CYBERSECURITY ANALYST L1 TRAINING WITH EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

INTRODUCTION

1. UNDERSTANDING THE SOC ENVIRONMENT

Objective: Familiarise with the SOC structure, tools and responsibilities of an L1 Analyst.

Scenario: You have just joined the SOC team at "Manchester United." Your manager has assigned you to learn about the environment.

SOC Structure:

- SOC operates 24/7 in shifts.
- Teams: L1, L2, Incident Response (IR), Threat Hunting.
- Key Tools: SIEM, EDR, Firewall Logs, Vulnerability Management Tools.

Task:

- **Map Tools to Functions:** Identify which tools are used for monitoring, log collection and response.
- **Document Escalation Workflow:** For example, suspicious alerts are escalated from L1 to L2 after triaging.

2. NETWORK AND IT BASICS

Objective: Understand basic network concepts essential for analysing cybersecurity alerts.

Scenario: An employee reports that their system is "slow," and your manager suspects network issues.

Supporting Data:

- IP Address: 10.10.1.15
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.1.1
- Ping Results: 100ms to 10.10.1.1.

Tasks:

- Calculate the network range from the given subnet mask.
- Use ping and traceroute commands to simulate troubleshooting.
- Hypothesize whether the issue could be internal or external.

3. LOG ANALYSIS BASICS

Objective: Learn to interpret and filter raw logs.

Scenario: Your SIEM has flagged the following logs for review:

```
Nov 26 08:15:01 Firewall: Outbound traffic detected from 192.168.1.10 to 8.8.8.8 on port 53.

Nov 26 08:15:02 Endpoint: Login success - User: "dsmith" from 192.168.1.10.

Nov 26 08:15:05 Firewall: Suspicious outbound traffic to 185.200.120.10 on port 443.
```

Tasks:

- Identify suspicious activity (unexpected IPs or ports).
- Flag logs with possible Indicators of Compromise (IoCs).
- Document your findings.

4. SIEM TOOL BASICS

Objective: Use the SIEM tool to monitor and triage alerts.

Scenario: Your SIEM displays the following alert:

- **Alert Name:** Phishing Email Activity.
- **Severity:** High.
- **Details:** A user clicked a link from an email, leading to a flagged domain: malicious-site.com.

Tasks:

- Query logs to find all events associated with malicious-site.com.
- Identify the user who clicked the link and any related IP traffic.
- Update the incident case in the SIEM.

5. INCIDENT PRIORITISATION AND ESCALATION

Objective: Learn how to prioritise incidents and escalate appropriately.

Scenario: You receive two alerts:

- **Alert 1:** Brute-force attempt on an admin account (Severity: High).
- **Alert 2:** Malware detected on an endpoint (Severity: Medium).

Tasks:

- Prioritise the alerts based on their potential impact.
- Write an escalation report for the high-severity alert, detailing the affected system, time and recommended actions.

6. THREAT INTELLIGENCE INTEGRATION

Objective: Use OSINT tools to validate potential threats.

Scenario: You are investigating an outbound connection to IP 45.67.89.101, flagged as suspicious.

Tasks:

- Use tools like VirusTotal or AbuseIPDB to check the reputation of 45.67.89.101.
- Investigate related domains or URLs linked to this IP.
- Correlate findings with internal logs to confirm whether the IP is part of a known attack.

7. REPORTING AND COMMUNICATION

Objective: Write a clear and actionable incident report.

Scenario: Based on the previous scenario.

Tasks:

- Draft a final incident report for the SOC Manager.

SIMULATED TRAINING

TRAINING 1: UNDERSTANDING THE SOC ENVIRONMENT

Scenario: Welcome to Manchester United SOC

You have joined "Manchester United" as an L1 SOC Analyst. Your onboarding tasks are to:

1. Understand the SOC's structure.
2. Map tools to their functions.
3. Document the escalation workflow.

To achieve this, your manager has provided a dataset and mock incident examples.

SOC Structure Overview

1. Teams and Roles:

- **L1 Analysts (You):**
    - Monitor SIEM dashboards.
    - Investigate alerts and perform triage.
    - Escalate unresolved or complex incidents.
- **L2 Analysts:**
    - Deep-dive into escalated incidents.
    - Perform root-cause analysis.
    - Develop response playbooks.
- **Incident Response (IR):**
    - Respond to high-severity incidents.
    - Contain and remediate active threats.
- **Threat Hunters:**
    - Proactively search for advanced threats.

- Analyse behaviour patterns and attack surfaces.

