ROLES AND RESPONSIBILITIES OF L1, L2 AND L3 CYBERSECURITY ANALYSTS WITH SCENARIO EXAMPLE

BY IZZMIER IZZUDDIN

TABLE OF CONTENTS

ROLES AND RESPONSIBILITIES OF L1, L2 AND L3 CYBERSECURITY ANALYSTS 3

L1 Cybersecurity Analyst (Triage and Basic Analysis) 3
L2 Cybersecurity Analyst (Detailed Analysis & Investigation) 4
L3 Cybersecurity Analyst (Expert-Level Threat Intelligence & Strategic Response) 5

COLLABORATION AND WORKFLOW BETWEEN L1, L2 AND L3 CYBERSECURITY ANALYSTS 8

SCENARIO EXAMPLE OF WORK COLLABORATIVELY TO ANALYSE, INVESTIGATE AND RESPOND TO AN ALERT 9

SCENARIO 1: SUSPICIOUS LOGIN ATTEMPT DETECTED 9
SCENARIO 2: MALWARE DETECTED ON END-USER SYSTEM.....14
SCENARIO 3: UNUSUAL LOGIN ATTEMPT DETECTED 19
SCENARIO 4: SUSPICIOUS FILE EXECUTION DETECTED 24
SCENARIO 5: BRUTE FORCE LOGIN ATTEMPT DETECTED 29
SCENARIO 6: PHISHING EMAIL WITH MALICIOUS ATTACHMENT.....34
SCENARIO 7: SUSPICIOUS INTERNAL FILE TRANSFER DETECTED 39
SCENARIO 8: PHISHING EMAIL LEADING TO MALWARE DOWNLOAD 44

ROLES AND RESPONSIBILITIES OF L1, L2 AND L3 CYBERSECURITY ANALYSTS

The role of Cybersecurity Analyst in Security Operations Center (SOC) is divided into three levels (L1, L2 and L3). Each level has distinct responsibilities based on the complexity and severity of security incidents, ensuring an efficient workflow that allows for quick detection, analysis and response. Below is a breakdown of the tasks each analyst performs at each level, from L1 (entry-level) to L3 (advanced-level).

L1 Cybersecurity Analyst (Triage and Basic Analysis)

Primary Focus:

- **Initial Alert Detection & Triage**
- **Basic Incident Validation and Categorisation**

Responsibilities:

1. **Alert Monitoring:**
    - L1 analysts are responsible for monitoring security alerts generated by tools like SIEM (Security Information and Event Management) systems, firewalls, endpoint protection systems and other security tools.
    - They ensure that alerts are reviewed in real-time and properly logged.
2. **Initial Triage of Alerts:**
    - L1 analysts perform a first-pass review of incoming alerts to determine whether the alert represents a legitimate security incident or if it is a false positive.
    - They categorise the severity of the alert (low, medium, high) based on pre-defined thresholds.
3. **Incident Documentation:**
    - They document all relevant details about the security incident, including timestamps, affected systems, users and a description of the behavior that triggered the alert.
    - Basic details such as the source of the alert and affected assets are recorded for later review.
4. **Initial Analysis:**

- L1 analysts will often perform basic investigative actions, such as checking logs or reviewing traffic patterns to understand if there is any immediate threat.
- If the investigation shows the alert is genuine, they escalate it to L2 for further analysis.

5. **Escalation:**
    - When L1 analysts determine an alert requires further in-depth analysis or investigation, they escalate it to L2 analysts for a deeper investigation.

Example of L1 Tasks:

- Monitoring SIEM for unusual login attempts or anomalous traffic.
- Checking for phishing emails or malicious attachments.
- Identifying initial signs of a potential malware infection on an endpoint.
- Triage and escalate suspicious activities to L2 when unsure.

L2 Cybersecurity Analyst (Detailed Analysis & Investigation)

Primary Focus:

- **In-depth Analysis and Investigation**
- **Threat Identification and Containment**

Responsibilities:

1. **Detailed Incident Analysis:**
    - L2 analysts take over incidents that have been escalated by L1 analysts. They conduct detailed analysis to determine the nature and scope of the threat.
    - They work with advanced tools and methods to analyse log files, network traffic and endpoint activity to understand the threat and its potential impact.
2. **Root Cause Analysis:**
    - L2 analysts are responsible for identifying the root cause of the alert. They investigate whether it was caused by a phishing attempt, malware infection, vulnerability exploitation, insider threat, etc.
    - They perform deeper forensics, including reviewing system configurations, authentication logs and event sequences, to track the attack path.

3. **Containment:**
    - If the incident is confirmed to be a valid threat, L2 analysts work to contain the attack. This may involve isolating compromised endpoints, blocking malicious IPs, disabling accounts or applying temporary mitigations to reduce further damage.
    - In cases of malware infections, L2 may initiate processes to remove the malware from the affected systems.
4. **Coordination with L3:**
    - L2 analysts may require input from L3 for high-level threat intelligence, advanced investigation methods or if the attack appears to be a complex or evolving threat.
    - They document their findings and provide L3 analysts with the data necessary for further analysis.

Example of L2 Tasks:

- Investigating network traffic or file activity for suspicious patterns or unauthorised access.
- Running virus and malware scans on affected endpoints.
- Reviewing file hashes, network indicators and correlating this data with threat intelligence feeds.
- Escalating high-severity incidents or complex attacks to L3 for further intelligence and countermeasures.

L3 Cybersecurity Analyst (Expert-Level Threat Intelligence & Strategic Response)

Primary Focus:

- **Advanced Threat Intelligence and Incident Response**
- **Strategic Remediation and Prevention**

Responsibilities:

1. **Advanced Threat Hunting & Intelligence:**
    - L3 analysts are the most experienced in identifying and mitigating advanced threats, such as targeted attacks, APTs (Advanced Persistent Threats) and zero-day exploits.

- They have a deep understanding of threat actor tactics, techniques and procedures (TTPs) and often rely on advanced threat intelligence feeds, external research and collaboration with global CERTs (Computer Emergency Response Teams) and other intelligence-sharing organisations.
- L3 analysts correlate data from multiple sources, including external threat intelligence and determine whether the incident is part of a broader campaign.

