example:

- Incident Detected: SIEM flags large outbound traffic from the payment database to an unfamiliar IP.
- SOC Response:

  - Analysts identify encrypted data leaving the server, confirming exfiltration attempts.
  - Escalate to Level 3 analysts to investigate deeper.
  - Disconnect the affected server and initiate forensic procedures to identify root cause and prevent recurrence.

2.3 Compliance

Regulatory Standards:

1. Healthcare (HIPAA):
   - Enforces safeguards to protect patient data (e.g., PHI monitoring).
2. Finance (PCI-DSS):
   - Ensures secure storage, processing and transmission of payment card data.
   - Requires encryption, regular vulnerability assessments and secure log storage.
3. General (GDPR):
   - Protects user privacy by ensuring proper data handling and breach notifications within 72 hours.

Example Scenario: Ensuring PCI-DSS Compliance for Izzmier E-Commerce

- Key Actions:
  - Encrypt customer payment data using AES-256.
  - Monitor payment gateway logs for unauthorised attempts.
  - Store all logs securely for a minimum of 1 year for audit purposes.

Simulation Example:

- Audit Findings: PCI-DSS audit identifies insufficient logging of database access attempts.
- SOC Action:
  - Implement database logging for every access query.
  - Review logs monthly to identify anomalies.

- Conduct regular compliance assessments to ensure adherence.

3. SOC ARCHITECTURE DESIGN

3.1 SOC Layers

1. Core Components:

- SIEM (Security Information and Event Management):
  - Function: Central hub for collecting, correlating and analysing security logs.
  - Example Use: Detect brute force login attempts by correlating multiple failed login events from different servers.
  - Key Features:
    - Real-time alerts.
    - Log normalisation and aggregation.
    - Customisable dashboards for security monitoring.
- Threat Intelligence Platform (TIP):
  - Function: Enhances SOC capabilities by enriching alerts with threat context.
  - Example Use: Matching IPs flagged in SIEM alerts to known malicious indicators in threat feeds.
  - Key Features:
    - Aggregation of multiple threat feeds.
    - Automated threat scoring.
    - Integration with SIEM for enriched alert context.
- Case Management:
  - Function: Tracks incidents from detection to resolution.
  - Example Use: Assigning a high-severity ransomware alert to a Level 2 analyst for investigation.
  - Key Features:
    - Task assignments with timelines.
    - Incident documentation for audits.

        - SLA (Service Level Agreement) tracking.

2. Data Sources:

- Network Devices:
    - Logs from firewalls, routers and switches to monitor and analyse network traffic.
    - Example: Identifying unusual outbound traffic from a specific IP range that bypasses firewall rules.
- Endpoint Devices:
    - Logs from Endpoint Detection and Response (EDR) tools and antivirus software for identifying threats on workstations or servers.
    - Example: Detecting malware execution via suspicious processes flagged by EDR.
- Cloud Environments:
    - Logs from cloud services like AWS CloudTrail, Microsoft Azure Activity Logs and Google Cloud Operations.
    - Example: Monitoring login attempts to a cloud environment from anomalous geolocations.
- Applications:
    - Logs from business-critical applications such as email platforms, customer management systems or ERP tools.
    - Example: Detecting unauthorised administrative access in Microsoft 365.

3. Integration:

- A unified SOC ecosystem requires seamless integration of all data sources to enable efficient monitoring.
- Example Integration:
    - Scenario: SD-WAN logs integrated into the SIEM to detect potential data exfiltration through abnormal traffic patterns.
    - Outcome: Enhanced visibility into branch office traffic and quick identification of network anomalies.

3.2 Choose SIEM Technology

1. SIEM Options:

- Splunk:
  - Strengths: Advanced analytics, scalability and robust visualisation tools.
  - Ideal For: Large organisations with high log volumes or diverse data sources.
  - Example: A multinational e-commerce company processing millions of transactions daily benefits from Splunk's scalable log ingestion.
- QRadar:
  - Strengths: AI-driven detection and strong compliance features.
  - Ideal For: Industries with stringent regulatory requirements (e.g., healthcare, finance).
  - Example: A hospital uses QRadar to ensure HIPAA compliance by monitoring patient data access.
- Azure Sentinel:
  - Strengths: Native integration with Microsoft Defender and seamless cloud monitoring.
  - Ideal For: Organisations with heavy Microsoft investments or multi-cloud environments.
  - Example: A tech company monitors Azure workloads and Office 365 logs through Azure Sentinel.
- Elastic SIEM:
  - Strengths: Cost-effective, open-source solution with high customisability.
  - Ideal For: Organisations with budget constraints or technical expertise for customisation.
  - Example: A startup uses Elastic SIEM to build cost-efficient custom detection rules for its SaaS platform.

2. Factors to Consider:

- Log Ingestion Rates:

- Estimate current and future log volumes to prevent SIEM performance bottlenecks.
- Example: A company generating 2TB of logs daily needs a SIEM with scalable ingestion capacity.

- Scalability:
  - Ensure the chosen SIEM can grow with the organisation’s needs.
  - Example: Elastic SIEM offers scalable architecture for growing startups.
- Budget:
  - Evaluate licensing, hardware, support and personnel costs.
  - Example: Azure Sentinel offers predictable costs based on data ingested, ideal for cloud-first organisations.
- Integration Capabilities:
  - Choose a SIEM compatible with existing tools and platforms.
  - Example: Splunk integrates easily with TIPs, firewalls and EDR solutions for centralised monitoring.

Example Scenario: SIEM Selection for an E-Commerce Company

- Context: Multi-cloud environment with AWS, Azure and on-premise systems.
- Solution: Splunk is selected for its ability to handle diverse log sources and high data volumes.
- Outcome: Enhanced visibility and streamlined threat detection across all environments.

3.3 SOC Deployment Model

1. Deployment Options:

- In-House SOC:
  - Full control over operations, enabling custom workflows and deeper integrations.
  - Challenges: Requires significant investment in infrastructure, personnel and training.

    - Example: A bank establishes an in-house SOC to meet strict compliance standards like PCI-DSS.

- Hybrid SOC:
    - Combines internal capabilities with MSSPs for cost efficiency and extended coverage.
    - Example: A manufacturing company operates an in-house SOC during business hours and relies on an MSSP for 24/7 monitoring.
    - Advantages: Reduced costs and access to MSSP expertise.

2. Example Hybrid Deployment:

- Scenario:
    - An organisation with limited staffing maintains in-house analysts for daytime operations.
    - MSSP monitors during off-hours, ensuring round-the-clock threat detection.
- Outcome:
    - Continuous monitoring, cost optimisation and reduced alert fatigue for in-house analysts.

4. BUILD THE SOC TEAM

4.1 Define Roles and Responsibilities

A SOC (Security Operations Centre) team is structured with distinct roles, each critical for effective threat detection, investigation and response. Below are the typical roles and their responsibilities:

Role	Responsibilities
SOC Manager	- Oversees the SOC's operations, strategy and performance. - Allocates resources and defines workflows. - Prepares reports and aligns SOC goals with organisational objectives.
Level 1 (L1) Analyst	- Monitors alerts generated by SIEM tools. - Triages and prioritises incidents based on severity and impact. - Creates tickets and escalates incidents to L2 analysts if needed.
Level 2 (L2) Analyst	- Investigates escalated incidents and performs in-depth analysis of logs and alerts. - Conducts root cause analysis (RCA). - Responds to incidents by containing and remediating threats.
Level 3 (L3) Analyst	- Handles advanced incident investigations, including digital forensics and malware analysis. - Performs proactive threat hunting to identify unknown threats. - Develops detection use cases and optimises SOC processes.
SOC Engineer	- Maintains and updates SOC infrastructure, including SIEM, TIP and EDR tools. - Configures log collection and ensures seamless tool integration. - Monitors system health and resolves operational issues.