Tools and Data

Key Tools

1. **SIEM (Splunk):**
    - Centralised platform for log aggregation and alert generation.
    - Example Logs:

```
Nov 26 10:00:01 WIN-SRV-01: Login success by user "admin".
Nov 26 10:05:15 FW-Gateway: Outbound traffic to 45.67.89.101 flagged as malicious.
```

2. **EDR (Endpoint Detection and Response):**
    - Monitors endpoint activity (laptops, servers).
    - Example Alert:

```
Nov 26 10:10:45 WIN-ENDPOINT-02: Suspicious process "malware.exe" executed by user "izzmier".
```

3. **Firewall Logs (Palo Alto):**
    - Tracks network activity and blocks malicious traffic.
    - Example Logs:

```
Nov 26 10:15:30 FW-Gateway: Blocked inbound traffic from IP "203.0.113.45" on port 3389 (RDP).
```

4. **Vulnerability Management Tools (Nessus):**
    - Identifies outdated or vulnerable systems.
    - Example Scan Results:

```
Nov 26 10:20:00 WIN-SRV-03: Detected CVE-2024-12345 (Critical). Patch missing.
```

Task 1: Map Tools to Functions

Using the provided data, map the tools to their SOC functions.

Tool	Function	Example Data
SIEM	Aggregates logs, detects anomalies, and generates alerts.	Login and network traffic logs.
EDR	Tracks endpoint activity, flags malicious processes.	Suspicious process "malware.exe" flagged.
Firewall Logs	Monitors network connections, blocks malicious IPs.	Inbound traffic blocked from "203.0.113.45".
Vulnerability Management	Scans for vulnerabilities and missing patches.	CVE-2024-12345 detected on WIN-SRV-03.

Task 2: Document the Escalation Workflow

Based on a simulated incident, create an escalation process.

Scenario: The SIEM flagged outbound traffic from an endpoint (192.168.1.10) to a malicious IP (45.67.89.101).

1. **L1 Analyst Actions (You):**
   - Investigate the alert in SIEM.
   - Query logs for related activity:

Query: source_ip="192.168.1.10" OR dest_ip="45.67.89.101".

Results:

- Nov 26 10:30:00: Connection established from 192.168.1.10 to 45.67.89.101.

- Nov 26 10:31:15: Download initiated from 45.67.89.101 to 192.168.1.10.

   - Use EDR to confirm endpoint behaviour:

EDR: Malicious process "trojan.exe" detected on 192.168.1.10.

   - Document findings:

Case Update: Malicious outbound connection and process detected. Escalating to L2 for further action.

2. **L2 Analyst Actions:**
   - Analyse the process execution path.

  - Identify the malware’s persistence mechanisms.

3. **IR Team Actions:**
   - Contain the endpoint (isolate from the network).
   - Perform remediation (remove malware, patch vulnerabilities).

Sample Escalation Workflow

Step 1: Alert Generated in SIEM.

- Source: SIEM Alert - Outbound traffic to malicious IP.
- Initial Triage: Confirmed by L1 Analyst.

Step 2: Escalate to L2 Analyst.

- Details: Malicious process detected (trojan.exe).
- Request: Deep analysis and guidance on next steps.

Step 3: Escalate to IR Team (if necessary).

- Details: Malware confirmed, active communication with Command & Control (C2).
- Request: Isolate endpoint and perform remediation.

Step 4: Document Incident and Close Case.

- L1 Updates: Alert details, initial triage findings.
- L2 Updates: Root cause analysis.
- IR Updates: Containment and remediation steps.

TRAINING 2: NETWORK AND IT BASICS

Objective

Understand foundational network concepts and apply them to analyse and troubleshoot cybersecurity issues.

Scenario: Investigating Network Issues at Manchester United

You receive a report from an employee at IP 192.168.1.10 that their system is slow and experiencing connectivity issues. Your manager suspects it could be a network-related problem.

To troubleshoot, you are provided with some simulated data.

Key Concepts to Know Before Proceeding

1. **IP Address and Subnetting:**
    - IP Address: Identifies devices on a network (192.168.1.10).
    - Subnet Mask: Defines the network and host portions of an IP (255.255.255.0 means the network is 192.168.1.0/24).
2. **Gateway:**
    - Acts as the access point for devices to communicate with external networks.
3. **Network Troubleshooting Tools:**
    - **Ping:** Tests if a device is reachable.
    - **Traceroute:** Shows the path packets take to a destination.
    - **Netstat:** Displays active connections on a system.

Data

Network Configuration of the Employee's System

Parameter	Value

IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

Additional Logs

Timestamp	**Event**
08:30:00	Outbound traffic to 8.8.8.8 (Google DNS).
08:30:05	Timeout while connecting to 10.10.10.5.
08:30:10	ARP request failed for 192.168.1.1.

Tasks and Instructions

1. Calculate the Network Range

Given the subnet mask 255.255.255.0, determine:

- **Network Address:**
- **Broadcast Address:**
- **Range of Usable IPs:**

Hint: Subnet 255.255.255.0 means the first three octets (192.168.1) represent the network, and the last octet represents hosts.