2. **Threat Actor Attribution:**
    - L3 analysts provide detailed insight into the nature of the threat by attributing it to known threat actors or attack groups, using open-source intelligence (OSINT), commercial threat feeds and internal historical data.
    - They often rely on information from cyber threat intelligence (CTI) sources to identify and understand the motivations, tools and techniques used by attackers.
3. **Strategic Response and Countermeasures:**
    - Once the threat is identified, L3 analysts provide recommendations for long-term countermeasures and preventive actions to avoid future incidents. This includes patching vulnerable systems, improving security controls or enhancing detection mechanisms.
    - They may also help define incident response (IR) plans and recovery strategies, ensuring proper communication with stakeholders and ensuring compliance with regulations (GDPR, HIPAA).
4. **Post-Incident Review:**
    - After an incident is contained and mitigated, L3 analysts lead post-mortem reviews to identify lessons learned, improve response procedures and help strengthen defenses.
    - They generate comprehensive incident reports for senior management and clients, summarising findings, actions taken and any recommendations for improving security posture.

Example of L3 Tasks:

- Analysing advanced malware (fileless or memory-based) or sophisticated exploits.
- Correlating data with global threat intelligence sources to determine if the incident is related to a broader attack campaign.

- Providing recommendations to enhance detection capabilities and prevent future similar incidents.
- Supporting executive leadership and clients with high-level technical and strategic recommendations.

COLLABORATION AND WORKFLOW BETWEEN L1, L2 and L3 CYBERSECURITY ANALYSTS

- **L1 Analyst:**
    - **Role:** First responder to security incidents. L1 analysts detect, validate and categorise alerts and escalate more complex incidents to L2 for further investigation.
    - **Escalation to L2:** If L1 analysts are unsure about an alert or if an incident seems to require further analysis, it is passed to L2 for more detailed investigation.
- **L2 Analyst:**
    - **Role:** Conducts in-depth analysis of validated alerts, investigates incidents to find the root cause and contains threats. If the incident involves advanced techniques or external threat intelligence, they escalate to L3.
    - **Escalation to L3:** When an attack is particularly sophisticated or linked to known threat actors or if further intelligence is needed, L2 analysts consult L3 for expert analysis and strategic guidance.
- **L3 Analyst:**
    - **Role:** Provides advanced expertise, correlates incidents with global threat intelligence and offers strategic countermeasures. L3 is involved in complex investigations and guides the entire team on advanced response strategies.
    - **Escalation to Senior Management/Clients:** L3 analysts generate reports and guide clients and senior management on the long-term impact and steps to mitigate risks.

SCENARIO EXAMPLE OF WORK COLLABORATIVELY TO ANALYSE, INVESTIGATE AND RESPOND TO AN ALERT

SCENARIO 1: SUSPICIOUS LOGIN ATTEMPT DETECTED

Alert Details in SIEM:

- **Alert Name:** Multiple Failed Logins Followed by Successful Login
- **Severity:** High
- **Source:** SIEM (via Windows Event Logs and VPN Logs)
- **Time:** 2024-11-18 01:15:43 UTC
- **Source IP:** 203.0.113.200 (External)
- **Host Name:** DC01 (Domain Controller)
- **User:** admin@manchesterunited.com

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. **Review the SIEM Alert Details:**
    - Analyse the event description, timestamps and related logs.
2. **Validate Alert Severity:**
    - Identify whether the alert is a false positive or requires escalation.
3. **Correlate Logs:**
    - Check for related logs to understand the scope of the issue.

L1 Workflow:

1. **Step 1: Analyse SIEM Alert:**

- Alert shows multiple failed login attempts (Event ID 4625).

- Followed by a successful login from the same external IP (Event ID 4624).

2. **Step 2: Check Logs for Context:**

- **Login Failure Logs:**

2024-11-18 01:10:43 UTC | Event ID: 4625 | User: admin@manchesterunited.com | Source IP: 203.0.113.200 | Reason: Incorrect Password

- **Successful Login Logs:**

2024-11-18 01:15:43 UTC | Event ID: 4624 | User: admin@manchesterunited.com | Source IP: 203.0.113.200

3. **Step 3: Validate Severity:**
    - Source IP is from a suspicious external location not typically associated with the user (Nigeria).
    - User account is an admin account—high risk.
4. **Step 4: Escalate to L2 Analyst:**

Suspicious login activity detected for admin@manchesterunited.com.

Multiple failed attempts followed by a successful login from an external IP (203.0.113.200).

User is privileged; potential brute force attack. Escalating to L2 for deeper analysis.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. **Deep Dive Analysis:**
    - Correlate additional logs from SIEM, VPN logs and endpoint tools.
    - Check for indicators of lateral movement or privilege escalation.
2. **Determine the Root Cause:**
    - Investigate if credentials were compromised.
3. **Provide Remediation Recommendations.**

L2 Workflow:

1. **Step 1: Gather Related Logs:**
    - **VPN Logs:**

2024-11-18 01:15:43 UTC | Successful VPN Login | User: admin@manchesterunited.com | Source IP: 203.0.113.200

- **Windows Event Logs (File Access):**

2024-11-18 01:16:00 UTC | User: admin@manchesterunited.com | File Access: C:\Confidential\SensitiveData.xlsx

2. **Step 2: Analyse Patterns:**
    - **Behavioral Analysis:**
        - User logged in from an IP not associated with past behavior.
        - Immediately accessed sensitive files.
    - **Credential Compromise Indicators:**
        - Failed logins indicate potential brute force or password spraying.
3. **Step 3: Validate Threat:**
    - External IP (203.0.113.200) is listed in threat intelligence feeds as associated with known brute force campaigns.
4. **Step 4: Recommend Actions:**

- Block IP 203.0.113.200 at the firewall.

- Temporarily disable admin@manchesterunited.com account.

- Notify client to enforce password reset for all admin users.

- Escalate to L3 for deeper threat intelligence and IOC analysis.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. **Enrich Incident with CTI:**
    - Identify threat actor or campaign associated with the external IP.
    - Provide Indicators of Compromise (IOCs) for client defence.
2. **Advise on Long-Term Mitigation:**
    - Recommend strategic actions based on CTI findings.

L3 Workflow:

1. **Step 1: CTI Enrichment:**
    - Investigate IP 203.0.113.200 in threat intelligence databases:

IP: 203.0.113.200

Associated Threat Actor: "BlackHydra" Group

Known Activity: Brute force attacks targeting privileged accounts.