Threat Intelligence Analyst	- Gathers and analyses external threat intelligence to provide context for SOC alerts. - Identifies Indicators of Compromise (IOCs) and Indicators of Attack (IOAs) for proactive defence. - Works with L2/L3 analysts to enhance detection rules.

4.2 Training and Certification

Continuous learning and skill development are essential for an effective SOC team. Training and certifications should align with the roles and responsibilities.

Certifications:

- Level 1 (L1) Analyst:
    - CompTIA Security+: Covers foundational cybersecurity knowledge, including network security, threats and vulnerability management.
    - EC-Council Certified SOC Analyst (CSA): Focuses on SOC operations, incident monitoring and basic threat detection skills.
- Level 2/Level 3 (L2/L3) Analyst:
    - GIAC Certified Incident Handler (GCIH): Specialises in incident response techniques, forensic analysis and malware investigation.
    - Certified Ethical Hacker (CEH): Covers penetration testing techniques and attacker methodologies.
- SOC Manager:
    - Certified Information Systems Security Professional (CISSP): Emphasises leadership in security strategy, risk management and governance.
    - Certified Information Security Manager (CISM): Focuses on aligning security operations with organisational goals.

Training Exercises:

- Simulated Incident Response:

    - Use tools like Cyber Range to simulate real-world attacks (e.g., ransomware or DDoS attacks).
    - Ensure the team practices triaging, RCA, containment and remediation during these scenarios.

- Red Team/Blue Team Exercises:
    - Blue Team Training: Focuses on monitoring, detection and response using SOC tools.
    - Red Team Simulation: Simulates adversarial tactics to test SOC defences.
    - Outcome: Identifies gaps in detection rules and response procedures.
- Tabletop Exercises:
    - Walkthrough of hypothetical incidents, such as insider threats or advanced persistent threats (APTs).
    - Helps the team understand roles, communication channels and escalation paths.
- Threat Hunting Labs:
    - Focused exercises where L3 analysts use tools like Splunk or Elastic Stack to identify suspicious patterns and anomalies.
- Incident Retrospectives:
    - Post-incident review sessions to evaluate the effectiveness of detection and response strategies.
    - Outcome: Updates detection rules and improves SOC processes based on lessons learned.

5. MONITORING AND INCIDENT HANDLING

Monitoring and incident handling are the backbone of effective SOC operations, ensuring proactive threat detection and timely response to minimise damage.

5.1 Log Sources to Monitor

Effective monitoring requires comprehensive visibility across an organisation's infrastructure. Below are key log sources and their relevance:

- Endpoint Logs:
    - Tools: Endpoint Detection and Response (EDR), antivirus.
    - Importance: Capture malware infections, unauthorised application execution and privilege escalation attempts.
    - Example: Detect PowerShell execution with unusual parameters indicative of malware.
- Network Traffic Logs:
    - Tools: Firewalls, switches, intrusion detection/prevention systems (IDS/IPS).
    - Importance: Identify suspicious traffic patterns, port scans and lateral movement.
    - Example: Alert on unusual traffic from an internal server to an external IP address.
- Cloud Logs:
    - Tools: AWS CloudTrail, Azure Monitor, Google Cloud Logging.
    - Importance: Monitor user activity, configuration changes and unauthorised access in cloud environments.
    - Example: Flag multiple failed login attempts followed by a successful login from an unusual location.
- Application Logs:
    - Sources: Web servers (e.g., Apache, NGINX), database logs (e.g., MySQL, MSSQL).
    - Importance: Detect injection attacks, abuse of application functionalities and anomalies in database queries.

  - Example: Log and alert on excessive SELECT statements that suggest potential data scraping.

5.2 Define Detection Rules

Detection rules help identify suspicious behaviours or deviations from normal activity. Below are some examples:

- Unauthorised Access Attempts:
  - Rule: Monitor failed login attempts across endpoints, applications and cloud services.
  - Threshold: Trigger an alert after 5 failed logins within 10 minutes from the same IP.
  - Example Alert: "Multiple failed login attempts on admin account from IP 192.168.1.25."
- Lateral Movement:
  - Rule: Detect unusual communication between internal servers, such as SMB or RDP connections.
  - Example: Alert when a workstation initiates RDP sessions with multiple servers within a short period.
- Data Exfiltration:
  - Rule: Monitor large outbound data transfers to unknown or blacklisted IPs.
  - Example: "Outbound traffic exceeding 500 MB to 123.45.67.89 detected from file server."
- Malware Execution:
  - Rule: Alert on the execution of known malicious hashes or tools like Mimikatz.
  - Example: "Mimikatz.exe execution detected on endpoint DESKTOP-01."
- Privilege Escalation:
  - Rule: Detect the addition of users to privileged groups, e.g., "Domain Admins."
  - Example: "User 'attacker' added to 'Domain Admins' group via PowerShell."

5.3 Incident Response Playbooks

Incident response playbooks are step-by-step guides to handle specific threats effectively. Below is a detailed example:

Example Playbook: Ransomware Response SOP

Objective: Contain and mitigate ransomware attacks to minimise data loss and downtime.

Step 1: Isolate Affected Systems

- Actions:
  - Disconnect infected endpoints from the network (manual or automated).
  - Shut down any shared drives or storage systems to prevent further encryption.
- Tools:
  - Endpoint isolation features in EDR tools.
  - Network Access Control (NAC).

Step 2: Use SIEM to Trace Initial Access

- Actions:
  - Analyse logs to determine how ransomware entered (e.g., phishing email, RDP attack).
  - Identify the "patient zero" endpoint or user.
- Tools:
  - SIEM correlation rules to trace suspicious activities preceding encryption.
  - Analyse email logs for malicious attachments or links.

Step 3: Block Associated IPs/Domains in the Firewall

- Actions:
  - Identify Command and Control (C2) IPs from threat intelligence feeds.
  - Block associated IPs/domains at the perimeter firewall.
- Tools:

    - Firewall management consoles.
    - Threat intelligence platforms (TIP).

Step 4: Conduct Root Cause Analysis (RCA)

- Actions:
    - Examine malware samples to understand encryption mechanisms.
    - Identify weaknesses in the environment (e.g., unpatched software, weak passwords).
- Tools:
    - Sandbox environments for malware analysis.
    - Vulnerability scanners like Nessus or Qualys.

Step 5: Recovery and Lessons Learned

- Actions:
    - Restore from clean backups.
    - Apply patches and tighten security configurations.
    - Conduct a post-incident review to update playbooks and detection rules.
- Tools:
    - Backup solutions like Veeam or Acronis.
    - Collaboration tools for incident debriefs.

Simulation Example

Incident: The SIEM generates an alert indicating an unusual spike in outbound encrypted traffic. Further investigation reveals files on a server have been renamed with a .locked extension.

SOC Actions:

1. The L1 analyst isolates the server to prevent further spread.
2. The L2 analyst reviews firewall logs and discovers communication with a known ransomware C2 IP.

3. The L3 analyst analyses the encrypted files and malware samples, identifying the ransomware strain.

4. The SOC updates detection rules and blocks the malicious IP globally across firewalls.

6. TEST AND OPTIMISE

Testing and optimising the SOC ensures its effectiveness in detecting and responding to threats while continuously improving performance and efficiency.