2. Investigate Connectivity Issues

Using the data provided, simulate the troubleshooting process:

1. **Ping the Gateway (192.168.1.1):**
   - **Command:** ping 192.168.1.1
   - **Expected Result:**

```
Request timed out.

ARP request failed.
```

2. **Traceroute to External IP (8.8.8.8):**

    - **Command:** traceroute 8.8.8.8
    - **Expected Output:**

```
1  * * *

2  10.10.10.5  (timeout)
```

3. **Check Local ARP Cache:**
    - **Command:** arp -a
    - **Expected Output:**

```
No ARP entry found for 192.168.1.1.
```

4. **Netstat to Identify Active Connections:**
    - **Command:** netstat -an
    - **Expected Output:**

```
Active Connections:

TCP    192.168.1.10:50437   10.10.10.5:443   SYN_SENT
```

3. Hypothesize the Issue

Based on the outputs:

- The gateway (192.168.1.1) is unreachable, indicating a potential **gateway failure** or **network misconfiguration**.
- The traceroute suggests the path fails at the internal router (10.10.10.5).
- The netstat output shows incomplete connections to external IPs.

4. Propose a Resolution Plan

- **Immediate Actions:**
    - Check if the gateway device (192.168.1.1) is powered on and functional.
    - Verify physical network connectivity (cables, switches).
- **Long-Term Recommendations:**

- Review network monitoring logs for consistent gateway failures.
- Configure a backup gateway for redundancy.

TRAINING 3: LOG ANALYSIS BASICS

Objective

Learn how to analyse and interpret logs from various sources to identify potential security incidents.

Scenario: Investigating Suspicious Activity at Manchester United

As an L1 Analyst, you've received an alert from the SIEM system indicating unusual login activity on a critical server, WEB-SRV-01. The alert shows that there was a failed login attempt from an IP address outside the normal range of corporate IPs.

You are tasked with reviewing the logs from various sources to determine if there's any malicious activity.

Key Log Sources to Understand

1. **SIEM Logs (Splunk)**:
    - Aggregates and correlates logs from various sources (servers, network devices, endpoints).
    - Example Event:

```
Nov 26 10:45:00 WEB-SRV-01: Failed login attempt from IP 203.0.113.50.

Nov 26 10:47:00 WEB-SRV-01: Failed login attempt from IP 203.0.113.50.

Nov 26 10:48:00 WEB-SRV-01: Failed login attempt from IP 203.0.113.50.
```

2. **Firewall Logs**:
    - Records network activity, including blocked or allowed connections.
    - Example Event:

```
Nov 26 10:30:00 FW-Gateway: Outbound traffic to 203.0.113.50 on port 22 allowed.

Nov 26 10:35:00 FW-Gateway: Inbound traffic from 203.0.113.50 on port 80 blocked.
```

3. **System Logs (Syslog)**:

   - Provides system events, such as logins, configuration changes, or errors.
   - Example Event:

Nov 26 10:46:00 WEB-SRV-01: User "admin" logged in from IP 203.0.113.50.

Nov 26 10:49:00 WEB-SRV-01: Failed SSH connection from IP 203.0.113.50.

4. **EDR Logs (Endpoint Detection and Response)**:
   - Tracks activity on endpoints and flags suspicious behaviour.
   - Example Event:

Nov 26 10:40:00 WIN-ENDPOINT-01: Failed attempt to execute "malware.exe" from IP 203.0.113.50.

Tasks and Instructions

1. Review the Logs for Suspicious Activity

You receive the following logs from different sources. Review them carefully to identify if there's any suspicious behaviour related to the IP 203.0.113.50.

Step 1: Review the SIEM Logs

- **Alert:**
  The SIEM flagged multiple failed login attempts from the IP address 203.0.113.50 at 10:45:00, 10:47:00, and 10:48:00. This could be an attempt to brute-force the login.

Action:
Investigate the pattern and frequency of failed login attempts. Determine if the login attempts are unusual for the time of day or outside of normal corporate IP ranges.

Step 2: Review the Firewall Logs

- **Event:**
  The firewall logs show an allowed outbound connection to 203.0.113.50 on port 22 (SSH) at 10:30:00. However, at 10:35:00, inbound traffic from the same IP on port 80 (HTTP) was blocked.

Action:
Determine why the inbound connection on port 80 was blocked and investigate if the

outbound SSH connection to 203.0.113.50 was part of a legitimate communication or a possible attack attempt.

Step 3: Review the System Logs

- **Event:**
  At 10:46:00, a user with the name admin logged into WEB-SRV-01 from IP 203.0.113.50, but there was a failed SSH connection attempt at 10:49:00 from the same IP.

Action:
Verify whether the admin login was legitimate and investigate any failed login attempts right after. Failed login attempts followed by a successful login could indicate credential stuffing or brute-force attacks.

Step 4: Review the EDR Logs

- **Event:**
  At 10:40:00, a failed attempt to execute a suspicious file, malware.exe, was detected on WIN-ENDPOINT-01originating from 203.0.113.50.

Action:
Investigate the origin of the malware file. Look for any related indicators of compromise (IoC) such as file hashes, and check if this IP address is associated with any previous incidents.