- Retrieve related IOCs:

IPs: 203.0.113.200, 203.0.113.201

Domains: brute-force-attacker.com

Hashes: abc123def456...

2. **Step 2: Threat Hunt for Broader Scope:**
    - Search for additional logs indicating communication with 203.0.113.200 across other client systems (none found).
3. **Step 3: Provide Strategic Insights:**

This incident is linked to the BlackHydra group, known for targeting admin accounts via brute force.

Recommend adding IOCs to the client's SIEM and network devices.

Suggest implementing MFA for all admin accounts and restricting access based on geolocation.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A potential credential compromise for admin@manchesterunited.com was detected. The account logged in from a suspicious external IP (203.0.113.200) after multiple failed attempts. Following the login, sensitive files were accessed.

Incident Details:

- Source IP: 203.0.113.200 (linked to BlackHydra brute force campaigns).
- Action Taken: IP blocked, account disabled and client notified to enforce password reset.
- Recommended Mitigation:
  - Enable MFA for all privileged accounts.
  - Add IOCs to network defence systems:
    - IPs: 203.0.113.200, 203.0.113.201
    - Domains: brute-force-attacker.com

Next Steps:

We recommend reviewing user activity for anomalies, enabling geolocation-based restrictions and conducting phishing awareness training for privileged users.

SCENARIO 2: MALWARE DETECTED ON END-USER SYSTEM

Alert Details in SIEM:

- **Alert Name:** Suspicious Executable Download Detected
- **Severity:** Critical
- **Source:** SIEM (via Endpoint Detection & Response - EDR)
- **Time:** 2024-11-18 10:25:32 UTC
- **Host:** USER-PC (Employee Workstation)
- **User:** user1@manchesterunited.com
- **File Name:** invoice2024.exe
- **File Path:** C:\Users\User1\Downloads\invoice2024.exe
- **SHA256 Hash:** e3b0c44298...
- **Source URL:** http://malicious-site[.]com/invoice2024.exe

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. **Review Alert Details in SIEM:**
    - Identify suspicious activity, source and affected system.
2. **Validate Alert Severity:**
    - Check if the file is potentially malicious using OSINT tools like VirusTotal or in-house sandboxing.
3. **Correlate Logs:**
    - Gather related logs (network, EDR and proxy logs).

L1 Workflow:

1. **Step 1: Analyse SIEM Alert Details:**

- Suspicious executable `invoice2024.exe` was downloaded by user1@manchesterunited.com.

- Host: USER-PC

- Source: `http://malicious-site[.]com/invoice2024.exe`

2. **Step 2: Verify File Hash:**
    - Search SHA256 hash (e3b0c44298...) on VirusTotal:

Detected as malicious by 20/30 antivirus engines.

Associated malware: LokiBot (credential-stealing trojan).

3. **Step 3: Gather Related Logs:**
    - **Proxy Logs:**

2024-11-18 10:24:30 UTC | GET | malicious-site[.]com/invoice2024.exe | Source IP: 192.168.1.45 (USER-PC)

    - **EDR Logs:**

2024-11-18 10:25:32 UTC | File Execution | Path: C:\Users\User1\Downloads\invoice2024.exe

4. **Step 4: Escalate to L2 Analyst:**

Alert of malicious file detected on USER-PC.

File: invoice2024.exe, confirmed as LokiBot via VirusTotal.

Execution observed on endpoint. Escalating for deeper investigation and containment.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. **Conduct Detailed Malware Analysis:**
    - Correlate logs from endpoint, firewall and DNS for potential command-and-control (C2) traffic.
    - Check for lateral movement or data exfiltration.
2. **Contain and Remediate Threat.**

L2 Workflow:

1. **Step 1: Investigate File Behavior:**
    - Check EDR telemetry for post-execution activity:

- Created registry persistence:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\malware.exe

- Established outbound connection to C2 server: 45.76.123.10:443

    - **Firewall Logs:**

2024-11-18 10:26:15 UTC | Outbound Traffic | Destination IP: 45.76.123.10 | Port: 443

2. **Step 2: Determine Root Cause:**
    - Infection occurred due to the user downloading and executing a malicious file.
    - No lateral movement detected; activity contained to USER-PC.
3. **Step 3: Containment Actions:**
    - Isolate the host from the network.
    - Quarantine the file using EDR.
    - Block C2 IP (45.76.123.10) and domain (malicious-site[.]com) at the firewall.
4. **Step 4: Recommend Remediation Steps:**

- Disconnect USER-PC for forensic analysis.

- Re-image the system and reset user1's credentials.

- Notify the user and train on phishing awareness.

- Escalate to L3 for IOC enrichment and long-term recommendations.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. **Enrich Incident with Threat Intelligence:**
    - Link file hash and C2 IP to known campaigns.
    - Provide additional IOCs.
2. **Advise on Long-Term Mitigation:**
    - Recommend enhanced security measures.

L3 Workflow:

1. **Step 1: CTI Enrichment:**
    - Investigate LokiBot campaign linked to file hash:

- LokiBot is a credential-stealing malware delivered via phishing emails.

- Campaign active since November 2024 targeting finance departments.

    - Retrieve additional IOCs:

C2 IPs: 45.76.123.10, 198.51.100.22

Domains: download-malware[.]com

File Hashes: f1a2b3c4d5...

2. **Step 2: Recommend Strategic Actions:**

- Implement email filtering for phishing campaigns.

- Update endpoint protection to detect LokiBot variants.

- Add retrieved IOCs to the client's threat intelligence platform.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A critical malware infection (LokiBot) was detected on USER-PC. The malicious file (`invoice2024.exe`) was downloaded and executed, resulting in communication with a known command-and-control (C2) server.

Incident Details:

- File: invoice2024.exe (confirmed LokiBot malware).

- C2 Server: 45.76.123.10 (blocked).

- Host Impacted: USER-PC (isolated and quarantined).

- User: user1@manchesterunited.com.

Action Taken:

- Host isolated and file quarantined.

- C2 server and domain blocked at the firewall.

Recommendations:

1. Re-image the affected system.

2. Reset user1's credentials.

3. Conduct phishing awareness training.

4. Implement the following IOCs:

   - C2 IPs: 45.76.123.10, 198.51.100.22

   - Domains: malicious-site[.]com, download-malware[.]com

Next Steps:

We recommend reviewing all email systems for potential phishing campaigns and enhancing endpoint protection with updated rules for LokiBot malware detection.

