STEP-BY-STEP TO INVESTIGATE AN ALERT FROM SIEM WITH EXPLANATION & SIMULATION

BY IZZMIER IZZUDDIN

CONTENTS

GENERAL STEP-BY-STEP GUIDE TO INVESTIGATE AN ALERT FROM SIEM

1. **Initial Alert Triage**

    1. **Review Alert Details**
        - Examine the alert for key details: source, destination, type, time, etc.
    2. **Prioritise the Alert**
        - Assess the criticality based on the nature of the alert and potential impact.

2. **Data Collection**

    1. **Gather Relevant Logs**
        - Collect logs from various sources (e.g., firewalls, servers, endpoints) to analyse the alert.
    2. **Analyse Context**
        - Use OSINT tools to gather additional information about involved IPs, files, etc.

3. **Initial Analysis**

    1. **Check Indicators of Compromise (IoCs)**
        - Analyse IoCs such as IP addresses, file hashes, and URLs to identify known threats.
    2. **Assess Impact**
        - Evaluate the potential impact on the system and organisation.

4. **Deep Dive Analysis**

    1. **Use OSINT Tools**
        - Utilise OSINT tools for further investigation of IoCs and threat intelligence.
    2. **Analyse Patterns and Behaviour**
        - Examine logs and network traffic to understand the behaviour and pattern of the alert.

5. **Containment and Mitigation**

    1. **Quarantine or Block Malicious Entities**
        - Isolate or block malicious files, IPs, and other entities.
    2. **Enhance Security Measures**
        - Implement additional security measures to prevent recurrence.
    3. **Identify Related Activities**
        - Check for other systems or activities that might be related to the alert.

6. **Eradication**

    1. **Remove Malicious Entities**

    - Ensure all malicious files, connections, and access points are removed.

2. **Verify System Integrity**
    - Confirm that systems are secure and functioning correctly.

7. **Recovery**

    1. **Restore Operations**
        - Reconnect and monitor the system for any further issues.
    2. **Communication**
        - Inform stakeholders about the incident and remediation steps taken.

EXAMPLES WITH EXPLAINATION

Example Alert 1: Malware Detected On Endpoint

1. Initial Alert Triage

1. **Review Alert Details**
    - **Explanation**: Examine the alert to understand which endpoint is affected, the type of malware detected, and the time of detection.
    - **Example**: Endpoint: PC-01, Malware: Trojan.Win32.Generic, Time: 2024-07-28 10:00:00.
2. **Prioritise the Alert**
    - **Explanation**: Assess the criticality based on the potential impact of the malware.
    - **Example**: High-priority if the malware is capable of stealing sensitive information.

2. Data Collection

1. **Gather Endpoint Logs**
    - **Explanation**: Collect relevant logs from the affected endpoint to analyse the malware detection.
    - **Example Logs**:
        - **Antivirus Logs**:

```
Jul 28 10:00:00 AV: Malware detected on PC-01,
Trojan.Win32.Generic
```

2. **Analyse Malware Sample**
    - **Explanation**: Use OSINT tools to gather information about the detected malware.
    - **Example**: Checking if Trojan.Win32.Generic is known for malicious activities using OSINT tools like VirusTotal, Hybrid Analysis, and MalwareBazaar.

3. Initial Analysis

1. **Check User Actions**
    - **Explanation**: Determine if the user performed any actions that led to the malware infection.
    - **Example**: Checking if the user on PC-01 downloaded a suspicious file or visited a malicious website.
2. **Assess Malware Impact**
    - **Explanation**: Evaluate the potential impact of the malware on the affected endpoint and the organisation.
    - **Example**: Identifying if the malware has exfiltrated data or compromised other systems.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**
   - **Explanation**: Use various OSINT tools to gather more information about the detected malware.
   - **Example**:
     - **VirusTotal**: Check if the detected malware sample is flagged as malicious.
     - **Hybrid Analysis**: Analyse the behaviour of the malware sample in a sandbox environment.
     - **MalwareBazaar**: Investigate if the malware sample is known and categorised.
2. **Endpoint Behaviour Analysis**
   - **Explanation**: Analyse the behaviour of the affected endpoint to identify any anomalies.
   - **Example**: Reviewing system changes, network connections, and processes initiated by the malware on PC-01.

5. Containment and Mitigation

1. **Isolate Endpoint**
   - **Explanation**: If the malware is confirmed malicious, isolate the endpoint to prevent further spread.
   - **Example**: Disconnecting PC-01 from the network.
2. **Remove Malware**
   - **Explanation**: Ensure the malware is removed from the affected endpoint.
   - **Example**: Running a full system scan and malware removal tool on PC-01.
3. **Identify Other Infected Systems**
   - **Explanation**: Check if other systems are infected by the same malware.
   - **Example**: Searching antivirus logs for other instances of Trojan.Win32.Generic.