2. Identify the Attack Pattern

Based on your review of the logs, you hypothesize that the following activity may be linked to a potential attack pattern:

- **Brute-force attack on WEB-SRV-01:**
  Multiple failed login attempts within a short time frame from a single external IP, followed by a successful login from the admin account, could indicate credential stuffing or brute-force attempts. This is confirmed by the firewall logs showing outbound traffic to SSH and the subsequent failed SSH connection.
- **Malware attempt on endpoint (WIN-ENDPOINT-01):**
  The suspicious file malware.exe being flagged in the EDR logs indicates that the external IP may be attempting to deliver malware. This correlates with the SSH traffic and failed login attempts, suggesting a possible lateral movement or an attempt to establish persistence on the network.

3. Escalation Process

- **L1 Analyst Actions:**
  - Correlate all logs and confirm the malicious behaviour (failed logins, suspicious file, firewall events).
  - Document the incident and escalate to L2.
  - Create an initial incident ticket with all relevant logs and analysis.
- **L2 Analyst Actions:**
  - Deep dive into the login behaviour of the admin account (is it a known user or compromised?).
  - Investigate the malicious file malware.exe for IOCs.
  - Check if any systems were affected by malware or lateral movement attempts.
- **IR Team Actions:**
  - Contain and isolate any affected endpoints.
  - Perform malware analysis and take remediation steps.
  - Rebuild compromised accounts and systems if needed.

TRAINING 4: SIEM TOOL BASICS

Objective

Learn how to use a SIEM (Security Information and Event Management) tool to detect, investigate, and manage security events and alerts.

Scenario: Investigating Suspicious Activity Using SIEM

As an L1 Analyst, you've been tasked with reviewing security events using the company's SIEM system, **Splunk**. The system has raised an alert indicating potential malicious activity on a critical server, DB-SRV-02. The alert highlights several failed login attempts from an external IP address, followed by a successful login using a privileged account.

Your goal is to:

- Investigate the alert.
- Use Splunk's features to identify and understand the scope of the issue.
- Provide insights into the attack and take appropriate action.

Key SIEM Concepts to Understand

1. **Log Collection and Normalisation**:
    - SIEM tools collect data from various sources (servers, firewalls, network devices, endpoints).
    - The logs are normalised into a common format to make analysis easier.
2. **Alerting and Correlation**:
    - SIEM tools use correlation rules to group related events and generate alerts.
    - Example Alert:

[Alert] Suspicious Login Attempt

IP: 198.51.100.123

User: admin

Time: 2024-11-26 10:12:00

Source: DB-SRV-02

Event Type: Failed login (5 attempts)

Followed by: Successful login at 10:15:00

3. **Dashboards**:
   - Dashboards provide a graphical view of security events.
   - Example Dashboard for Splunk:
     - Shows the number of failed logins by IP address, the top users logging in, and the event frequency.
4. **Search Queries**:
   - SIEM tools allow you to search for specific events using queries (often in a language like SPL—Search Processing Language in Splunk).
   - Example SPL Query:

```
index=security_logs source="DB-SRV-02" "failed login"
```

   - This query searches for failed login events on the DB-SRV-02 server.

Tasks and Instructions

1. Investigate the Alert in Splunk

You've received an alert in Splunk indicating multiple failed login attempts followed by a successful login using the admin account from the external IP 198.51.100.123.

Step 1: Search for Failed Logins

- **Search Query in Splunk**:

```
index=security_logs source="DB-SRV-02" "failed login"
```

Action:
Run this query in Splunk to view the list of failed login attempts from the external IP 198.51.100.123.

Result:

```
Time                | Source         | User    | IP Address      | Event Type
2024-11-26 10:12:00      | DB-SRV-02       | admin   | 198.51.100.123  | Failed login (3 attempts)
2024-11-26 10:14:00      | DB-SRV-02       | admin   | 198.51.100.123  | Failed login (2 attempts)
```

Step 2: Search for Successful Login

- **Search Query in Splunk**:

```
index=security_logs source="DB-SRV-02" "successful login" user="admin"
```

Action:
Run this query to check for any successful logins by the admin account.

Result:

```
Time                | Source         | User    | IP Address      | Event Type
2024-11-26 10:15:00      | DB-SRV-02       | admin   | 198.51.100.123  | Successful login
```

Step 3: Review Login Times and Sequence

- Compare the failed login attempts and the subsequent successful login. You should notice a pattern that suggests brute-force or credential stuffing.

Analysis:

  - The external IP address 198.51.100.123 made several failed login attempts from 10:12:00 to 10:14:00.
  - Shortly after, at 10:15:00, a successful login occurred with the admin account from the same IP address.
  - This may indicate a successful login after a brute-force or credential stuffing attack.

2. Correlate Other Data Sources in SIEM

Step 1: Review Firewall Logs

- **Search Query in Splunk**:

```
index=firewall_logs src_ip="198.51.100.123"
```

Action:
Run this query to check if there were any unusual network activities or blocked traffic from the IP 198.51.100.123.