SCENARIO 3: UNUSUAL LOGIN ATTEMPT DETECTED

Alert Details in SIEM:

- **Alert Name:** Unusual Login Attempt Detected
- **Severity:** High
- **Source:** SIEM (via Identity and Access Management (IAM) System)
- **Time:** 2024-11-18 14:47:21 UTC
- **User:** admin@manchesterunited.com
- **Source IP:** 203.0.113.85 (Country: Russia)
- **Target Host:** Workstation1 (Head of IT Department)
- **Login Method:** Remote Desktop Protocol (RDP)
- **Geographic Location:** Russia
- **Additional Info:** Multiple failed login attempts followed by a successful login.

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. **Review Alert Details in SIEM:**
    - Check for any abnormal login attempts, especially regarding user access, source IP and login method.
2. **Verify Authenticity of Login:**
    - Cross-check the user's login history and validate geographic location.
3. **Determine Severity:**
    - Check for possible brute-force attack or compromised credentials.

L1 Workflow:

1. **Step 1: Examine Alert Details:**

- Alert shows a high severity due to unusual login attempts by admin@manchesterunited.com via RDP.

- Failed logins from IP address 203.0.113.85 (Russia), followed by a successful login.

- Target Host: Workstation1 (Head of IT Department).

2. **Step 2: Validate User's Typical Login Behavior:**
    - **User's last known login:**
        - 2024-11-18 10:15 UTC from IP 192.168.1.100 (Headquarters, Local Network).
    - **Geographical mismatch:**
        - User is typically based in Malaysia (Headquarters).
    - **Recent Activity:** No prior logins from Russia.
3. **Step 3: Escalate to L2 Analyst for Deeper Investigation:**

- Admin login attempt via RDP from Russia. Multiple failed attempts followed by successful login.

- Escalating for a full review of potential credential compromise or brute-force attack.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. **Analyse Login Attempts in Detail:**
    - Cross-check for abnormal login patterns, failed login attempts, or unusual user activity.
2. **Correlate with Network and Endpoint Logs:**
    - Investigate RDP session and check for any lateral movement or other suspicious activities.
3. **Determine Threat Source and Impact:**
    - Check if there is any sign of credential compromise.

L2 Workflow:

1. **Step 1: Investigate Login Details:**
    - **Login Attempts:**
        - 2024-11-18 14:45 UTC | Failed login from IP: 203.0.113.85 (Russia).

- 2024-11-18 14:46 UTC | Failed login from IP: 203.0.113.85 (Russia).
- 2024-11-18 14:47 UTC | Successful login from IP: 203.0.113.85 (Russia).

2. **Step 2: Review RDP Session Logs:**
    - **RDP Logs:**

2024-11-18 14:47:22 UTC | RDP session started | User: admin@manchesterunited.com | Source IP: 203.0.113.85

- Session lasted for 15 minutes.

- No signs of malicious activity detected during the session.

3. **Step 3: Correlate with Other Logs:**
    - **Network Logs:**

2024-11-18 14:47:21 UTC | Access to critical system: DatabaseServer01 | User: admin@manchesterunited.com | Source IP: 203.0.113.85

4. **Step 4: Escalate to L3 Analyst for Credential Theft Investigation:**

- Admin login from Russia detected on Workstation1. No clear signs of attack yet.

- Successful login despite previous failed attempts. Cross-referencing with network logs shows access to sensitive systems.

- Escalating for a deeper dive into credential theft or remote access tools.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. **Enrich Incident with Threat Intelligence:**
    - Link the IP address and unusual login behavior to known attack campaigns or threat actor TTPs (Tactics, Techniques and Procedures).
2. **Provide Threat Context:**
    - Offer insights into potential credential stuffing, brute-force attack, or misuse of RDP.

L3 Workflow:

1. **Step 1: CTI Enrichment:**
    - Investigate the IP address (203.0.113.85), identified as originating from a known Russian threat actor group:

- Known threat actor: APT28 (Fancy Bear).

- Recent campaigns involving credential stuffing and exploitation of weak RDP configurations.

2. **Step 2: Investigate Potential Brute-Force or Credential Stuffing Attack:**
    - Review related incidents within the environment or client:

- Multiple failed login attempts followed by successful login is consistent with a brute-force attempt.

- Connection to known C2 infrastructure used by APT28 for credential harvesting.

3. **Step 3: Provide Strategic Recommendations:**
    - **Immediate Actions:**

- Force a password reset for admin@manchesterunited.com.

- Revoke any existing RDP sessions from external IPs.

- Implement MFA (Multi-Factor Authentication) on all RDP endpoints.

    - **Long-Term Mitigation:**

- Restrict RDP access from external IPs.

- Update firewall rules to block foreign IP addresses for critical systems.

- Implement more robust password policies and detect brute-force attempts early.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A high-severity login anomaly was detected for admin@manchesterunited.com via Remote Desktop Protocol (RDP). The login attempt originated from an unusual geographic location (Russia), followed by a successful login despite multiple failed attempts.

Incident Details:

- User: admin@manchesterunited.com.

- Source IP: 203.0.113.85 (Russia).

- Target Host: Workstation1 (Head of IT Department).

- RDP session started at 14:47 UTC, with access to critical systems.

Action Taken:

- Password reset for admin@manchesterunited.com.

- Revoked all active RDP sessions from external sources.

- Enhanced network defenses and restricted RDP access to local network.

Recommendations:

1. Implement Multi-Factor Authentication (MFA) for all RDP users.

2. Restrict RDP access to trusted IP addresses only.

3. Enhance monitoring for unusual login behavior and external access.

Next Steps:

We recommend revising RDP access policies and implementing stronger network segmentation to mitigate future risks.

SCENARIO 4: SUSPICIOUS FILE EXECUTION DETECTED

Alert Details in SIEM:

- **Alert Name:** Suspicious File Execution Detected
- **Severity:** Critical
- **Source:** Endpoint Detection and Response (EDR) system
- **Time:** 2024-11-18 10:25:15 UTC
- **User:** User123@clientcompany.com
- **Host:** Workstation25 (Finance Department)
- **File Executed:** invoice_update.exe
- **File Path:** C:\Users\User123\Downloads\invoice_update.exe
- **Hash:** 5f4dcc3b5aa765d61d8327deb882cf99
- **Behavior:**
    - Spawns cmd.exe to execute obfuscated PowerShell commands.
    - Downloads additional payload from http://malicious-site.com/payload.exe.
    - Attempts to establish connection with external IP: 198.51.100.10 (Country: Ukraine).