6.1 Simulate Threat Scenarios

Simulating threat scenarios allows SOC teams to assess their readiness and improve detection and response capabilities. Below are detailed examples:

Phishing Simulation:

1. **Objective:** Test SOC analysts' ability to detect and respond to phishing attempts.
2. **Steps:**
    - Create a realistic phishing email, e.g., a fake message from HR requesting credentials to view a "policy update."
    - Distribute the email to test accounts or analysts in a controlled environment.
    - Monitor how quickly and accurately analysts identify the email as phishing.
    - Escalate the case through the SOC workflow to measure response times.
3. **Evaluation Metrics:**
    - Time taken to detect and report the phishing attempt.
    - Accuracy in identifying the phishing indicators.
    - Effectiveness of escalation and response actions.

Insider Threat Simulation:

1. **Objective:** Test the SOC's ability to detect and mitigate insider threats.
2. **Steps:**
    - Simulate privilege escalation by a "rogue" employee account.
    - Example: An account suddenly gains administrative privileges and accesses sensitive files.
    - Use SIEM to create correlation rules that flag unusual activity, such as privilege changes or abnormal file access patterns.
3. **Evaluation Metrics:**

    - Detection speed for suspicious account activity.
    - Ability to correlate logs from multiple sources (e.g., Active Directory, file servers).
    - Resolution time and accuracy of mitigation actions.

6.2 Conduct SOC Audits

Regular audits provide insights into the SOC's operational effectiveness and alignment with industry standards.

Testing Against Industry Benchmarks:

- Compare the SOC's performance against established standards like:
    - MITRE ATT&CK Framework: Validate the detection of common tactics and techniques used by adversaries.
    - NIST Cybersecurity Framework: Assess adherence to guidelines for identify, protect, detect, respond and recover functions.

Red Teaming and Penetration Testing:

- Red Teaming: Simulate real-world attacks to test the SOC's readiness and response.
    - Example: Conduct a simulated ransomware attack that includes initial access, lateral movement and data exfiltration.
- Penetration Testing: Identify vulnerabilities in systems and applications before attackers do.
    - Example: Test web applications for SQL injection or cross-site scripting (XSS) and evaluate the SOC's response.

Compliance Testing:

- Ensure the SOC aligns with regulatory requirements like GDPR, PCI DSS or ISO 27001.
- Use automated compliance tools to validate log retention policies, access controls and incident reporting.

6.3 Continuous Improvement

A SOC must evolve continuously to address emerging threats and improve efficiency.

Monitor Key Performance Indicators (KPIs):

1. **False Positive Rate:**
    - Measure the percentage of alerts that are incorrectly classified as threats.
    - Goal: Minimise false positives by refining detection rules and leveraging machine learning.
2. **Mean Time to Detect (MTTD):**
    - The average time taken to identify a security incident after its occurrence.
    - Goal: Reduce MTTD by improving alert prioritisation and analyst training.
3. **Mean Time to Respond (MTTR):**
    - The average time taken to resolve a security incident.
    - Goal: Optimise MTTR by automating repetitive tasks and improving playbooks.

Update SOPs and Training Regularly:

1. **SOP Updates:**
    - Incorporate lessons learned from incidents and simulations into existing playbooks.
    - Example: After detecting a new malware strain, update the ransomware response SOP with specific indicators of compromise (IOCs).
2. **Regular Training:**
    - Conduct ongoing training for analysts using cyber ranges, Capture the Flag (CTF) challenges and hands-on labs.
    - Focus on emerging threats, such as cloud-native attacks or supply chain compromises.

Leverage Feedback Loops:

- Gather feedback from post-incident reviews, red team exercises and external audits to improve processes.
- Example: If a simulated phishing attack takes too long to detect, adjust email filtering rules and provide additional training on phishing indicators.

Automation and AI Integration:

- Use SOAR (Security Orchestration, Automation and Response) tools to streamline repetitive tasks, such as ticketing or blocking IPs.
- Integrate AI-driven analytics to identify anomalies and reduce alert fatigue.

Example Continuous Improvement Workflow:

1. Simulate a scenario where an insider accesses sensitive customer data.
2. Review SOC's performance in detecting and mitigating the activity.
3. Adjust correlation rules to improve detection.
4. Update training sessions to reinforce learning and address gaps.
5. Monitor KPIs post-implementation to assess the impact of changes.

7. STANDARD OPERATING PROCEDURES (SOPS)

The purpose of SOPs is to provide a clear, repeatable and consistent process for handling specific tasks and incidents within the SOC. Below are detailed SOPs for incident response, threat hunting and log monitoring.

7.1 Incident Response SOP

Purpose: To define the steps for handling and responding to cybersecurity incidents in a structured and efficient manner, minimising damage and ensuring a coordinated response.

Steps:

1. **Preparation:**
    - **Incident Response Tools:**
        - Ensure that all tools required for the incident response process, such as forensic tools (e.g., EnCase, FTK), malware analysis tools (e.g., Cuckoo Sandbox, VirusTotal) and network traffic analysis tools (e.g., Wireshark, Zeek), are up-to-date and functioning.
    - **Training:**
        - Regularly train all SOC team members on the usage of these tools, ensuring familiarity with their capabilities and interfaces. Conduct regular drills to ensure the team can efficiently use these tools during an active incident.
2. **Identification:**
    - **Alert Monitoring and Detection:**
        - Detect anomalies and potential incidents using SIEM alerts, network monitoring and endpoint detection solutions. Look for patterns like multiple failed logins, high traffic volume or unusual file access patterns.
    - **Alert Validation:**
        - Cross-reference the SIEM alerts with additional data sources like endpoint logs, firewall logs and intrusion detection systems (IDS). Confirm the legitimacy of the alert and escalate if necessary.
3. **Containment:**

- **System Isolation:**
  - As soon as an incident is confirmed, isolate affected systems from the network. This can involve disconnecting them physically or using network segmentation methods (e.g., placing the systems in a quarantine VLAN).
- **Block Malicious Entities:**
  - Use firewalls, proxy servers and DNS filtering tools to block malicious IP addresses, domains or known Command and Control (C2) servers.

4. **Eradication:**
   - **Root Cause Analysis:**
     - Identify the source of the breach, which could be a vulnerability, misconfiguration or compromised account. Perform forensic analysis to determine the attack vector.
   - **Remove Artifacts:**
     - Delete any malware, backdoors or compromised accounts that the attacker may have used. Patch vulnerabilities or change compromised credentials to ensure the attacker cannot re-enter the network.
5. **Recovery:**
   - **Restore Systems:**
     - Once the threat is eradicated, begin restoring systems from known clean backups or rebuild compromised systems.
   - **Monitor Restored Systems:**
     - After systems are restored to normal operations, monitor them closely for any signs of residual compromise or unusual activity.
6. **Post-Incident Review:**
   - **Post-Mortem Analysis:**
     - Conduct a thorough post-incident review to evaluate the effectiveness of the response and identify areas for improvement. Analyse the timeline of events, decision-making process and tools used during the incident.

- **Update Playbooks:**
  - Update incident response playbooks based on lessons learned and ensure they reflect current threat intelligence, tactics, techniques and procedures (TTPs) identified during the incident.

7.2 Threat Hunting SOP

Purpose: To proactively search for undetected threats within the organisation, improving detection capabilities and reducing the time attackers remain undetected.