6. Eradication

1. **Remove Malicious Files**
   - **Explanation**: Ensure any malicious files and registry changes made by the malware are removed.
   - **Example**: Deleting malicious files and reverting registry changes on PC-01.
2. **Verify Integrity**
   - **Explanation**: Confirm that the endpoint is secure and functioning correctly before reconnecting it to the network.
   - **Example**: Reviewing system logs and configurations on PC-01 to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
   - **Explanation**: Reconnect the cleaned and secured endpoint to the network and monitor for any further issues.
   - **Example**: Reconnecting PC-01 and monitoring for any signs of malware activity.
2. **Communication**
   - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
   - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Antivirus Logs:

```
Jul 28 10:00:00 AV: Malware detected on PC-01, Trojan.Win32.Generic
Jul 28 10:00:05 AV: Quarantined file C:\Users\User\Downloads\suspicious_file.exe
```

System Event Logs:

```
Jul 28 10:00:00 PC-01: Suspicious file downloaded from http://malicious.example.com
Jul 28 10:00:05 PC-01: Executed file C:\Users\User\Downloads\suspicious_file.exe
```

Example Alert 2: Suspicious Network Activity

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand the source and destination IP addresses, the type of suspicious activity, and the time it was detected.
   - **Example**: Source IP: 192.168.1.10, Destination IP: 203.0.113.50, Activity: Unusual data transfer, Time: 2024-07-28 12:30:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the potential impact of the suspicious activity.
   - **Example**: High-priority if the data transfer involves sensitive information.

2. Data Collection

1. **Gather Network Logs**
   - **Explanation**: Collect relevant network logs to analyse the suspicious activity.
   - **Example Logs**:
     - **Firewall Logs**:

       ```
       Jul 28 12:30:00 Firewall: Large data transfer detected from 192.168.1.10 to 203.0.113.50
       ```

2. **Analyse Network Traffic**
   - **Explanation**: Use OSINT tools to gather information about the source and destination IP addresses.
   - **Example**: Checking if 203.0.113.50 is known for malicious activities using OSINT tools like Shodan, IPinfo, and AbuseIPDB.

3. Initial Analysis

1. **Check User Actions**
   - **Explanation**: Determine if the user on the source IP performed any actions that led to the suspicious activity.
   - **Example**: Checking if the user on 192.168.1.10 initiated the data transfer or if it was automated.
2. **Assess Activity Impact**
   - **Explanation**: Evaluate the potential impact of the suspicious activity on the network and the organisation.
   - **Example**: Identifying if any sensitive data was transferred to the destination IP.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**
    - **Explanation**: Use various OSINT tools to gather more information about the source and destination IP addresses.
    - **Example**:
        - **Shodan**: Investigate if the IP 203.0.113.50 has open ports or is associated with known malicious activity.
        - **IPinfo**: Check the geolocation and ownership details of the IP address.
        - **AbuseIPDB**: Verify if the IP address is reported for abusive activities.
2. **Network Traffic Analysis**
    - **Explanation**: Analyse the network traffic involved in the suspicious activity to identify any anomalies.
    - **Example**: Reviewing the payload of the data transfer to detect any signs of malicious content.

5. Containment and Mitigation

1. **Block Malicious IP**
    - **Explanation**: If the destination IP is confirmed malicious, block it to prevent further suspicious activity.
    - **Example**: Adding 203.0.113.50 to the firewall block list.
2. **Secure Source IP**
    - **Explanation**: Ensure the source IP is secured to prevent further suspicious activity.
    - **Example**: Checking the security configuration and applying necessary patches on 192.168.1.10.
3. **Identify Other Suspicious Activity**
    - **Explanation**: Check if other systems exhibit similar suspicious network activity.
    - **Example**: Searching network logs for other instances of unusual data transfers.

6. Eradication

1. **Remove Malicious Access**
    - **Explanation**: Ensure any unauthorised access to the network is removed and the network is secured.
    - **Example**: Disabling any suspicious user accounts and changing credentials for all affected systems.
2. **Verify Integrity**
    - **Explanation**: Confirm that the network is secure and functioning correctly before reconnecting it to the network.
    - **Example**: Reviewing network logs and configurations to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
   - **Explanation**: Reconnect the cleaned and secured network to the organisation and monitor for any further issues.
   - **Example**: Reconnecting the network and monitoring for any signs of suspicious activity.
2. **Communication**
   - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
   - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Firewall Logs:

```
Jul 28 12:30:00 Firewall: Large data transfer detected from 192.168.1.10 to
203.0.113.50
Jul 28 12:30:05 Firewall: Data transfer allowed
```

Network Traffic Logs:

```
Jul 28 12:30:00 Network: Connection attempt from 192.168.1.10 to 203.0.113.50
Jul 28 12:30:05 Network: Data transfer of 500MB from 192.168.1.10 to 203.0.113.50
```

Example Alert 3: Brute-Force Attack Detected On Web Server

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand the source IP, target server, and the number of failed login attempts.
   - **Example**: Source IP: 198.51.100.25, Target Server: WebServer-01, Failed Attempts: 50, Time: 2024-07-28 14:45:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the potential impact of the brute-force attack.
   - **Example**: High-priority if the target server hosts sensitive applications or data.