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. **Review the alert in the SIEM:**
    - Check for context about the file, user activity and host.
    - Note any abnormal behavior or connections to external IPs.
2. **Validate file authenticity:**
    - Check the file hash against VirusTotal or similar tools.
    - Determine if the file is malicious.
3. **Escalate if necessary:**

- If malicious behavior is confirmed or highly suspected, escalate to L2 for further analysis.

L1 Workflow:

1. **Step 1: Examine Alert Details in SIEM:**

- Alert flagged suspicious execution of `invoice_update.exe` by User123 on Workstation25.

- File attempted to spawn PowerShell, download additional payloads and connect to an external IP.

2. **Step 2: Validate File Hash:**
    - Perform a hash lookup on VirusTotal:
        - **Result:** Malicious file identified as part of Emotet malware family.
        - Reputation: Highly malicious (detected by 57/70 AV engines).
3. **Step 3: Correlate User and Host Activity:**
    - Recent activities on the user's host show the file was downloaded from an email attachment:

- Email subject: "Urgent Invoice Update"

- Sender: invoices@malicious-domain.com

4. **Step 4: Escalate to L2:**

- Suspicious file execution confirmed as malicious (Emotet malware).

- Escalating for deeper investigation and containment.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. **Investigate full impact on the endpoint:**
    - Identify all processes spawned by the malicious file.
    - Investigate any network connections established by the malware.
2. **Check for lateral movement:**
    - Look for other hosts accessed from the infected machine.

3. **Determine the infection vector:**
    - Validate how the malicious file was introduced (phishing email).

L2 Workflow:

1. **Step 1: Investigate Endpoint Activity:**
    - Review EDR logs for invoice_update.exe:

- Executed at: 2024-11-18 10:25:15 UTC

- Spawned Process: `cmd.exe /c powershell.exe -enc (obfuscated commands)`.

- Dropped File: `C:\Temp\payload.exe`.

- New Payload Hash: d41d8cd98f00b204e9800998ecf8427e (also malicious).

2. **Step 2: Review Network Traffic Logs:**
    - Check connections from the infected host:

- 2024-11-18 10:26:00 UTC | Outbound Connection | External IP: 198.51.100.10 (Ukraine).

- Data exchanged: 500 KB.

3. **Step 3: Correlate with Email Logs:**
    - Review email logs for User123:

- Email received from invoices@malicious-domain.com at 2024-11-18 09:50 UTC.

- Attachment: `invoice_update.exe` (confirmed malicious).

4. **Step 4: Escalate to L3 for Threat Intelligence and Strategic Recommendations:**

- Emotet malware detected on Workstation25.

- Malware executed PowerShell commands, downloaded additional payloads and attempted C2 communication.

- Escalating to L3 for deeper CTI insights and recommendations for broader containment.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. **Enrich incident with threat intelligence:**

- Link the malicious IP, domain and hashes to known campaigns or actors.
- Provide recommendations for containment and prevention.

2. **Advise on mitigating the broader threat:**
    - Identify if similar activity exists in the environment.
    - Suggest proactive measures.

L3 Workflow:

1. **Step 1: CTI Enrichment:**
    - Investigate IP and domain associated with the attack:

- Malicious IP: 198.51.100.10

- Associated with Emotet C2 servers.

- Recent campaigns targeting finance departments in APAC.

- Domain: malicious-site.com

- Known phishing domain hosting Emotet payloads.

2. **Step 2: Check for Broader Threats in the Environment:**
    - Review SIEM for related activity:

- No similar suspicious activity observed across other endpoints.

3. **Step 3: Provide Strategic Recommendations:**
    - **Immediate Actions:**

- Isolate Workstation25 from the network.

- Quarantine the malicious files and terminate processes.

- Block external IP: 198.51.100.10 at the firewall.

    - **Long-Term Measures:**

- Implement advanced email filtering to block phishing attempts.

- Conduct user awareness training on identifying phishing emails.

- Deploy endpoint controls to prevent unauthorised PowerShell execution.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A critical malware infection (Emotet) was detected on Workstation25 in the Finance Department. The malware originated from a phishing email and exhibited malicious behavior, including PowerShell execution, payload download and C2 communication.

Incident Details:

- File Executed: `invoice_update.exe`.

- Malicious IP: 198.51.100.10 (Ukraine).

- Infection Vector: Phishing email from invoices@malicious-domain.com.

Action Taken:

- Workstation25 isolated from the network.

- Malicious file and processes quarantined.

- External IP blocked at the firewall.

Recommendations:

1. Implement enhanced email filtering and sandboxing for attachments.

2. Train employees on identifying phishing emails.

3. Deploy endpoint controls to block PowerShell misuse.

Next Steps:

We recommend a review of email filtering policies and conducting organisation-wide phishing simulations to enhance user awareness.

SCENARIO 5: BRUTE FORCE LOGIN ATTEMPT DETECTED

Alert Details in SIEM:

- **Alert Name:** Brute Force Login Attempt Detected
- **Severity:** High
- **Source:** Active Directory Audit Logs
- **Time:** 2024-11-18 03:15:42 UTC
- **User:** admin.user (Active Directory Account)
- **Host:** VPN Gateway (192.168.10.25)
- **Source IP:** 203.0.113.5 (Unknown Location)
- **Failed Login Attempts:** 150 attempts in 2 minutes
- **Successful Login?:** No

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. **Review the SIEM alert details:**
    - Confirm the origin of the brute force attempt and its impact.
2. **Check account status and recent activity:**
    - Verify if the targeted account has been locked or is still active.
3. **Determine initial severity and escalate if needed:**
    - If the attempt was unsuccessful, mark it as suspicious and escalate to L2 for further investigation.

L1 Workflow:

1. **Step 1: Analyse SIEM Alert:**

- Multiple failed login attempts detected for `admin.user` from Source IP 203.0.113.5.

- Attempts occurred over a short timeframe, indicating brute force behavior.

2. **Step 2: Review Account Activity:**
    - Query Active Directory logs for the targeted account:

- Account Status: Locked due to multiple failed login attempts.

- Recent Activities: No legitimate access from IP 203.0.113.5.