Steps:

1. **Hypothesis Generation:**
   - Leverage Threat Intelligence:
     - Utilise threat intelligence feeds (e.g., from open-source or commercial sources) to generate hypotheses on potential attack scenarios based on emerging trends, new vulnerabilities and active threat actor tactics (e.g., MITRE ATT&CK).
   - Use Known Attack Patterns:
     - Build hypotheses around known attack methodologies like lateral movement, privilege escalation or data exfiltration that may not yet be detected by traditional controls.
2. **Data Collection:**
   - Query SIEM and Endpoint Logs:
     - Use SIEM platforms (e.g., Splunk, QRadar) to query logs for patterns related to your hypothesis (e.g., looking for signs of privilege escalation or unusual login times).
     - Gather logs from endpoint detection and response (EDR) systems, firewall logs and network traffic logs for signs of suspicious activity.
3. **Analysis:**
   - Use Analytics Tools:
     - Leverage tools like Splunk or Kibana to analyse large datasets and identify suspicious patterns in the data. Look for anomalies in behavior, such as abnormal access patterns or unusual network traffic.

- Manual and Automated Correlation:
    - Correlate different data sources to identify activity that may suggest an ongoing attack, such as an unusual sequence of events leading to a privilege escalation attempt or data exfiltration.

4. **Response:**
    - Escalate Confirmed Findings:
        - When suspicious or malicious activity is identified, escalate findings to the incident response team for immediate action. Provide them with comprehensive data from the hunt to aid their investigation.
    - Communicate Findings:
        - Share all relevant findings with the broader SOC team to enhance their knowledge and improve future threat detection capabilities.
5. **Documentation:**
    - Log Findings:
        - Ensure all threat hunting activities are logged into a case management system for documentation purposes. Include details about the hypothesis, data collected, analysis performed and any findings.
    - Reporting:
        - Create formal reports summarising the findings and any actions taken during the threat hunt. Share these reports with stakeholders to increase awareness of potential threats.

7.3 Log Monitoring SOP

Purpose: To ensure consistent and effective log analysis, enabling the detection of security incidents early and providing insight into network and endpoint activity.

Steps:

1. **Log Collection:**
    - Identify Critical Log Sources:

        - Ensure that logs from critical sources such as firewalls, EDR systems, web servers, database servers and operating systems are being collected and centralised into the SIEM.

    - Validate Log Ingestion:

        - Regularly validate that logs are properly ingested into the SIEM without loss of data. This ensures that no critical data is missing, which could impact the detection of malicious activity.

2. **Alert Configuration:**

    - Set Thresholds for Anomalies:

        - Configure the SIEM to generate alerts based on defined thresholds for anomalous behavior (e.g., more than 10 failed login attempts in 5 minutes, unusual traffic volume or access to sensitive files at odd hours).

    - Tuning Alerts:

        - Continuously fine-tune SIEM alert rules to reduce false positives while ensuring they accurately reflect significant security events.

3. **Review and Analysis:**

    - Prioritise High-Severity Alerts:

        - Use dashboards or customised views in the SIEM to quickly identify and prioritise high-severity alerts. Investigate these alerts promptly to determine whether they represent legitimate threats.

    - Log Correlation:

        - Correlate logs from multiple sources (e.g., firewall logs, EDR data and system event logs) to uncover potential threats or patterns that might not be obvious when analysed in isolation.

4. **Escalation:**

    - Handle False Negatives:

        - If alerts are deemed false negatives or recurrent patterns that aren't adequately detected, escalate the findings to the SOC Engineer or other appropriate personnel to fine-tune detection rules.

    - Ongoing Improvement:

- As part of continuous improvement, update detection rules and fine-tune the SIEM to ensure it remains responsive to new attack techniques.

8. PROCESS FLOWS

In a Security Operations Center (SOC), having clear and structured process flows ensures that incidents and threats are handled efficiently and effectively. Below are detailed process flows for Incident Management and Threat Hunting, outlining each stage from detection to closure or escalation.

8.1 Incident Management Process Flow

This process flow outlines the lifecycle of an incident from the moment it's detected until its closure.

1. **Detection:**
   - Trigger Event:
     - An event or anomaly in the network, endpoint or application triggers an alert in the SIEM (Security Information and Event Management) system. Examples include multiple failed login attempts, abnormal traffic patterns or known indicators of compromise (IoCs).
   - Alerting:
     - The SIEM generates an alert with detailed information such as the source of the event, type of anomaly and severity. The alert can be classified as low, medium or high severity and the SOC team uses this classification to prioritise the response.
2. **Triage:**
   - L1 SOC Analyst Action:
     - The L1 SOC analyst receives the alert and conducts the initial triage, which involves:
       - Classifying the alert based on severity (e.g., false positive, potential threat).
       - Validating the alert by cross-referencing with related data sources (e.g., endpoint logs, firewall logs).
       - Determining Impact: Checking whether the alert is localised to a single system or affecting multiple systems in the network.
     - The L1 analyst classifies the alert and determines whether further investigation is needed.

3. **Investigation:**
    - L2 SOC Analyst Action:
        - If the alert is validated as a potential threat, it is escalated to the L2 SOC analyst, who will conduct a deeper investigation:
            - Log Analysis: Analysing detailed logs from various sources like network traffic, endpoint devices and servers.
            - Network Packet Analysis: If necessary, the L2 analyst may perform packet capture and analysis using tools like Wireshark or Zeek to gain a deeper understanding of the attack.
            - Identifying Threats: Investigating possible attack vectors (e.g., compromised credentials, malware execution) and collecting indicators of compromise (IoCs).
4. **Escalation:**
    - L3 or Incident Response Team (IRT) Action:
        - If the threat is advanced or beyond the capabilities of the L2 SOC analyst, the incident is escalated to the L3 SOC analyst or the Incident Response Team (IRT).
            - L3 SOC Analysts perform advanced forensics (e.g., examining disk images, reverse-engineering malware) and detailed threat analysis.
            - IRT works to contain the threat, prevent further damage and manage the legal, communication and recovery aspects of the incident.
        - The escalation process ensures that threats are tackled by experts with the necessary skills to mitigate the risk.
5. **Resolution:**
    - Containment, Eradication and Recovery:
        - Containment: Systems identified as compromised are isolated to prevent further damage, such as disconnecting from the network or shutting them down.

    - Eradication: The root cause of the incident (e.g., malware, attacker access points) is removed. This may include deleting malicious files, patching vulnerabilities and changing compromised credentials.
    - Recovery: Affected systems are restored to normal operations. This may involve rebuilding compromised systems, restoring from clean backups and monitoring for any signs of re-infection.
    - Once these steps are completed, the incident is considered resolved from a technical perspective.

6. **Closure:**
    - Documentation and Reporting:
        - The incident is formally documented and a report is generated, detailing the timeline of events, response actions and lessons learned.
        - Playbook Update: If any new techniques or tactics were used by the attacker, the incident response playbook is updated to include steps for handling similar threats in the future.
        - The closure process also includes conducting a post-incident review to analyse the effectiveness of the response and identify areas for improvement in the SOC's procedures.

8.2 Threat Hunting Process Flow

Threat hunting is a proactive process designed to uncover threats that may not have been detected by traditional security tools. It involves actively searching for signs of compromise based on known tactics, techniques and procedures (TTPs).