2. Data Collection

1. **Gather Web Server Logs**
   - **Explanation**: Collect relevant logs from the affected web server to analyse the brute-force attack.
   - **Example Logs**:
     - **Authentication Logs**:

       ```
       Jul 28 14:45:00 WebServer-01: Failed login attempt for user admin from IP 198.51.100.25
       ```

2. **Analyse Attack Pattern**
   - **Explanation**: Use OSINT tools to gather information about the source IP and the attack pattern.
   - **Example**: Checking if 198.51.100.25 is known for brute-force attacks using OSINT tools like AbuseIPDB, AlienVault OTX, and Censys.

3. Initial Analysis

1. **Check Attack Duration**
   - **Explanation**: Determine the duration and intensity of the brute-force attack.
   - **Example**: Identifying if the attack is ongoing or if it was a one-time event.
2. **Assess Impact**
   - **Explanation**: Evaluate the potential impact of the brute-force attack on the target server and the organisation.
   - **Example**: Identifying if any user accounts were compromised during the attack.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**

   - **Explanation**: Use various OSINT tools to gather more information about the source IP and the nature of the brute-force attack.
   - **Example**:
     - **AbuseIPDB**: Check if the IP 198.51.100.25 is reported for brute-force attacks.
     - **AlienVault OTX**: Investigate if the IP address is part of a known attack campaign.
     - **Censys**: Examine the services and vulnerabilities associated with the source IP.
2. **Attack Pattern Analysis**
   - **Explanation**: Analyse the pattern of the brute-force attack to identify any anomalies.
   - **Example**: Reviewing the frequency and timing of the failed login attempts to detect any specific patterns.

5. Containment and Mitigation

1. **Block Malicious IP**
   - **Explanation**: If the source IP is confirmed malicious, block it to prevent further brute-force attempts.
   - **Example**: Adding 198.51.100.25 to the firewall block list.
2. **Enhance Authentication Security**
   - **Explanation**: Ensure the target server has strong authentication mechanisms to prevent brute-force attacks.
   - **Example**: Implementing multi-factor authentication (MFA) and account lockout policies on WebServer-01.
3. **Identify Other Targets**
   - **Explanation**: Check if other servers are targeted by the same brute-force attack.
   - **Example**: Searching authentication logs for other instances of failed login attempts from IP 198.51.100.25.

6. Eradication

1. **Remove Malicious Access**
   - **Explanation**: Ensure any unauthorised access resulting from the brute-force attack is removed and the server is secured.
   - **Example**: Disabling any suspicious user accounts and changing credentials for all affected systems.
2. **Verify Integrity**
   - **Explanation**: Confirm that the server is secure and functioning correctly before reconnecting it to the network.
   - **Example**: Reviewing server logs and configurations on WebServer-01 to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
    - **Explanation**: Reconnect the cleaned and secured server to the network and monitor for any further issues.
    - **Example**: Reconnecting WebServer-01 and monitoring for any signs of brute-force attacks.
2. **Communication**
    - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
    - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Authentication Logs:

```
Jul 28 14:45:00 WebServer-01: Failed login attempt for user admin from IP
198.51.100.25
Jul 28 14:45:05 WebServer-01: Failed login attempt for user admin from IP
198.51.100.25
```

Web Server Logs:

```
Jul 28 14:45:00 WebServer-01: Connection attempt from IP 198.51.100.25
Jul 28 14:45:05 WebServer-01: Multiple failed login attempts for user admin
```

Example Alert 4: Unauthorised Access To Critical File

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand which file was accessed, the user who accessed it, and the time of access.
   - **Example**: File: /etc/passwd, User: izzmier, Time: 2024-07-28 16:00:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the sensitivity of the accessed file and the potential impact.
   - **Example**: High-priority if the file contains sensitive information like user credentials.

2. Data Collection

1. **Gather File Access Logs**
   - **Explanation**: Collect relevant logs to analyse the unauthorised access.
   - **Example Logs**:
     - **System Logs**:

       ```
       Jul 28 16:00:00 Server-01: Unauthorised access attempt by user izzmier to file /etc/passwd
       ```

2. **Analyse User Actions**
   - **Explanation**: Use OSINT tools to gather information about the user and their previous activities.
   - **Example**: Checking if izzmier has any history of suspicious activity using OSINT tools like LinkedIn, social media profiles, and internal user behaviour analysis tools.

3. Initial Analysis

1. **Check User Permissions**
   - **Explanation**: Determine if the user should have access to the critical file.
   - **Example**: Verifying izzmier’s role and permissions to access /etc/passwd.
2. **Assess Access Impact**
   - **Explanation**: Evaluate the potential impact of the unauthorised access on the system and the organisation.
   - **Example**: Identifying if any sensitive information was accessed or modified.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**

    - **Explanation**: Use various OSINT tools to gather more information about the user and the accessed file.
    - **Example**:
        - **LinkedIn**: Verify izzmier’s job role and responsibilities.
        - **Social Media**: Check for any suspicious behaviour or posts indicating potential insider threats.
        - **Internal User Behaviour Analysis**: Review izzmier’s recent activities and access patterns.
2. **File Access Analysis**
    - **Explanation**: Analyse the accessed file to identify any unauthorised changes or data exfiltration.
    - **Example**: Reviewing file integrity and comparing it with previous versions to detect any modifications.