Result:

```
Time                  | Source          | Action  | Destination IP | Port

2024-11-26 10:00:00      | FW-Gateway       | Blocked | DB-SRV-02     | 22 (SSH)

2024-11-26 10:30:00      | FW-Gateway       | Allowed | DB-SRV-02     | 80 (HTTP)
```

Step 2: Check for Any Lateral Movement

- **Search Query in Splunk**:

```
index=security_logs src_ip="198.51.100.123" "lateral movement"
```

Action:
This query checks if there are any other events tied to this external IP that show signs of lateral movement within the network.

Result:
No related events found, indicating no immediate lateral movement was detected.

3. Escalation and Reporting

Step 1: Incident Documentation

- **L1 Analyst Actions**:
  - Document the failed login attempts and successful login event, correlating them with the external IP address.
  - Review any additional related events (firewall blocks, system alerts).
  - Prepare an initial analysis report for escalation.

Step 2: Escalate to L2

- **L2 Analyst Actions**:
  - Review the full timeline of events and correlate with any known threat intelligence regarding the IP 198.51.100.123.

    - Investigate if the admin account was compromised, or if other accounts were affected.
    - Run additional queries to confirm the full scope of the attack.

Step 3: IR Actions

- **Incident Response Team**:
    - Contain the compromised account if needed.
    - Reset the admin account's password and enforce stronger authentication methods.
    - Investigate the source of the external IP and determine if any data exfiltration occurred.

TRAINING 5: INCIDENT PRIORITISATION AND ESCALATION

Objective

Learn how to prioritise security incidents based on severity, impact, and risk, and understand when to escalate incidents from L1 to L2 or Incident Response (IR) teams.

Scenario: Prioritising and Escalating an Incident

As an L1 Analyst at **Manchester United.**, you receive multiple alerts from the SIEM system that require immediate attention. These alerts are tied to different systems in the environment. It is your responsibility to prioritise the incidents, determine their potential impact, and escalate them appropriately.

Your task is to:

1. Assess the severity of different security alerts.
2. Prioritise incidents based on risk and impact.
3. Decide which incidents need to be escalated to L2 or IR.
4. Document the escalation process for each incident.

Key Concepts: Incident Severity and Prioritisation

1. **Severity Levels**:
   Incidents can be categorised based on their severity:
   - **Critical**: Immediate action required; could result in data loss, breach, or system compromise.
   - **High**: Requires urgent attention but not necessarily immediate action; could impact systems or services.
   - **Medium**: Needs to be investigated but doesn't pose an immediate threat; could be a warning of potential issues.
   - **Low**: Minor incidents that may not require immediate attention.

2. **Impact and Risk Assessment**:
   Incidents should be prioritised based on:
   - **Scope**: How widespread the issue is.
   - **Impact**: What systems or services are affected.
   - **Risk**: How likely it is to cause harm or escalate into something more severe.
3. **Escalation Protocol**:
   - **L1 to L2**: If the incident requires deeper analysis or advanced technical expertise that L1 cannot provide.
   - **L1 to Incident Response (IR)**: If the incident is a confirmed or suspected compromise that requires immediate containment and remediation.

Task 1: Review the Security Alerts

You receive the following alerts in the SIEM system:

1. **Alert 1**: **Multiple failed login attempts from external IP**
   - **Severity**: High
   - **Description**: An external IP address has attempted to login multiple times to the critical DB-SRV-01 server using an admin account.
   - **Timestamp**: 2024-11-26 08:35:00
   - **IP Address**: 198.51.100.123
   - **Number of Failed Logins**: 8 attempts
   - **Account Affected**: admin
   - **Initial Actions Taken**: None yet.
2. **Alert 2**: **Ransomware Alert**
   - **Severity**: Critical
   - **Description**: A potential ransomware infection has been detected on an endpoint server, HR-SRV-03. The endpoint has been flagged for abnormal file encryption activity.
   - **Timestamp**: 2024-11-26 08:40:00

   - **Endpoint**: HR-SRV-03
   - **Malware Indicator**: Abnormal file modification and encryption
   - **Initial Actions Taken**: None yet.

3. **Alert 3**: **Suspicious Internal User Activity**
   - **Severity**: Medium
   - **Description**: An internal user, John.Doe, has accessed sensitive financial data outside of business hours.
   - **Timestamp**: 2024-11-26 09:00:00
   - **User**: John.Doe
   - **System Accessed**: Finance Database
   - **Initial Actions Taken**: Logged, waiting for investigation.

4. **Alert 4**: **Unusual Port Scanning Activity**
   - **Severity**: Low
   - **Description**: A network device has detected unusual port scanning activity from an internal device, Workstation-42, targeting various servers.
   - **Timestamp**: 2024-11-26 09:15:00
   - **Device**: Workstation-42
   - **Port Scan Target**: Multiple servers
   - **Initial Actions Taken**: Logged, monitoring.

Task 2: Prioritise and Assess the Incidents

Step 1: Incident Assessment

1. **Alert 1: Multiple Failed Login Attempts**
   - **Severity**: High
   - **Reason**: Multiple failed login attempts from an external IP, targeting a critical server (DB-SRV-01). This could indicate a brute-force attack or credential stuffing. If successful, it may lead to a data breach or system compromise.