1. **Threat Intel Analysis:**
    - Leverage External Intelligence:
        - Threat intelligence feeds are gathered from various sources (e.g., commercial threat intelligence providers, open-source intelligence, vendor reports). The SOC team reviews this intel to identify emerging trends, new attack techniques or indicators of compromise (IoCs).
        - Review MITRE ATT&CK Framework: Use frameworks like MITRE ATT&CK to guide hypothesis generation by reviewing known attack vectors and techniques used by advanced persistent threats (APT) groups or cybercriminals.

2. **Query Logs:**
    - Log Review for IoCs:
        - Armed with external intelligence, the SOC analyst begins querying logs from SIEM, EDR (Endpoint Detection and Response) systems and network monitoring tools to identify IoCs such as unusual login times, abnormal network traffic or the presence of known malware signatures.
        - Analysts use search tools in the SIEM or other log aggregation platforms (e.g., Splunk, Kibana) to look for patterns matching the identified IoCs.
3. **Correlate Findings:**
    - Cross-Check with Historical Data:
        - Any suspicious or anomalous findings are cross-checked with historical data to determine whether they are part of a larger pattern or ongoing threat campaign.
        - Correlation of multiple data sources (e.g., historical alerts, past incidents, network traffic and endpoint activity) helps identify complex attack scenarios that may not be immediately obvious from individual logs.
4. **Escalate Threats:**
    - Incident Response Escalation:
        - If the threat hunt uncovers evidence of malicious activity, the findings are escalated to the Incident Response Team (IRT) or L3 SOC analysts for immediate investigation and response.
        - The escalation includes detailed reports of the findings, including the IoCs, affected systems and potential impact to help the response team quickly assess the situation and initiate containment actions.

9. SOC WORKFLOW

A well-structured workflow is essential for the smooth operation of a Security Operations Center (SOC), especially in a 24/7 environment. It helps ensure that all incidents are addressed promptly, investigations are thorough and threats are detected and mitigated efficiently. Below are detailed workflows for both Daily Workflow and Shift Workflow in a 24/7 SOC environment.

9.1 Daily Workflow

The daily workflow establishes a consistent process for SOC teams to monitor and respond to incidents, review past activities and ensure effective transitions between shifts.

1. **Morning:**
   - Review Previous Day's Incidents:
     - The first task of the day is to review incidents that occurred during the previous shift. This allows the team to stay up to date on ongoing incidents and provides an opportunity to ensure that all actions taken were documented and follow-up tasks are assigned.
     - The review also includes checking any unresolved tickets or incidents that might require additional investigation.
   - Check SIEM for Overnight High-Severity Alerts:
     - The SOC team examines SIEM logs to identify high-severity alerts that were generated overnight (during the night shift or after business hours). These may include potential threats or suspicious activities that need immediate attention.
     - The team prioritises any alerts that could escalate into critical incidents or affect business operations.
2. **Midday:**
   - Monitor Dashboards:
     - Throughout the day, SOC analysts monitor SOC Dashboards for active incidents, ongoing investigations and newly triggered alerts. Dashboards provide a visual overview of system health, network activity and security incidents.
     - The team continuously checks the status of open incidents, ensuring that high-priority alerts are being handled efficiently.

- Conduct Investigations or Threat Hunts:
    - Investigations: Analysts examine ongoing incidents, following escalation paths, analysing logs, conducting root cause analysis (RCA) and performing forensic investigations if required.
    - Threat Hunts: SOC teams proactively search for unknown threats by analysing logs, network traffic and endpoints for suspicious activity (e.g., lateral movement, data exfiltration). The goal is to identify hidden threats that may have evaded detection by automated systems.

3. **End of Day:**
    - Handover Documentation for Next Shift:
        - As the shift ends, it is crucial for the team to prepare a handover report for the incoming shift. This ensures that the next shift is aware of any ongoing incidents, high-severity alerts or any actions that need to be taken.
        - The handover should include:
            - Incident Status: A summary of current incidents, their severity and ongoing actions.
            - Pending Tasks: Any tasks that were not completed, with details on what is required to address them.
            - Critical Alerts: Any major alerts or issues requiring immediate attention.
            - Log Analysis Results: If ongoing investigations or threat hunts were initiated, the handover should provide key findings and next steps.

9.2 Shift Workflow (24/7 SOC)

For a 24/7 SOC, where there are multiple shifts in a day, each shift is responsible for specific activities that ensure continuous monitoring, detection and response to security incidents.

Time	Activity	Responsibility
Start of Shift	Receive shift handover. The incoming shift reviews the handover documentation from the previous shift to understand ongoing incidents, escalations or pending investigations.	All team members (L1, L2, L3)
Mid-Shift	Perform log analysis and investigations. Analysts continuously monitor logs and alerts, performing detailed investigations into detected anomalies. L1 analysts focus on monitoring and triaging alerts, while L2 analysts dive deeper into high-priority or escalated incidents.	L1/L2 Analysts
End of Shift	Escalate critical issues if needed. The Shift Lead ensures that any critical incidents or unresolved issues are escalated to the next shift and that the incident response team is informed. The Shift Lead also reviews ongoing investigations, ensuring that no major gaps are left in coverage. Handover Documentation: The Shift Lead or designated team member prepares a report for the next shift, summarising the current status of incidents, alerts and any actions taken, ensuring seamless continuity between shifts.	Shift Lead (L3)

Additional Details for Shift Workflow:

- Incoming Shift Responsibilities:

    - The team members starting their shift should read through the incident logs and SIEM alerts from the previous shift, taking note of high-priority or time-sensitive issues.

    - Team Coordination: All team members should coordinate to address outstanding tasks or escalate issues that require immediate attention. This can include restarting monitoring of specific systems or escalating certain alerts that were not fully addressed.

- **Mid-Shift Monitoring:**

    - The SOC team's focus during this phase is continuous monitoring and incident investigation. This involves real-time monitoring and tracking of logs, network activity and system alerts.

    - The SOC team must constantly reassess the severity of ongoing incidents to ensure that no alerts fall through the cracks.

    - Analysts should also review dashboards to detect any unusual patterns or anomalies, which might not be captured by automatic alerting mechanisms.

- **End of Shift Responsibilities:**

    - The Shift Lead plays a crucial role in the end-of-day handover process. They ensure that incidents are not left unresolved and that critical alerts and ongoing investigations are escalated to the incoming shift.

    - A shift report should include details such as:

        - Current Incident Status: Including any ongoing investigations or critical issues.

        - Pending Tasks: Any tasks that were not completed during the shift.

        - New Alerts: Any alerts that emerged during the shift but require attention.

        - Escalation Summary: If any issues need immediate escalation, the Shift Lead ensures a detailed explanation is provided.

10. PLAYBOOKS

Playbooks are critical for guiding security operations center (SOC) teams through structured responses to common cybersecurity incidents. By following these playbooks, the team can respond consistently, minimise damage and ensure effective recovery from various security breaches. Below are more detailed descriptions of two common playbooks: Ransomware and Phishing.

10.1 Ransomware Playbook

Objective:
To contain, respond to and recover from a ransomware attack, ensuring minimal damage and fast restoration of affected systems.

1. **Detection:**
   - Alert Triggered for Encrypted Files:
     - The SIEM system detects and raises an alert when files begin to show signs of encryption. This could involve specific file extensions being renamed or the use of encryption-related tools.
   - Lateral Movement or Data Exfiltration:
     - The SIEM may also identify lateral movement across the network or data exfiltration attempts, which are often associated with ransomware spreading or preparing for an attack.
2. **Initial Response:**
   - L1 Analyst Isolates Affected Machines:
     - The first action taken by L1 analysts is to immediately isolate affected systems from the network to prevent further encryption or spread of the ransomware.
     - Affected machines should be disconnected from the network and if possible, any shared resources like file servers should be locked down.
   - Notify Stakeholders:
     - The incident response team notifies internal stakeholders, including IT, management and relevant departments, ensuring everyone is aware of the ongoing issue and can assist if needed.