3. **Step 3: Check the Source IP Details:**
    - Perform IP lookup:

- Geo-Location: Unknown region (No prior history for this IP in the client network).

- Reputation: Listed in spam/malicious IP databases.

4. **Step 4: Escalate to L2:**

- Confirmed brute force attempt targeting `admin.user`.

- Account locked as a precaution.

- Escalating for in-depth network and attack vector analysis.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. **Trace the origin of the attack:**
    - Correlate the source IP with VPN logs and other systems to determine its path.
2. **Investigate any potential successful breaches:**
    - Validate whether any sensitive accounts or systems were accessed.
3. **Identify related activity:**
    - Check if this source IP or similar login attempts occurred across other accounts or systems.

L2 Workflow:

1. **Step 1: Investigate Source IP Logs:**
    - Query VPN gateway and firewall logs:

- Source IP: 203.0.113.5

- Attempts to access multiple accounts (admin.user, backup.admin, it.manager).

- No successful authentication detected.

    - Traffic flagged as suspicious due to geographic mismatch (unknown region).

2. **Step 2: Check for Lateral Movement:**

    - Verify if similar activity occurred across the network:

- Additional Brute Force Attempts: Found targeting `backup.admin` and `it.manager` accounts.

- No successful logins detected.

3. **Step 3: Review Logs for Other Threat Indicators:**

    - Identify any related activity within the same timeframe:

- No signs of malware or unusual activity on endpoints associated with these accounts.

4. **Step 4: Escalate to L3 for Threat Intelligence and Recommendations:**

plaintext

Copy code

- Confirmed brute force attempt targeting admin and IT accounts.

- Source IP linked to known malicious campaigns.

- No successful logins or evidence of compromise detected.

- Escalating for CTI enrichment and client-specific recommendations.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. **Enrich the incident with threat intelligence:**

    - Correlate the source IP with known threat actor campaigns.

2. **Advise on proactive measures:**

    - Recommend account hardening and threat prevention strategies.

L3 Workflow:

1. **Step 1: CTI Enrichment:**
    - Investigate IP 203.0.113.5 in global threat databases:

- IP linked to `APT33` (Advanced Persistent Threat Group).

- Known for brute force attacks targeting admin accounts to infiltrate networks.

- Recent campaigns targeting organisations in APAC.

2. **Step 2: Provide Strategic Recommendations:**
    - **Immediate Actions:**

- Block IP 203.0.113.5 at the perimeter firewall.

- Enforce account lockout policies after five failed login attempts.

    - **Long-Term Measures:**

- Implement multi-factor authentication (MFA) for all admin and critical accounts.

- Conduct regular audits of privileged accounts for unusual activity.

- Use geolocation restrictions to block access from high-risk regions.

3. **Step 3: Check for Similar Campaigns:**
    - Search for related incidents using the IOC (Indicators of Compromise):

- No other linked IPs or malicious domains detected in this environment.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A brute force login attempt targeting administrative accounts was detected. The source IP was linked to known APT33 threat activity. No successful login or compromise was identified.

Incident Details:

- Targeted Accounts: `admin.user`, `backup.admin`, `it.manager`.

- Source IP: 203.0.113.5 (Malicious IP from APT33 campaigns).

- Number of Failed Login Attempts: 150 in 2 minutes.

Actions Taken:

1. Source IP blocked at the firewall.

2. Accounts temporarily locked to prevent unauthorised access.

Recommendations:

1. Enable MFA for administrative and critical accounts.

2. Restrict VPN access to trusted geographic regions.

3. Conduct a review of privileged account activity to detect anomalies.

Next Steps:

We recommend enabling geolocation-based access controls and conducting phishing simulation training to prepare staff for targeted campaigns.

SCENARIO 6: PHISHING EMAIL WITH MALICIOUS ATTACHMENT

Alert Details in SIEM:

- **Alert Name:** Malicious Email Attachment Detected
- **Severity:** High
- **Source:** Email Security Gateway
- **Time:** 2024-11-18 10:23:17 UTC
- **Recipient:** finance.manager@manchesterunited.com
- **Sender:** invoices@maliciousdomain.com
- **Subject Line:** "Outstanding Invoice - Action Required"
- **Attachment:** invoice.pdf.exe (Flagged as malware)
- **Attachment Hash:** 5f4dcc3b5aa765d61d8327deb882cf99
- **Detection Engine:** Static and Behavioral Analysis

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. **Review email details and attachment analysis report.**
2. **Verify the recipient's interaction with the email.**
3. **Escalate if the attachment was downloaded or executed.**

L1 Workflow:

1. **Step 1: Analyse SIEM Alert Details:**

- Email flagged by security gateway due to a suspicious attachment (`invoice.pdf.exe`).

- Sender domain `maliciousdomain.com` not whitelisted or previously seen.

2. **Step 2: Verify Recipient Interaction:**
    - Check email logs for recipient activity:

- Recipient: `finance.manager@manchesterunited.com`

- Email opened: Yes.

- Attachment downloaded: No.

3. **Step 3: Verify Attachment Details:**
    - Review malware analysis report from sandbox:

- Behavior: Drops payloads, communicates with external IP `45.67.89.10`.

- Hash linked to known malware family: Emotet.

4. **Step 4: Escalate to L2:**

- Suspicious email detected with malware attachment targeting finance manager.

- Email opened but attachment not downloaded.

- Escalating for further investigation of sender domain and payload analysis.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. **Investigate sender domain and email headers.**
2. **Analyse related email logs for similar activity across the organisation.**
3. **Check if malicious payloads communicated with external IPs or domains.**

L2 Workflow:

1. **Step 1: Investigate Email Headers and Sender Domain:**

- Sender Domain: `maliciousdomain.com`

- SPF, DKIM, DMARC checks: Failed.

- Associated IP: 203.0.113.10 (blacklisted).

2. **Step 2: Check for Lateral Spread:**
    - Query email gateway for similar emails sent organisation-wide:

- Additional Emails: 12 similar emails sent to various recipients.

- Status: Blocked by the gateway, no other emails delivered.

3. **Step 3: Analyse Attachment Communication:**
    - Investigate if any endpoints communicated with external IP 45.67.89.10:

- No outbound connections detected from the recipient's endpoint.

4. **Step 4: Escalate to L3 for Threat Intelligence Enrichment:**

- Confirmed malicious email campaign targeting finance personnel.