   - **Action**:
      - Investigate further by searching for successful logins from the same IP.
      - Review the server's authentication logs for any signs of compromised accounts.
      - Block the IP if suspicious activity is confirmed.

2. **Alert 2: Ransomware Alert**
   - **Severity**: Critical
   - **Reason**: Ransomware detection on an endpoint server (HR-SRV-03). This is a high-priority incident as it can quickly escalate to affect the entire network and cause significant data loss. Immediate containment is required.
   - **Action**:
      - Disconnect HR-SRV-03 from the network.
      - Initiate malware analysis and identify the scope of the infection.
      - Escalate to Incident Response (IR) team for remediation.
3. **Alert 3: Suspicious Internal User Activity**
   - **Severity**: Medium
   - **Reason**: The internal user John.Doe accessed sensitive financial data outside of business hours. While this may be a valid action (working late), it could also be a sign of insider threat or suspicious activity.
   - **Action**:
      - Check if John.Doe has a valid reason for accessing the data at this time.
      - Investigate any recent changes in user behaviour.
      - If suspicious, escalate to L2 for a deeper investigation.
4. **Alert 4: Unusual Port Scanning Activity**
   - **Severity**: Low

  - **Reason**: Port scanning activity from an internal workstation (Workstation-42) is usually not a major threat but can indicate network reconnaissance. This could be a misconfigured device or an early sign of an internal attack.
  - **Action**:
    - Monitor the device for any other unusual activity.
    - Investigate whether the device is compromised or just misconfigured.
    - No immediate escalation unless further suspicious activity is observed.

Task 3: Escalation and Reporting

Step 1: Document Incident Details

- **Alert 1 (Failed Login Attempts)**:
  - Severity: High
  - Action Taken: Investigating. Block IP if necessary.
  - Escalation: If evidence of a successful login is found, escalate to L2 for further analysis.
- **Alert 2 (Ransomware Alert)**:
  - Severity: Critical
  - Action Taken: Disconnect endpoint from the network. Initiate malware analysis.
  - Escalation: Immediately escalate to IR team for containment and remediation.
- **Alert 3 (Suspicious Internal User Activity)**:
  - Severity: Medium
  - Action Taken: Investigating user activity. Verify if access was legitimate.
  - Escalation: Escalate to L2 if further suspicious activity is found.
- **Alert 4 (Port Scanning Activity)**:
  - Severity: Low

  - Action Taken: Monitoring. No immediate action required.
  - Escalation: No escalation unless further suspicious activity occurs.

Step 2: Escalation Process

- **L1 to L2**:
  If you are unable to fully resolve the issue or if advanced analysis is required (Alert 1 and Alert 3), escalate to L2 for deeper investigation.
- **L1 to IR**:
  For high-impact incidents such as ransomware (Alert 2), escalate immediately to the IR team for containment, investigation, and recovery.

TRAINING 6: THREAT INTELLIGENCE INTEGRATION

Objective

Learn how to integrate and use threat intelligence to enhance the detection and response to security incidents, enabling more proactive protection against emerging threats.

Scenario: Using Threat Intelligence to Detect and Respond to Emerging Threats

You are working as an L1 Analyst at **Manchester United.** and have just been introduced to integrating threat intelligence feeds into your SIEM platform. These threat feeds contain information about emerging threats, known malicious IP addresses, file hashes, and other indicators of compromise (IoCs).

In this training, you will:

1. Understand the concept of threat intelligence and how it fits into your day-to-day operations.
2. Learn how to access and integrate threat intelligence feeds into the SIEM system.
3. Use threat intelligence data to identify malicious activity in the network.
4. Follow procedures for responding to incidents based on threat intelligence indicators.

Key Concepts: Threat Intelligence

1. **Types of Threat Intelligence**:
    - **Strategic**: High-level information about current and emerging threats that can influence long-term security strategies.
    - **Tactical**: More actionable intelligence detailing attack methods, tactics, techniques, and procedures (TTPs) used by threat actors.
    - **Operational**: Intelligence about specific threats, including IoCs (IP addresses, domain names, file hashes, URLs) that are currently being observed.

  - **Technical**: Detailed information used to mitigate immediate threats, such as signatures, malware analysis reports, and IP blacklists.

2. **Threat Intelligence Feeds**:
   - Threat intelligence feeds are typically provided by external sources, such as commercial vendors, government agencies, or open-source projects.
   - These feeds are integrated into your SIEM system to automate the identification of known threats and enable proactive responses.

3. **Indicators of Compromise (IoCs)**:
   - **IP addresses**: Identifying malicious sources of attacks.
   - **File hashes**: Recognising known malware files.
   - **URLs and domains**: Detecting command-and-control servers or phishing websites.
   - **Email addresses**: Identifying phishing attempts.

4. **Threat Intelligence Platforms**:
   - Platforms like **MISP**, **OpenDXL**, and **AlienVault OTX** provide structured threat intelligence that can be integrated into SIEM and other security tools.