        - Communication should be clear, concise and aimed at limiting panic or confusion.

3. **Investigation:**

    - L2 Analyst Traces the Origin of the Attack:

        - The L2 analyst reviews system logs and network traffic data to trace back the origin of the ransomware attack. This includes looking for unusual login activities, suspicious file access or other signs of initial compromise.

        - The analyst checks for any suspicious activity in endpoints, such as unexpected installations or changes in file structures.

    - Identify Indicators of Compromise (IoCs):

        - L2 analysts gather indicators of compromise, such as:

            - IPs associated with the attack.

            - File hashes of encrypted files or malicious executables.

            - Any domains or URLs linked to the attack.

        - These IoCs are crucial for blocking further malicious activity and assisting in a broader investigation.

4. **Eradication:**

    - Disconnect and Clean Affected Machines:

        - Once the origin and extent of the attack are understood, all affected machines must be disconnected from the network to prevent the ransomware from spreading further.

        - The systems should undergo a deep cleaning process where all traces of the ransomware (including malware, executables and registry entries) are removed.

    - Apply Patches to Vulnerabilities:

        - Any vulnerabilities that the ransomware exploited should be patched immediately. This could involve updating software, applying security patches or removing any unneeded services that may have been targeted.

5. **Recovery:**
    - Restore Data from Backups:
        - Once systems are cleaned and vulnerabilities patched, data should be restored from clean backups. It's crucial to ensure the backups are free from ransomware before restoring them.
        - Any systems that were fully encrypted should be restored to a known good state from backups.
    - Monitor Restored Systems for Anomalies:
        - After restoration, analysts should monitor the restored systems for unusual behavior that might suggest remnants of the ransomware or new vulnerabilities.
        - Continuous monitoring is necessary for at least 24-48 hours after recovery to ensure no malicious activity resurfaces.
6. **Post-Incident Actions:**
    - Conduct a Root Cause Analysis:
        - A root cause analysis (RCA) is performed to understand how the attack happened, what vulnerabilities were exploited and whether any existing controls failed.
        - The results of the RCA can be used to adjust security measures and strengthen defenses.
    - Update the Ransomware Playbook:
        - The lessons learned from the attack are used to update the ransomware playbook to reflect new tactics, techniques and procedures (TTPs) that can help prevent or better respond to future attacks.
        - This includes adjusting detection rules in SIEM and improving preventive measures like network segmentation, endpoint protection or email filters.

10.2 Phishing Playbook

Objective: To efficiently respond to phishing incidents, including email-based attacks that attempt to steal user credentials, install malware or gain unauthorised access.

1. **Detection:**
    - Alert Triggered for Malicious Email Attachment or Link:
        - The SIEM or email security system generates an alert when a malicious email is detected, typically containing a harmful attachment or link that could lead to malware execution or credential harvesting.
        - This could be triggered by identifying known phishing signatures or abnormal email behavior (e.g., email spoofing or unusual attachment types).
    - User Reports a Phishing Attempt:
        - Users who receive phishing emails may report them to the SOC, enabling a faster response. A clear and accessible process for reporting phishing attempts should be in place, such as a "Report Phishing" button or email address.
2. **Initial Response:**
    - L1 Analyst Verifies the Email:
        - L1 analysts first verify the reported email or detected alert to confirm it is a phishing attempt. This involves checking:
            - Sender's email address and verifying if it matches the claimed identity.
            - Links or attachments within the email to determine if they lead to malicious sites or contain harmful payloads.
        - If verified, the L1 analyst begins initial containment actions.
    - Notify Recipients of the Phishing Email:
        - The SOC team should notify all users who received the phishing email, warning them not to open attachments or click on links. If the email was targeted at specific users, they should be informed individually.
        - Organisations can use their internal communication tools (e.g., email, chat or intranet) to notify affected users.
3. **Investigation:**

- L2 Analyst Analyses the Payload:
    - The L2 analyst inspects any malicious payload contained within the phishing email. This could include analysing the malicious link, attachment or malware. Common tools include sandbox environments to observe how the attachment behaves.
    - The analyst looks for signatures or patterns in the payload that can help identify the type of attack (e.g., credential phishing, malware distribution).
- Check for Affected Accounts:
    - Analysts should check whether any user accounts were compromised by verifying logins or signs of unauthorised access. They may look for unusual login times, IP addresses or locations.
    - Account-related activities, such as password resets or changes, should be carefully reviewed.

4. **Mitigation:**
    - Block Sender Domain and Associated IPs:
        - The first mitigation step involves blocking the sender's email domain and any associated IP addresses in the email security system to prevent further emails from reaching users.
        - Organisations may also add these domains and IPs to blacklists or blocklists.
    - Reset Compromised Credentials:
        - If any accounts are confirmed as compromised, password resets should be performed immediately. Multi-factor authentication (MFA) should be enabled on affected accounts to provide an extra layer of security.
        - Users may need guidance on selecting strong passwords or using password managers to avoid future incidents.
5. **Follow-Up:**
    - Train Users on Phishing Awareness:

    - SOC teams should use the incident as an opportunity to educate users on phishing awareness. This could include sending out a phishing awareness training session or a reminder on identifying phishing emails.

    - Users should also be encouraged to report suspicious emails to the SOC.

  - Update Phishing Detection Rules in SIEM:

    - The playbook concludes by ensuring that the detection rules in the SIEM are updated based on the attack method used. If new indicators or patterns are identified during the incident investigation, they should be incorporated into the detection mechanisms.

    - This improves the ability of the SOC to detect similar attacks in the future.

11. ADDITIONAL INSIGHTS

This section focuses on enhancing SOC operations through the use of Key Performance Indicators (KPIs) and effective tools integration. These metrics and tools are essential for measuring the performance of a SOC, streamlining workflows and improving threat detection and response capabilities.

11.1 KPIs for SOC Operations

Key Performance Indicators (KPIs) help monitor the effectiveness of SOC operations and highlight areas for improvement. These metrics track detection speed, response efficiency and the overall health of the SOC. Below are some critical KPIs used in SOC operations:

1. **Detection Metrics:**
   - Time to Detect (TTD):
     - Definition: TTD measures how quickly the SOC can identify a threat after it enters the network or an event occurs. It is critical because the longer it takes to detect a threat, the more damage it can cause.
     - How to Measure: Track the time between the initial attack or anomaly and the time it is flagged by the monitoring tools (SIEM).
     - Optimisation Tip: Lowering TTD involves improving detection methods, enhancing SIEM capabilities and refining alert rules.
   - Target: A lower TTD signifies quicker detection of threats. Ideal TTD ranges from minutes to a couple of hours, depending on the severity and complexity of the threat.
2. **Response Metrics:**
   - Time to Contain (TTC):
     - Definition: TTC measures how long it takes from the detection of a threat to its containment. Containment refers to isolating the affected systems or network segments to prevent further damage.
     - How to Measure: Track the duration from the time a threat is detected to the time containment actions are initiated (e.g., isolating affected machines, blocking malicious IP addresses).
     - Optimisation Tip: Improve automation in response workflows and better integration of incident response tools to shorten containment time.