5. Containment and Mitigation

1. **Revoke Unauthorised Access**
    - **Explanation**: If the access is unauthorised, revoke the user's permissions to the critical file.
    - **Example**: Removing izzmier’s access to /etc/passwd.
2. **Enhance File Security**
    - **Explanation**: Ensure the critical file is secured with appropriate access controls and monitoring.
    - **Example**: Implementing file integrity monitoring and access controls for /etc/passwd.
3. **Identify Other Unauthorised Access**
    - **Explanation**: Check if other users have accessed the critical file without authorisation.
    - **Example**: Searching system logs for other unauthorised access attempts to /etc/passwd.

6. Eradication

1. **Remove Unauthorised Changes**
    - **Explanation**: Ensure any unauthorised changes to the critical file are removed and the file is restored to its original state.
    - **Example**: Restoring /etc/passwd from a secure backup.
2. **Verify File Integrity**
    - **Explanation**: Confirm that the critical file is secure and functioning correctly before allowing access.
    - **Example**: Reviewing file integrity and access controls to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**

    - **Explanation**: Ensure the system is secure and monitor for any further unauthorised access attempts.
    - **Example**: Reconnecting the system to the network and monitoring access to /etc/passwd.

2. **Communication**
    - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
    - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

System Logs:

```
Jul 28 16:00:00 Server-01: Unauthorised access attempt by user izzmier to file
/etc/passwd
Jul 28 16:00:05 Server-01: Access denied to file /etc/passwd for user izzmier
```

Access Control Logs:

```
Jul 28 16:00:00 Server-01: User izzmier attempted to access restricted file /etc/passwd
Jul 28 16:00:05 Server-01: User izzmier denied access to /etc/passwd
```

Example Alert 5: Data Exfiltration Detected

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand which data was exfiltrated, the source and destination IP addresses, and the time of detection.
   - **Example**: Data: Customer Database, Source IP: 192.168.1.15, Destination IP: 203.0.113.100, Time: 2024-07-28 18:00:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the sensitivity of the exfiltrated data and the potential impact.
   - **Example**: High-priority if the data includes sensitive customer information.

2. Data Collection

1. **Gather Network Logs**
   - **Explanation**: Collect relevant network logs to analyse the data exfiltration.
   - **Example Logs**:
     - **Firewall Logs**:

       ```
       Jul 28 18:00:00 Firewall: Large data transfer detected from
       192.168.1.15 to 203.0.113.100
       ```

2. **Analyse Exfiltration Path**
   - **Explanation**: Use OSINT tools to gather information about the destination IP and the nature of the exfiltrated data.
   - **Example**: Checking if 203.0.113.100 is known for receiving exfiltrated data using OSINT tools like Shodan, IPinfo, and AbuseIPDB.

3. Initial Analysis

1. **Check User Actions**
   - **Explanation**: Determine if the user on the source IP performed any actions that led to the data exfiltration.
   - **Example**: Checking if the user on 192.168.1.15 intentionally transferred the data or if it was automated.
2. **Assess Exfiltration Impact**
   - **Explanation**: Evaluate the potential impact of the data exfiltration on the organisation.
   - **Example**: Identifying if any sensitive customer information was transferred to the destination IP.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**
   - **Explanation**: Use various OSINT tools to gather more information about the destination IP and the nature of the exfiltrated data.
   - **Example**:
     - **Shodan**: Investigate if the IP 203.0.113.100 has open ports or is associated with known malicious activity.
     - **IPinfo**: Check the geolocation and ownership details of the IP address.
     - **AbuseIPDB**: Verify if the IP address is reported for abusive activities.
2. **Network Traffic Analysis**
   - **Explanation**: Analyse the network traffic involved in the data exfiltration to identify any anomalies.
   - **Example**: Reviewing the payload of the data transfer to detect any signs of malicious content.

5. Containment and Mitigation

1. **Block Malicious IP**
   - **Explanation**: If the destination IP is confirmed malicious, block it to prevent further data exfiltration.
   - **Example**: Adding 203.0.113.100 to the firewall block list.
2. **Secure Source IP**
   - **Explanation**: Ensure the source IP is secured to prevent further data exfiltration.
   - **Example**: Checking the security configuration and applying necessary patches on 192.168.1.15.
3. **Identify Other Data Exfiltration Attempts**
   - **Explanation**: Check if other systems are involved in data exfiltration.
   - **Example**: Searching network logs for other instances of unusual data transfers.

6. Eradication

1. **Remove Malicious Access**
   - **Explanation**: Ensure any unauthorised access to the network is removed and the network is secured.
   - **Example**: Disabling any suspicious user accounts and changing credentials for all affected systems.
2. **Verify Data Integrity**
   - **Explanation**: Confirm that the exfiltrated data is secure and functioning correctly before allowing access.
   - **Example**: Reviewing network logs and configurations to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
   - **Explanation**: Reconnect the cleaned and secured network to the organisation and monitor for any further issues.
   - **Example**: Reconnecting the network and monitoring for any signs of data exfiltration.
2. **Communication**
   - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
   - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Firewall Logs:

```
Jul 28 18:00:00 Firewall: Large data transfer detected from 192.168.1.15 to
203.0.113.100
Jul 28 18:00:05 Firewall: Data transfer allowed
```