Task 1: Accessing and Integrating Threat Intelligence Feeds into the SIEM

Manchester United. has subscribed to a threat intelligence feed that provides real-time data on emerging threats, including known malicious IP addresses, URLs, and file hashes. As part of your training, you need to integrate this feed into your SIEM system and ensure that it works correctly.

Steps to Integrate Threat Intelligence Feed:

1. **Obtain Feed URL and Credentials**:
   You receive an API URL and API key from your threat intelligence provider. This is the first step to integrate the feed into the SIEM platform.

2. **Configure SIEM to Ingest the Feed**:
   You access the SIEM system (**Splunk**, **QRadar**, or **ArcSight**) and navigate to the threat intelligence configuration page. Here, you input the feed URL and the API key provided by the vendor.

    - **Example Feed URL**: https://threatfeed.example.com/api/v1/data
    - **API Key**: xyz12345apikey

3. **Validate Integration**:
   Once configured, verify the integration by checking if the SIEM starts receiving threat intelligence data. You should be able to see new indicators in the system.

4. **Correlating Threat Intelligence with Network Data**:
   With the threat feed integrated, the SIEM will automatically correlate the threat intelligence indicators with incoming logs and alerts. For example:
    - If a known malicious IP address from the threat feed matches one in your logs, the SIEM will flag this as a potential security incident.

Task 2: Identifying Malicious Activity Using Threat Intelligence

Now that the threat intelligence feed is integrated into the SIEM system, your next task is to identify potential threats based on this data. Your goal is to spot known threats and malicious activity early to mitigate risks.

Review of Security Alerts:

1. **Alert 1**: **Suspicious IP Address Detected**
    - **Description**: A connection from external IP 198.51.100.123 has been logged into the WebApp-SRV-02server. This IP address is flagged as malicious in the threat intelligence feed.
    - **Severity**: High
    - **Threat Intelligence Data**: IP 198.51.100.123 is associated with known phishing campaigns.

2. **Alert 2**: **File Hash Match for Malware**
    - **Description**: A suspicious file with the hash 4d4e9b70bc4e6c4d9b0f123f3a7b7cfa was detected on the Accounting-SRV-03 server. This file matches a known malware hash from the threat intelligence feed.
    - **Severity**: Critical

    - **Threat Intelligence Data**: File hash 4d4e9b70bc4e6c4d9b0f123f3a7b7cfa is associated with a ransomware variant.

3. **Alert 3**: **Phishing Domain Detected**
    - **Description**: An email link from http://securelogin.xyz was flagged as a phishing attempt. This domain is listed in the threat intelligence feed as a known phishing domain.
    - **Severity**: Medium
    - **Threat Intelligence Data**: Domain securelogin.xyz is identified in the feed as a phishing website.

Task 3: Responding to Threat Intelligence Indicators

Once the threat intelligence data is integrated and alerts are triggered, the next step is to respond effectively to these threats.

Response Steps for Each Alert:

1. **Alert 1: Suspicious IP Address Detected**
    - **Action**:
        - Verify the incoming connection from IP 198.51.100.123 and check if any data was exfiltrated or compromised.
        - Block the IP address at the firewall level.
        - Escalate to L2 for further investigation if suspicious activity is confirmed.
        - Monitor for any additional connections from this IP.
2. **Alert 2: File Hash Match for Malware**
    - **Action**:
        - Immediately quarantine the affected file on Accounting-SRV-03.
        - Disconnect the server from the network to prevent the malware from spreading.
        - Escalate the alert to the Incident Response (IR) team for malware analysis and remediation.

        - Track any other servers or workstations that may have been infected by the same malware.

3. **Alert 3: Phishing Domain Detected**
    - **Action**:
        - Investigate the email linked to the phishing domain securelogin.xyz.
        - Block access to the phishing site at the network perimeter.
        - Report the phishing attempt to the IR team and monitor if any user accounts were compromised.
        - Send an awareness alert to all employees about the phishing domain.

TRAINING 7: REPORTING AND COMMUNICATION

Objective

Learn how to effectively communicate security incidents, report findings to the relevant stakeholders, and follow incident response protocols in the SOC environment.

Scenario: Incident Reporting and Communication

You are working as an L1 Analyst at **Manchester United.** A high-priority security incident has occurred, and it's your responsibility to report it in a clear, accurate, and structured manner. Your report will need to be delivered to both technical teams (such as L2 Analysts and the Incident Response team) and non-technical stakeholders (such as management).

In this training, you will:

1. Learn the structure of incident reports.
2. Practice reporting on a security incident.
3. Understand the importance of clear and concise communication in a cybersecurity context.
4. Simulate communication with other teams, including escalation protocols.

Key Concepts: Reporting and Communication

1. **Incident Report Structure**:
   - **Title/Identifier**: A concise name for the incident ("Suspicious IP Address Infiltration").
   - **Summary**: A brief overview of the incident, what was affected, and why it is significant.
   - **Severity**: Define the severity level (Low, Medium, High, Critical) based on the impact and urgency.
   - **Timeline**: Document key events of the incident (when it was detected, escalated, actions taken).