- Time to Remediate (TTR):
    - Definition: TTR measures how long it takes to completely address and resolve a security incident. Remediation includes cleaning up infected systems, removing malicious artifacts and restoring normal operations.
    - How to Measure: Track the time from containment to the complete removal of the threat and restoration of services.
    - Optimisation Tip: Conduct regular vulnerability assessments and improve patch management processes to speed up remediation.
- Target: A well-performing SOC will aim for low TTC and TTR times. The faster containment and remediation happen, the lower the overall impact of the attack.

3. **Efficiency Metrics:**
    - Number of False Positives:
        - Definition: False positives occur when a legitimate activity or benign event is incorrectly flagged as a threat by the monitoring system. High numbers of false positives can drain resources and reduce analyst productivity.
        - How to Measure: Track the number of alerts flagged by the SIEM or other detection systems that, upon investigation, turn out to be non-malicious.
        - Optimisation Tip: Fine-tune alert rules and improve detection thresholds to minimise false positives. Regularly update threat intelligence feeds and correlation rules to improve accuracy.
    - Target: Strive for minimal false positives, ensuring that the alerts raised are mostly actionable and relevant to ongoing investigations.

11.2 Tools Integration

Effective tools integration is vital for a smooth SOC workflow, enabling teams to detect, respond and manage security incidents more efficiently. Here are the primary categories of tools that enhance SOC operations:

1. **Orchestration Tools:**
    - SOAR Platforms:

    - Definition: Security Orchestration, Automation and Response (SOAR) platforms provide integrated tools to automate and streamline security operations. They help automate repetitive tasks, improve response times and orchestrate workflows across different security tools.
    - Examples:
        - Palo Alto Cortex XSOAR: A comprehensive SOAR platform that integrates threat intelligence, incident response and security monitoring tools. It enables automated workflows to help SOC teams respond faster and with fewer manual interventions.
        - Splunk Phantom: An automation platform designed for security operations, allowing SOC teams to automate manual tasks and integrate with other tools, such as SIEM, threat intel sources and ticketing systems, to facilitate faster responses.
    - Use Cases: Automating common workflows like investigating alerts, correlating data from multiple sources and generating incident reports. SOAR platforms also enable the creation of playbooks that provide SOC teams with predefined, automated response actions.
  - Optimisation Tip: By integrating SOAR platforms, SOCs can significantly reduce manual intervention, improve response consistency and reduce human error during incident response.

2. **Threat Intel:**
    - Definition: Threat intelligence tools provide SOC teams with up-to-date information on emerging threats, attack techniques and known Indicators of Compromise (IoCs). Integrating threat intelligence sources into SOC operations improves detection, analysis and decision-making.
    - Examples:
        - VirusTotal: A tool used to analyse and identify files, URLs and domains for potential threats. It aggregates data from multiple antivirus engines and threat databases to give a comprehensive view of the security status of a file or domain.
        - Recorded Future: A threat intelligence platform that provides real-time data on cyber threats by analysing external sources, including dark web data, to predict potential attacks and provide actionable insights.

  - MISP (Malware Information Sharing Platform): An open-source threat intelligence platform that facilitates the sharing of threat data among organisations. It helps to detect emerging threats and understand attack patterns.

  - Use Cases: SOCs can use threat intelligence tools to enhance detection accuracy by adding external data to SIEM systems, correlate indicators of compromise and prioritise incidents based on the latest threat landscape.

- Optimisation Tip: Regularly integrate threat intelligence sources like VirusTotal and MISP into SIEM and SOAR platforms to ensure up-to-date, accurate and actionable threat data.

12. SIMULATIONS

Simulations are crucial for testing and improving the response strategies of SOC teams. They mimic real-world attack scenarios, allowing analysts to practice detecting, responding to and mitigating incidents in a controlled environment. Below are examples of common cybersecurity incident simulations, outlining the triggers and workflows for both insider threats and Distributed Denial-of-Service (DDoS) attacks.

12.1 Insider Threat Simulation

Objective: To simulate an insider threat scenario where a privileged user misuses their access to sensitive data or systems.

1. **Trigger:**
    - A privileged user (e.g., system administrator, IT support staff or executive) accesses files or systems that are restricted to their role. This could involve attempts to view, copy or exfiltrate sensitive company data, such as financial records or personal customer information.
    - The SIEM system detects this anomaly based on predefined rules (e.g., accessing files outside of the user's job role, access to large volumes of data).
2. **SOC Workflow:**
    - L1 Analyst (Detection):
        - Action: The L1 analyst receives an alert from the SIEM system regarding unusual access or unauthorised activity by a privileged user.
        - Step-by-Step:
            - Investigate the source of the alert, including the user account, the files accessed and the time of access.
            - Cross-reference the activity with the user’s defined role to determine whether the access aligns with their job duties.
            - Verify the alert with any contextual data (e.g., email or message history, task assignments) to determine if the access was valid or malicious.
        - Tools: SIEM, User and Entity Behavior Analytics (UEBA), Access Control Logs.

- L2 Analyst (Investigation):
    - Action: Once the anomaly is detected, the L2 analyst performs deeper analysis to confirm whether the access was unauthorised or potentially malicious.
    - Step-by-Step:
        - Review access logs for signs of data exfiltration or lateral movement within the network (e.g., abnormal file access patterns, use of external devices or abnormal login times).
        - Check for indicators of privilege escalation to ensure that the user did not gain unauthorised administrative rights.
        - Correlate data with other logs or alerts from endpoint security tools (e.g., antivirus, EDR) for any signs of malware or further compromise.
    - Tools: SIEM, Endpoint Detection and Response (EDR), Log Analysis Tools.
- Mitigation:
    - Action: If the unauthorised access is confirmed, take immediate mitigation actions to limit further damage.
    - Step-by-Step:
        - Disable the user's account to prevent further access to sensitive systems or data.
        - Audit all user actions to review what data or systems were accessed and determine if any data was exfiltrated or altered.
        - Forensically capture relevant system and access logs to maintain evidence for further investigation or legal purposes.
        - Conduct a user activity review to confirm if other colleagues are involved or if this is an isolated incident.
    - Tools: IAM (Identity and Access Management), Network Monitoring Tools, Forensic Tools.

12.2 DDoS Attack Simulation

Objective: To simulate a Distributed Denial-of-Service (DDoS) attack, where attackers attempt to overwhelm a target system or network with massive volumes of traffic to disrupt services.

1. **Trigger:**
    - The firewall or traffic monitoring systems generate alerts indicating a sudden surge in traffic or abnormal network activity that could indicate a DDoS attack.
    - This may include a large number of requests coming from multiple source IPs targeting a specific service (e.g., a web application, DNS service or database).
2. **SOC Workflow:**
    - L1 Analyst (Detection):
        - Action: The L1 analyst receives an alert about a traffic spike or potential DDoS attack from the firewall or load balancer.
        - Step-by-Step:
            - Examine the traffic sources to identify patterns that match DDoS attack behaviors, such as floods of requests or spikes in traffic volume targeting a specific IP.
            - Correlate traffic spikes with known maintenance windows, scheduled events or business hours to rule out normal spikes in legitimate traffic.
            - Review the alert thresholds in the firewall or WAF (Web Application Firewall) to ensure they are appropriately set and to assess the severity of the anomaly.
        - Tools: Firewall, SIEM, Network Traffic Monitoring Tools (e.g., Wireshark, NetFlow).
    - L2 Analyst (Investigation):
        - Action: If the L1 analyst determines that the traffic spike is suspicious, the L2 analyst takes over to confirm if it is a DDoS attack or a legitimate issue (e.g., a surge in demand or traffic).
        - Step-by-Step:

- Analyse the IP addresses to determine if the traffic is coming from a distributed set of locations (typical of DDoS) or if it’s more localised.
- Use geo-location tools to check if the traffic is coming from high-risk regions or IP addresses known to have been involved in previous attacks.
- Look for patterns such as SYN floods, UDP floods or HTTP request floods that are common in different types of DDoS attacks.