Network Traffic Logs:

```
Jul 28 18:00:00 Network: Connection attempt from 192.168.1.15 to 203.0.113.100
Jul 28 18:00:05 Network: Data transfer of 1GB from 192.168.1.15 to 203.0.113.100
```

Example Alert 6: Brute Force Attack Detected

1. Initial Alert Triage

1. **Review Alert Details**
    - **Explanation**: Examine the alert to understand the source IP, target system, and the number of failed login attempts.
    - **Example**: Source IP: 198.51.100.25, Target System: DB-Server, Failed Attempts: 100, Time: 2024-07-28 20:00:00.
2. **Prioritise the Alert**
    - **Explanation**: Assess the criticality based on the potential impact of the brute-force attack.
    - **Example**: High-priority if the target system hosts critical applications or data.

2. Data Collection

1. **Gather System Logs**
    - **Explanation**: Collect relevant logs to analyse the brute-force attack.
    - **Example Logs**:
        - **Authentication Logs**:

          ```
          Jul 28 20:00:00 DB-Server: Failed login attempt for user admin from IP 198.51.100.25
          ```

2. **Analyse Attack Pattern**
    - **Explanation**: Use OSINT tools to gather information about the source IP and the attack pattern.
    - **Example**: Checking if 198.51.100.25 is known for brute-force attacks using OSINT tools like AbuseIPDB, AlienVault OTX, and Censys.

3. Initial Analysis

1. **Check Attack Duration**
    - **Explanation**: Determine the duration and intensity of the brute-force attack.
    - **Example**: Identifying if the attack is ongoing or if it was a one-time event.
2. **Assess Impact**
    - **Explanation**: Evaluate the potential impact of the brute-force attack on the target system and the organisation.
    - **Example**: Identifying if any user accounts were compromised during the attack.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**

    - **Explanation**: Use various OSINT tools to gather more information about the source IP and the nature of the brute-force attack.
    - **Example**:
        - **AbuseIPDB**: Check if the IP 198.51.100.25 is reported for brute-force attacks.
        - **AlienVault OTX**: Investigate if the IP address is part of a known attack campaign.
        - **Censys**: Examine the services and vulnerabilities associated with the source IP.
2. **Attack Pattern Analysis**
    - **Explanation**: Analyse the pattern of the brute-force attack to identify any anomalies.
    - **Example**: Reviewing the frequency and timing of the failed login attempts to detect any specific patterns.

5. Containment and Mitigation

1. **Block Malicious IP**
    - **Explanation**: If the source IP is confirmed malicious, block it to prevent further brute-force attempts.
    - **Example**: Adding 198.51.100.25 to the firewall block list.
2. **Enhance Authentication Security**
    - **Explanation**: Ensure the target system has strong authentication mechanisms to prevent brute-force attacks.
    - **Example**: Implementing multi-factor authentication (MFA) and account lockout policies on DB-Server.
3. **Identify Other Targets**
    - **Explanation**: Check if other systems are targeted by the same brute-force attack.
    - **Example**: Searching authentication logs for other instances of failed login attempts from IP 198.51.100.25.

6. Eradication

1. **Remove Malicious Access**
    - **Explanation**: Ensure any unauthorised access resulting from the brute-force attack is removed and the system is secured.
    - **Example**: Disabling any suspicious user accounts and changing credentials for all affected systems.
2. **Verify Integrity**
    - **Explanation**: Confirm that the system is secure and functioning correctly before reconnecting it to the network.
    - **Example**: Reviewing system logs and configurations on DB-Server to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
   - **Explanation**: Reconnect the cleaned and secured system to the network and monitor for any further issues.
   - **Example**: Reconnecting DB-Server and monitoring for any signs of brute-force attacks.
2. **Communication**
   - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
   - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Authentication Logs:

```
Jul 28 20:00:00 DB-Server: Failed login attempt for user admin from IP 198.51.100.25
Jul 28 20:00:05 DB-Server: Failed login attempt for user admin from IP 198.51.100.25
```

System Logs

```
Jul 28 20:00:00 DB-Server: Connection attempt from IP 198.51.100.25
Jul 28 20:00:05 DB-Server: Multiple failed login attempts for user admin
```

Example Alert 7: Phishing Email Detected

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand the source email, recipient, and the time of detection.
   - **Example**: Source Email: attacker@example.com, Recipient: iffah@example.com, Time: 2024-07-28 22:00:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the potential impact of the phishing email.
   - **Example**: High-priority if the email targets high-level executives or contains links to malicious sites.

2. Data Collection

1. **Gather Email Logs**
   - **Explanation**: Collect relevant email logs to analyse the phishing email.
   - **Example Logs**:
     - **Email Server Logs**:

       ```
       Jul 28 22:00:00 EmailServer: Received email from
       attacker@example.com to iffah@example.com
       ```

2. **Analyse Email Content**
   - **Explanation**: Use OSINT tools to gather information about the phishing email and the sender.
   - **Example**: Checking if attacker@example.com is known for phishing attacks using OSINT tools like PhishTank, VirusTotal, and DomainTools.