- **Analysis**: Include technical details, such as the indicators of compromise (IoCs), methods of attack, and systems affected.
- **Response Actions**: Document the actions taken in response, such as IP blocking, server isolation, or patching.
- **Impact**: Describe the potential or actual impact on the business, systems, and users.
- **Lessons Learned**: Include recommendations for preventing similar incidents in the future.

2. **Escalation Protocols**:
   - **Escalation Criteria**: Understand when and how to escalate incidents to L2, Incident Response, or management. For example, if an incident is identified as critical, you should escalate it immediately.
   - **Clear and Concise Communication**: Use clear, non-technical language when communicating with management. Be ready to explain the significance of an incident in terms of business impact.
3. **Communication with Stakeholders**:
   - **Internal Communication**: Communicate effectively with L2 Analysts, Incident Response teams, and other technical staff. Provide them with the necessary details to carry out their tasks.
   - **Management Communication**: When communicating with management, focus on the business impact, the urgency of the issue, and the mitigation efforts. Avoid too much technical jargon.
   - **Post-Incident Briefings**: After the incident is resolved, conduct a post-mortem briefing to identify what went well, what didn't, and areas for improvement.

Task 1: Incident Report Example

You have detected a security incident based on an alert that indicates a known malicious IP address from the threat intelligence feed. This IP address has attempted to connect to one of your internal web servers. You now need to write a report detailing the incident.

Incident Report Example:

Title: Suspicious IP Address Detected – Potential Phishing Attack

- **Summary**:
  At **10:15 AM**, a connection attempt was made from IP address **198.51.100.123** to the internal server **WebApp-SRV-02**. This IP address is flagged as part of a known phishing campaign in the threat intelligence feed.
- **Severity**:
  High. The malicious IP is associated with phishing attempts, and the target server handles sensitive user information.
- **Timeline**:
  - **10:15 AM**: First detection of suspicious connection from IP address **198.51.100.123**.
  - **10:20 AM**: Alert escalated to L2 Analyst for further investigation.
  - **10:30 AM**: The IP address was blocked by the firewall.
  - **10:45 AM**: A full system scan was initiated on **WebApp-SRV-02**.
  - **11:00 AM**: Incident Response team notified for a deeper investigation.
- **Analysis**:
  - **Indicators of Compromise**:
    - IP address **198.51.100.123** is flagged in the threat intelligence feed.
    - The IP address was attempting to access login pages on the web server.
  - **Method of Attack**: The attacker may have been attempting a phishing or credential-stuffing attack using this IP.
- **Response Actions**:
  - The malicious IP was immediately blocked at the network perimeter by the firewall.
  - The server **WebApp-SRV-02** was isolated from the network for further inspection.
  - The Incident Response team was notified and has initiated additional investigation.

- **Impact**:
  - **Potential Impact**: If successful, this attack could have compromised user login credentials on the internal web application. At the time of the detection, no successful login attempts have been recorded.
  - **Business Impact**: The potential compromise of user credentials could lead to unauthorized access to sensitive data, damaging the company's reputation and possibly breaching compliance requirements.
- **Lessons Learned**:
  - **Recommendation**: Implement stronger multi-factor authentication (MFA) across all web applications.
  - **Recommendation**: Ensure that all firewalls and intrusion prevention systems (IPS) are configured to block known malicious IP addresses in real time.

Task 2: Communication with Teams

In addition to the incident report, you need to communicate with other teams to ensure a timely and effective response.

1. **Communicating with L2 Analysts**:
   - You send an email to L2 Analysts with a detailed summary of the incident, requesting them to look deeper into the connection logs for any signs of exploitation or further compromise.
   - **Example email**:
     "Hello L2 Team,
     We have detected suspicious activity involving IP address 198.51.100.123, which is flagged in the threat intelligence feed. This IP attempted to connect to our internal web server **WebApp-SRV-02**. Please investigate the connection logs to check for any signs of exploitation. The firewall has already blocked the IP, but we need to ensure there was no compromise.
     Regards, [Your Name]"
2. **Escalating to the Incident Response Team**:

- You escalate the alert to the Incident Response (IR) team, providing them with all necessary technical details and asking them to perform a full investigation and root cause analysis.
- **Example email**:
  "Hello IR Team,
  We have an ongoing investigation involving a suspicious IP (198.51.100.123) that attempted to access our internal web server. The IP has been blocked, but we would like your team to conduct a deeper analysis. Please confirm if any data has been exfiltrated or if further action is required. Regards, [Your Name]"

3. **Communicating with Management**:
   - For non-technical stakeholders, you prepare a concise summary of the incident, focusing on the potential business impact and the actions being taken to mitigate it.
   - **Example email**:
     "Hello Management Team,
     We have detected a high-severity security incident involving a malicious IP address that attempted to connect to one of our internal servers. The IP has been blocked, and we are conducting further investigation. At this point, no data breach has been confirmed, but we are taking proactive steps to ensure no compromise has occurred. We will update you with further details as the situation develops. Regards, [Your Name]"