- Tools: DDoS Protection Services (e.g., Cloudflare, Akamai), Traffic Analysis Tools, WAF.

- Mitigation:
  - Action: If the attack is confirmed to be a DDoS, the mitigation process begins to limit its impact on services.
  - Step-by-Step:
    - Activate rate-limiting and traffic filtering on the firewall or WAF to block malicious traffic.
    - Geo-block or block IP ranges identified as the source of the attack.
    - Implement traffic diversion by redirecting traffic through DDoS mitigation services (e.g., Cloudflare, AWS Shield, Akamai) to absorb excess traffic.
    - Alert stakeholders about the attack and potential impacts on services and maintain ongoing communication with the Incident Response Team (IRT).
  - Tools: Web Application Firewall (WAF), DDoS Mitigation Services, Rate-Limiting Tools.
- Post-Incident Review:
  - After the attack is mitigated, conduct a post-mortem to review the effectiveness of the response and to identify areas for improvement.
  - Update the DDoS mitigation playbook based on any lessons learned to better respond to future attacks.

13. EXAMPLE SIMULATION: LATERAL MOVEMENT DETECTION

Lateral movement is a critical tactic employed by attackers after they gain initial access to a network. Detecting and responding to lateral movement quickly is key to stopping a breach before it escalates further. Below is a detailed breakdown of how to handle an alert for lateral movement:

1. Trigger: SIEM Generates an Alert for Anomalous Lateral Movement

Lateral movement involves the attacker moving from one machine or network segment to another within the compromised network, typically using stolen credentials. The SIEM (Security Information and Event Management) system will generate an alert when unusual behavior is detected, such as:

- Unusual login patterns (e.g., a user logging into multiple systems in quick succession).
- Suspicious network traffic (e.g., RDP or SMB traffic appearing between devices where there's no legitimate need).
- Elevated privileges used on systems they typically don't access.

Alert Example:

- **Alert ID:** 12345
- **Severity:** High
- **Description:** Unusual SMB traffic between user 'Admin1' and several unmonitored workstations.
- **Time Detected:** 10:15 AM
- **IP Addresses:** Source: 192.168.1.105, Destination: 192.168.1.210, 192.168.1.215, etc.

2. L1 Action: Initial Investigation and Escalation

L1 Analysts are responsible for the first level of response and usually handle the initial analysis of alerts.

L1 Analyst Actions:

1. **Correlate Logs:**
    - Review event logs, such as Windows Security logs, to verify whether the source and destination of the lateral movement are valid.

    - Check for unusual patterns like unauthorised access to critical systems (e.g., an Admin account accessing non-admin workstations).
    - Look at network logs for signs of abnormal protocols used (RDP, SMB, etc.) between hosts that are normally not interacting.

2. **Alert Verification:**
    - Confirm the anomalous nature of the activity. Check the login times, account activity and affected systems.
    - Examine related alerts (e.g., failed login attempts before successful lateral movement).

3. **Escalate to L2:**
    - If the activity is deemed suspicious but requires further technical investigation, escalate the alert to an L2 Analyst.
    - Provide L2 Analysts with the correlated log data, including affected systems, user accounts and timeframes.

Example Output to L2 Analyst:

- Alert Summary: Admin1 using SMB to connect to multiple workstations. No prior access history between Admin1 and these systems.
- Recommendation: Further investigation needed to verify if credentials are compromised.

3. L2 Action: In-Depth Investigation and Compromise Identification

L2 Analysts are skilled in investigating more complex security incidents and use advanced tools to trace the root cause of the attack.

L2 Analyst Actions:

1. **Packet Analysis Using Wireshark or Zeek:**
    - Capture and analyse network traffic using tools like Wireshark or Zeek (formerly known as Bro). This helps identify any malicious or abnormal network activity related to lateral movement.
    - Look for tell-tale signs of tools like PsExec, Mimikatz or SMB/NetSession being used to propagate through the network.

   - Investigate communication between compromised endpoints and check for any abnormal data exfiltration or unusual remote access attempts.

2. **Identify Compromised Credentials:**
   - Correlate the lateral movement event with any signs of credential theft or misuse. Review logs for login events indicating the use of stolen credentials, such as failed login attempts followed by successful logins to other systems.
   - Use tools like Mimikatz or other credential dumping tools that attackers often use to escalate privileges and access other systems in the network.
   - Check if any administrative accounts are involved and determine if they've been exploited for movement.

3. **Escalate to L3:**
   - If the attack is confirmed to be part of a larger compromise and lateral movement has already spread across several systems, escalate the case to L3 for more advanced remediation.

Example Output to L3 Analyst:

- Analysis Summary: Detected use of PsExec tool for remote execution across several endpoints. SMB traffic suggests lateral movement with possible credential dumping.
- Recommendation: Immediate containment required for affected systems.

4. L3 Action: Containment and Eradication

L3 Analysts are responsible for taking decisive actions to contain and remediate security incidents. Their role includes isolating affected systems, applying containment strategies and restoring systems to a secure state.

L3 Analyst Actions:

1. **Isolate Affected Machines:**
   - Disconnect the compromised systems from the network to prevent further spread of the attacker's presence.
   - Identify the specific endpoints affected by lateral movement (e.g., workstations, servers) and isolate them from critical systems.
   - Ensure no other systems are infected by verifying logs from network traffic analysis and endpoint security tools.

2. **Apply Containment Actions:**
    - **Block IPs and Domains:** Use firewalls or network access control (NAC) tools to block traffic from suspicious IP addresses associated with the attack.
    - **Disable User Accounts:** Disable the accounts used in the lateral movement, especially if compromised credentials are identified (e.g., Admin1's account). Force password resets if necessary.
    - **Block Malicious Tools:** Use endpoint protection solutions to block or remove tools like Mimikatz or PsExec if identified on systems.
3. **Initial Root Cause Analysis (RCA):**
    - Begin gathering evidence for further investigation into how the attacker initially gained access to the network.
    - Check logs and network traffic for the first signs of compromise and follow the chain of events that led to lateral movement.
4. **Recover and Restore:**
    - Start restoring systems from clean backups once containment actions are implemented.
    - Re-image any infected systems and ensure no remnants of malicious software or tools remain.

Example Output to Management:

- Containment Summary: Affected machines have been isolated and accounts disabled. Attack vectors identified as SMB exploitation and credential dumping via Mimikatz.
- Next Steps: Full forensic investigation and root cause analysis to be conducted; systems will be restored after remediation.

Key Tools Used in the Simulation:

- SIEM (Splunk, QRadar or others): To correlate and detect lateral movement patterns across multiple devices.
- Wireshark/Zeek: For packet-level analysis to identify suspicious traffic and tool usage.
- Endpoint Protection: To block and remediate compromised systems.

- Network Firewalls: To isolate or block malicious traffic.

Outcome and Metrics:

- Detection Time: Measure how long it takes from the initial alert to the detection of the lateral movement.
- Containment Time: Measure how quickly the SOC can isolate compromised systems and prevent further lateral movement.
- RCA Completion: Evaluate the SOC's ability to determine the root cause of the lateral movement and identify how attackers gained access initially.