3. Initial Analysis

1. **Check Email Headers**
   - **Explanation**: Analyse the email headers to verify the authenticity of the sender and detect any spoofing attempts.
   - **Example**: Reviewing the email headers to identify any anomalies in the sender's domain.
2. **Assess Impact**
   - **Explanation**: Evaluate the potential impact of the phishing email on the recipient and the organisation.
   - **Example**: Identifying if the email contains malicious links or attachments that could compromise the recipient's account.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**

   - **Explanation**: Use various OSINT tools to gather more information about the phishing email and the sender.
   - **Example**:
     - **PhishTank**: Check if the email domain or links are reported for phishing.
     - **VirusTotal**: Analyse email attachments for any malicious content.
     - **DomainTools**: Investigate the domain associated with the sender's email address.
2. **Email Content Analysis**
   - **Explanation**: Analyse the content of the phishing email to identify any social engineering tactics or malicious intent.
   - **Example**: Reviewing the email body for any suspicious links, attachments, or requests for sensitive information.

5. Containment and Mitigation

1. **Block Malicious Sender**
   - **Explanation**: If the sender is confirmed malicious, block the email address to prevent further phishing attempts.
   - **Example**: Adding attacker@example.com to the email server block list.
2. **Enhance Email Security**
   - **Explanation**: Ensure the email server has strong security mechanisms to detect and block phishing emails.
   - **Example**: Implementing email filtering, anti-phishing software, and employee training on recognising phishing emails.
3. **Identify Other Phishing Emails**
   - **Explanation**: Check if other employees received similar phishing emails.
   - **Example**: Searching email logs for other instances of emails from attacker@example.com.

6. Eradication

1. **Remove Malicious Emails**
   - **Explanation**: Ensure any malicious emails are removed from the email server and the recipients' inboxes.
   - **Example**: Deleting any phishing emails from attacker@example.com in the email server and recipient's inboxes.
2. **Verify Email Server Security**
   - **Explanation**: Confirm that the email server is secure and functioning correctly before allowing normal email traffic.
   - **Example**: Reviewing email server logs and configurations to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**

  - **Explanation**: Reconnect the cleaned and secured email server to the network and monitor for any further issues.
  - **Example**: Reconnecting the email server and monitoring for any signs of phishing emails.
2. **Communication**
   - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
   - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Email Server Logs:

```
Jul 28 22:00:00 EmailServer: Received email from attacker@example.com to
iffah@example.com
Jul 28 22:00:05 EmailServer: Email marked as phishing
```

Email Headers:

```
Received: from attacker@example.com
  by EmailServer.example.com
  with SMTP id 12345
  for <iffah@example.com>;
  Mon, 28 Jul 2024 22:00:00 +0000
Subject: Urgent: Account Verification Required
From: "Support Team" <attacker@example.com>
To: iffah@example.com
```

Example Alert 8: Suspicious File Download Detected

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand the source, file details, and the time of detection.
   - **Example**: Source IP: 192.168.1.50, File: malicious.exe, Time: 2024-07-28 10:00:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the nature of the file and its potential impact.
   - **Example**: High-priority if the file is known to be associated with malware or other malicious activities.

2. Data Collection

1. **Gather Download Logs**
   - **Explanation**: Collect relevant logs to analyse the suspicious file download.
   - **Example Logs**:
     - **Web Server Logs**:

       ```
       Jul 28 10:00:00 WebServer: Download of malicious.exe from 192.168.1.50
       ```

2. **Analyse File Properties**
   - **Explanation**: Use OSINT tools to gather information about the suspicious file.
   - **Example**: Checking the file hash against VirusTotal and other malware databases.

3. Initial Analysis

1. **Check File Hash**
   - **Explanation**: Analyse the file hash to identify if it is known malware.
   - **Example**: Using VirusTotal to check the hash of malicious.exe.
2. **Assess Impact**
   - **Explanation**: Evaluate the potential impact of the downloaded file on the system and the organisation.
   - **Example**: Identifying if the file has executed and caused any damage.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**
   - **Explanation**: Use various OSINT tools to gather more information about the file and its behaviour.

   - **Example**:
      - **VirusTotal**: Check if the file hash is reported as malicious.
      - **Hybrid Analysis**: Analyse the file's behaviour in a sandbox environment.
      - **MalwareBazaar**: Investigate if the file is part of a known malware campaign.
2. **File Behaviour Analysis**
   - **Explanation**: Analyse the behaviour of the suspicious file to detect any malicious activity.
   - **Example**: Reviewing sandbox analysis results to understand what the file does when executed.

5. Containment and Mitigation

1. **Quarantine the File**
   - **Explanation**: If the file is confirmed malicious, quarantine it to prevent execution.
   - **Example**: Moving malicious.exe to a secure quarantine area.
2. **Enhance Endpoint Security**
   - **Explanation**: Ensure the endpoint has strong security mechanisms to detect and block malicious files.
   - **Example**: Implementing antivirus and anti-malware solutions on 192.168.1.50.
3. **Identify Other Downloads**
   - **Explanation**: Check if other systems downloaded the same or similar suspicious files.
   - **Example**: Searching web server logs for other instances of malicious.exe downloads.