- Attachment linked to known malware family (Emotet).

- Escalating for CTI enrichment and broader threat context.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. **Enrich the incident with broader intelligence on the malware family and campaign.**
2. **Advise on targeted user awareness and email security measures.**

L3 Workflow:

1. **Step 1: CTI Enrichment on Malware:**
    - Hash 5f4dcc3b5aa765d61d8327deb882cf99:

- Malware Family: Emotet.

- Characteristics: Credential theft, lateral movement, drops ransomware payloads.

- Campaigns: Known to target finance departments globally.

2. **Step 2: Investigate Associated Infrastructure:**
    - Review domains and IPs linked to maliciousdomain.com and 45.67.89.10:

- Additional IPs: `192.0.2.15`, `198.51.100.22` (active command-and-control servers).

- Malware linked to phishing campaigns in APAC.

3. **Step 3: Provide Recommendations:**
    - **Immediate Actions:**

- Block domain `maliciousdomain.com` and IP `45.67.89.10` at email gateway and firewall.

- Isolate and scan recipient's endpoint for potential compromise.

- **Preventative Measures:**

- Conduct targeted phishing awareness training for finance team.

- Enable stricter email attachment scanning policies.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A phishing email targeting the finance department was detected. The email contained a malicious attachment linked to the Emotet malware family.

Incident Details:

- Targeted Recipient: `finance.manager@manchesterunited.com`.

- Sender Domain: `maliciousdomain.com` (malicious).

- Attachment: `invoice.pdf.exe`.

- Associated Malware: Emotet (known for credential theft and ransomware).

Actions Taken:

1. Suspicious email flagged and quarantined by email gateway.

2. Domain and associated IPs blocked organisation-wide.

3. No evidence of payload execution or compromise on recipient's endpoint.

Recommendations:

1. Conduct phishing simulation training for finance department staff.

2. Block known malicious domains and IPs linked to the Emotet campaign.

3. Regularly update endpoint protection systems with latest malware signatures.

Next Steps:

We recommend enhancing email security policies to prevent similar attempts and monitoring for signs of credential abuse across critical systems.

SCENARIO 7: SUSPICIOUS INTERNAL FILE TRANSFER DETECTED

Alert Details in SIEM:

- **Alert Name:** Unusual File Transfer from Sensitive Server
- **Severity:** Critical
- **Source:** Data Loss Prevention (DLP) system
- **Time:** 2024-11-18 13:47:22 UTC
- **Source Host:** HR-DATA-SERVER
- **Destination Host:** DESKTOP-USER123
- **File Transferred:** Employee_Salary_Data_2024.xlsx
- **File Size:** 10 MB
- **Transfer Method:** SMB Protocol
- **User:** izzmier@manchesterunited.com
- **Geolocation of User's Device:** Internal Office Network

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. **Verify the legitimacy of the file transfer.**
2. **Check if the user had proper authorisation for access and transfer.**
3. **Escalate if it appears unauthorised or anomalous.**

L1 Workflow:

1. **Step 1: Analyse SIEM Alert Details:**

- File transfer from HR-DATA-SERVER to local desktop `DESKTOP-USER123`.

- File: `Employee_Salary_Data_2024.xlsx` (sensitive).

- User: `izzmier@manchesterunited.com`.

2. **Step 2: Verify User Activity:**
    - Check access logs for HR-DATA-SERVER:

- User Access Time: 2024-11-18 13:45:15 UTC.

- Transfer initiated 2 minutes later.

- Authentication: Successful (via Active Directory).

3. **Step 3: Review User Role:**
    - Confirm user's role:

- Role: Marketing Manager.

- Justification for accessing HR data: None.

4. **Step 4: Escalate to L2:**

- Anomalous file transfer detected involving sensitive HR data.

- User `izzmier@manchesterunited.com` lacks a valid reason for accessing this data.

- Escalating for further investigation and to determine if the file was exfiltrated.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. **Determine if the user’s account was compromised.**
2. **Check for lateral movement or further suspicious activity from the user.**
3. **Investigate whether the file was exfiltrated beyond the network.**

L2 Workflow:

1. **Step 1: Review User's Recent Activity:**
    - Query Active Directory and endpoint logs for anomalous behavior:

- Login Locations: Office network only.

- Suspicious Activity: None detected prior to file transfer.

- File Interaction: Copied the file to local desktop but did not share externally.

2. **Step 2: Check for Malware or Account Compromise:**
    - Conduct endpoint scan on DESKTOP-USER123:

- Malware Detected: None.

- External connections: None.

- Possible account misuse for unauthorised data access.

3. **Step 3: Investigate HR-DATA-SERVER Logs:**
    - Review server logs for unauthorised access attempts:

- No failed logins or brute force attempts.

- Single successful login by `izzmier@manchesterunited.com`.

4. **Step 4: Escalate to L3 for Incident Context:**

- File transfer appears unauthorised.

- No signs of compromise on user's endpoint or the server.

- Potential misuse of credentials to access sensitive HR data.

- Escalating to L3 for context on insider threats and policy violations.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. **Evaluate potential insider threat motivations or policy breaches.**
2. **Enrich incident details with behavioral insights and CTI.**
3. **Advise on disciplinary or preventive measures.**

L3 Workflow:

1. **Step 1: Analyse Behavioral Context:**
    - Review CTI for patterns in insider threats:

- Insider Threat Indicators:

  - Unauthorised access to sensitive data.

- Role misalignment for data access.

- Single file transfer, likely exploratory.

2. **Step 2: Investigate Previous Alerts on User:**
    - Query SIEM for historical alerts involving izzmier@manchesterunited.com:

- Past Alerts:

- June 2024: Attempted access to restricted finance server.

- September 2024: High-volume printing of confidential documents.

3. **Step 3: Provide Recommendations:**
    - **Immediate Actions:**

- Disable user account pending investigation.

- Notify HR and legal teams for policy review.

    - **Preventative Measures:**

- Implement user behavior analytics (UBA) for anomalous access patterns.

- Restrict access to sensitive data by enforcing role-based access controls (RBAC).

- Conduct periodic audits of user access permissions.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A suspicious file transfer of sensitive HR data was detected from `HR-DATA-SERVER` to a local desktop (`DESKTOP-USER123`). The user involved (`izzmier@manchesterunited.com`) lacked valid authorisation to access this data.