6. Eradication

1. **Remove Malicious Files**
   - **Explanation**: Ensure any malicious files are removed from the endpoint and the network.
   - **Example**: Deleting malicious.exe from 192.168.1.50 and any other affected systems.
2. **Verify System Integrity**
   - **Explanation**: Confirm that the system is secure and functioning correctly before allowing normal operations.
   - **Example**: Reviewing system logs and configurations on 192.168.1.50 to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
   - **Explanation**: Reconnect the cleaned and secured system to the network and monitor for any further issues.

    - **Example**: Reconnecting 192.168.1.50 and monitoring for any signs of suspicious file downloads.

2. **Communication**
    - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
    - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Web Server Logs:

```
Jul 28 10:00:00 WebServer: Download of malicious.exe from 192.168.1.50
Jul 28 10:00:05 WebServer: File download completed
```

Endpoint Logs:

```
Jul 28 10:00:00 Endpoint: File download initiated for malicious.exe
Jul 28 10:00:05 Endpoint: File download completed for malicious.exe
```

Example Alert 9: Unusual Network Activity Detected

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand the nature of the unusual activity, source and destination IPs, and the time of detection.
   - **Example**: Source IP: 192.168.1.100, Destination IP: 203.0.113.5, Activity: High volume of traffic, Time: 2024-07-28 12:00:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the potential impact of the unusual activity.
   - **Example**: High-priority if the activity suggests a potential data exfiltration or DDoS attack.

2. Data Collection

1. **Gather Network Logs**
   - **Explanation**: Collect relevant logs to analyse the unusual network activity.
   - **Example Logs**:
     - **Firewall Logs**:

       ```
       Jul 28 12:00:00 Firewall: High volume of traffic from 192.168.1.100 to 203.0.113.5
       ```
2. **Analyse Traffic Patterns**
   - **Explanation**: Use OSINT tools to gather information about the network activity and the involved IPs.
   - **Example**: Checking if 203.0.113.5 is associated with any known malicious activities using OSINT tools like Shodan, Censys, and GreyNoise.

3. Initial Analysis

1. **Check Traffic Volume**
   - **Explanation**: Analyse the volume and duration of the network activity to identify if it is truly unusual.
   - **Example**: Reviewing network logs to determine if the traffic volume is abnormal compared to baseline activity.
2. **Assess Impact**
   - **Explanation**: Evaluate the potential impact of the unusual network activity on the system and the organisation.
   - **Example**: Identifying if the activity caused any disruptions or data breaches.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**
   - **Explanation**: Use various OSINT tools to gather more information about the network activity and the involved IPs.
   - **Example**:
     - **Shodan**: Investigate the destination IP 203.0.113.5 for any known vulnerabilities or malicious activities.
     - **Censys**: Examine the services and configurations associated with the destination IP.
     - **GreyNoise**: Check if the source IP 192.168.1.100 is involved in any known scanning or attack activities.
2. **Traffic Pattern Analysis**
   - **Explanation**: Analyse the pattern of the network activity to detect any anomalies or malicious intent.
   - **Example**: Reviewing traffic flow and behaviour to understand if the activity is consistent with a known attack pattern.

5. Containment and Mitigation

1. **Block Malicious IPs**
   - **Explanation**: If the involved IPs are confirmed malicious, block them to prevent further unusual activity.
   - **Example**: Adding 203.0.113.5 to the firewall block list.
2. **Enhance Network Security**
   - **Explanation**: Ensure the network has strong security mechanisms to detect and block unusual activities.
   - **Example**: Implementing network intrusion detection systems (NIDS) and monitoring tools.
3. **Identify Other Unusual Activities**
   - **Explanation**: Check if other systems are experiencing similar unusual network activity.
   - **Example**: Searching network logs for other instances of high-volume traffic to 203.0.113.5.

6. Eradication

1. **Remove Malicious Connections**
   - **Explanation**: Ensure any malicious connections resulting from the unusual activity are terminated.
   - **Example**: Terminating any ongoing connections between 192.168.1.100 and 203.0.113.5.
2. **Verify Network Integrity**
   - **Explanation**: Confirm that the network is secure and functioning correctly before allowing normal operations.
   - **Example**: Reviewing network logs and configurations to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
    - **Explanation**: Reconnect the cleaned and secured network to normal operations and monitor for any further issues.
    - **Example**: Restoring network connectivity and monitoring for any signs of unusual activity.
2. **Communication**
    - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
    - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Firewall Logs:

```
Jul 28 12:00:00 Firewall: High volume of traffic from 192.168.1.100 to 203.0.113.5
Jul 28 12:00:05 Firewall: Traffic continued at high volume
```

Network Logs:

```
Jul 28 12:00:00 Network: Unusual network activity detected from 192.168.1.100 to
203.0.113.5
Jul 28 12:00:05 Network: Activity persists at high volume
```

Example Alert 10: Unauthorised Access Attempt Detected

1. Initial Alert Triage

1. **Review Alert Details**
   - **Explanation**: Examine the alert to understand the source, targeted system, and the time of detection.
   - **Example**: Source IP: 192.168.1.150, Target System: FileServer, Time: 2024-07-28 14:00:00.
2. **Prioritise the Alert**
   - **Explanation**: Assess the criticality based on the nature of the access attempt and the potential impact.
   - **Example**: High-priority if the targeted system contains sensitive data or critical infrastructure.