Incident Details:

- File: `Employee_Salary_Data_2024.xlsx`.

- Source: `HR-DATA-SERVER`.

- Destination: `DESKTOP-USER123`.

- User: `izzmier@manchesterunited.com`.

- Authentication: Successful.

Actions Taken:

1. User account disabled pending investigation.
2. No signs of external exfiltration detected.
3. Server and endpoint secured and logs collected for further review.

Recommendations:

1. Conduct internal investigation for potential insider threat or policy violation.
2. Review and enforce stricter role-based access controls (RBAC).
3. Implement user behavior analytics to monitor anomalous actions.

Next Steps:

Please coordinate with HR and legal departments to address this incident. Regular audits of sensitive data access permissions are advised.

SCENARIO 8: PHISHING EMAIL LEADING TO MALWARE DOWNLOAD

Alert Details in SIEM:

- **Alert Name:** Suspicious File Download After Email Click
- **Severity:** High
- **Source:** Email Security Gateway
- **Time:** 2024-11-18 09:15:42 UTC
- **Sender Email:** admin@secure-docs.com
- **Recipient Email:** iffah@manchesterunited.com
- **Subject:** "Secure Document: Payroll Update 2024"
- **Attachment/Link:** https://secure-docs.com/payroll2024.exe
- **Action:** Link clicked by the user, file downloaded.
- **File Type:** Executable file (payroll2024.exe)
- **Endpoint:** LAPTOP-IFFAH

Phase 1: L1 Analyst Triage and Initial Analysis

Tasks:

1. Confirm if the email was phishing or legitimate.
2. Investigate the user's actions.
3. Escalate if suspicious activities are confirmed.

L1 Workflow:

1. **Step 1: Review SIEM Alert:**

- Suspicious executable downloaded via email link.

- Source Email: admin@secure-docs.com (unknown).

- Recipient: iffah@manchesterunited.com.

2. **Step 2: Check Email Header and Reputation:**
    - Analyse email headers for spoofing:

- SPF: Fail.

- DKIM: Fail.

- DMARC: Fail.

- Sender domain reputation: Malicious (via OSINT).

3. **Step 3: Verify User Actions:**
    - Endpoint logs:

- File downloaded: payroll2024.exe.

- File executed: Yes, at 09:18:22 UTC.

4. **Step 4: Escalate to L2:**

- User clicked a phishing link and executed a suspicious file.

- Email source spoofed with malicious domain reputation.

- Endpoint potentially compromised. Escalating for deeper investigation.

Phase 2: L2 Analyst Investigation and Root Cause Analysis

Tasks:

1. Check for malware execution and persistence on the endpoint.
2. Identify potential lateral movement or C2 communications.
3. Investigate threat indicators related to the downloaded file.

L2 Workflow:

1. **Step 1: Scan Endpoint for Malware:**
    - Endpoint EDR results:

- Malware detected: Trojan.Downloader (via `payroll2024.exe`).

- Persistence mechanism: Registry key modification (`HKCU\Software\Microsoft\Windows\Run`).

- Additional payloads: Attempted download of `stealer.exe` from `92.122.54.12`.

2. **Step 2: Check for Lateral Movement:**
    - Lateral movement attempt logs:

- None detected.

- Malware confined to the infected endpoint.

3. **Step 3: Investigate Network Activity:**
    - C2 communication analysis:

- Outbound traffic to `92.122.54.12` (known malicious IP).

- Protocol: HTTP POST request (payload encoded).

- Frequency: Every 5 minutes since execution.

4. **Step 4: Escalate to L3 for Threat Intelligence Enrichment:**

- Malware `Trojan.Downloader` active on `LAPTOP-IFFAH`.

- Persistence and C2 communication detected.

- Additional payload attempted download from malicious IP `92.122.54.12`.

- Escalating to L3 for CTI insights and remediation strategy.

Phase 3: L3 Analyst Cyber Threat Intelligence (CTI) and Strategic Insights

Tasks:

1. Correlate malware behavior with known threat groups.
2. Provide detailed remediation and prevention recommendations.
3. Assess overall threat posture and potential risks.

L3 Workflow:

1. **Step 1: Identify Malware Family:**

- Threat Intelligence search:

- Malware: Trojan.Downloader (variant associated with FIN7 group).

- Known capabilities: Credential theft, secondary payload delivery, network reconnaissance.

- Target: Financial and sensitive organisational data.

2. **Step 2: Analyse C2 Communication:**
    - Malicious IP (92.122.54.12) details:

- OSINT status: Known C2 server tied to FIN7 campaigns.

- Geolocation: Russia.

3. **Step 3: Recommendations for Mitigation:**
    - **Immediate Actions:**

- Isolate infected endpoint (`LAPTOP-IFFAH`) from the network.

- Block outbound traffic to IP `92.122.54.12`.

- Remove persistence registry key and malware payloads.

    - **Preventative Measures:**

- Implement email filtering for spoofed domains.

- Educate users on phishing awareness.

- Deploy DNS filtering for malicious domains.

4. **Step 4: Provide Client Context:**

- Threat actor: Likely FIN7 based on malware and C2 infrastructure.

- Impact: Medium (limited to one endpoint, no lateral movement detected).

- Risks: Potential data exfiltration or further payload deployment.

Phase 4: SOC Team Prepares Notification for Client

Incident Summary:

A phishing email targeting `iffah@manchesterunited.com` led to the download and execution of a Trojan.Downloader malware (`payroll2024.exe`). The malware attempted to communicate with a known malicious IP and establish persistence.

Incident Details:

- **Sender Email:** admin@secure-docs.com (spoofed domain).

- **Attachment/Link:** https://secure-docs.com/payroll2024.exe.

- **Infected Endpoint:** `LAPTOP-IFFAH`.

- **Malicious IP:** 92.122.54.12 (C2 server).

Actions Taken:

1. Isolated the infected endpoint from the network.

2. Blocked outbound traffic to the malicious IP.

3. Removed malware and its persistence mechanism.

Recommendations:

1. Conduct a detailed forensic investigation of the infected endpoint.

2. Educate users about phishing risks and red flags.

3. Review email security configurations (SPF, DKIM, DMARC).

Threat Actor Attribution:

- Malware type and C2 infrastructure linked to FIN7 campaigns targeting sensitive organisational data.

Next Steps:

We recommend additional monitoring for similar phishing campaigns and enhanced endpoint detection.