2. Data Collection

1. **Gather Access Logs**
   - **Explanation**: Collect relevant logs to analyse the unauthorised access attempt.
   - **Example Logs**:
     - **File Server Logs**:

       ```
       Jul 28 14:00:00 FileServer: Unauthorised access attempt from
       192.168.1.150
       ```

2. **Analyse User Activity**
   - **Explanation**: Use OSINT tools to gather information about the source of the access attempt.
   - **Example**: Checking if 192.168.1.150 is associated with any known malicious activities using OSINT tools like Shodan, Censys, and GreyNoise.

3. Initial Analysis

1. **Check Access Patterns**
   - **Explanation**: Analyse the access patterns to identify if it is truly unauthorised.
   - **Example**: Reviewing access logs to determine if the attempt was outside normal user behaviour.
2. **Assess Impact**
   - **Explanation**: Evaluate the potential impact of the unauthorised access attempt on the system and the organisation.
   - **Example**: Identifying if the attempt caused any disruptions or data breaches.

4. Deep Dive Analysis

1. **OSINT Tools for Investigation**
    - **Explanation**: Use various OSINT tools to gather more information about the source IP and its activities.
    - **Example**:
        - **Shodan**: Investigate the source IP 192.168.1.150 for any known vulnerabilities or malicious activities.
        - **Censys**: Examine the services and configurations associated with the source IP.
        - **GreyNoise**: Check if the source IP 192.168.1.150 is involved in any known scanning or attack activities.
2. **Access Pattern Analysis**
    - **Explanation**: Analyse the pattern of the access attempt to detect any anomalies or malicious intent.
    - **Example**: Reviewing access logs and behaviour to understand if the attempt is consistent with a known attack pattern.

5. Containment and Mitigation

1. **Block Malicious IPs**
    - **Explanation**: If the source IP is confirmed malicious, block it to prevent further unauthorised access attempts.
    - **Example**: Adding 192.168.1.150 to the firewall block list.
2. **Enhance System Security**
    - **Explanation**: Ensure the targeted system has strong security mechanisms to detect and block unauthorised access attempts.
    - **Example**: Implementing multi-factor authentication and monitoring tools on FileServer.
3. **Identify Other Unauthorised Attempts**
    - **Explanation**: Check if other systems are experiencing similar unauthorised access attempts.
    - **Example**: Searching access logs for other instances of attempts from 192.168.1.150.

6. Eradication

1. **Remove Malicious Connections**
    - **Explanation**: Ensure any malicious connections resulting from the unauthorised access attempt are terminated.
    - **Example**: Terminating any ongoing connections between FileServer and 192.168.1.150.
2. **Verify System Integrity**
    - **Explanation**: Confirm that the system is secure and functioning correctly before allowing normal operations.
    - **Example**: Reviewing system logs and configurations to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
   - **Explanation**: Reconnect the cleaned and secured system to normal operations and monitor for any further issues.
   - **Example**: Restoring access to FileServer and monitoring for any signs of unauthorised access attempts.
2. **Communication**
   - **Explanation**: Inform relevant stakeholders about the incident and the remediation steps taken.
   - **Example**: Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

File Server Logs:

```
Jul 28 14:00:00 FileServer: Unauthorised access attempt from 192.168.1.150
Jul 28 14:00:05 FileServer: Access denied to 192.168.1.150
```

Firewall Logs:

```
Jul 28 14:00:00 Firewall: Blocked access attempt from 192.168.1.150 to FileServer
Jul 28 14:00:05 Firewall: Continued block on 192.168.1.150
```

SIMULATION

Simulation Alert: Suspicious Network Activity Detected

1. Initial Alert Triage

   1. **Review Alert Details**
      - **Source IP**: 192.168.1.50
      - **Destination IP**: 203.0.113.5
      - **Activity**: High volume of outbound traffic
      - **Time**: 2024-07-28 10:00:00
   2. **Prioritise the Alert**
      - High priority due to potential data exfiltration or communication with a command and control server.

2. Data Collection

   1. **Gather Network Logs**
      - **Logs**:

        ```
        Jul 28 10:00:00 Firewall: High volume of traffic from 192.168.1.50 to 203.0.113.5
        Jul 28 10:00:05 Firewall: Continued high volume of traffic from 192.168.1.50 to 203.0.113.5
        ```

   2. **Analyse Traffic Patterns**
      - Use OSINT tools to gather information about the destination IP (203.0.113.5).

3. Initial Analysis

   1. **Check Traffic Volume**
      - Normal outbound traffic is usually below 100 MB/hr; current traffic is 1 GB/hr.
   2. **Assess Impact**
      - Determine if any sensitive data was transferred.

4. Deep Dive Analysis

   1. **OSINT Tools for Investigation**
      - **VirusTotal**: The IP 203.0.113.5 is associated with a known command and control server.
      - **Shodan**: The IP has ports 80 and 443 open, indicating possible web services.
      - **GreyNoise**: The source IP 192.168.1.50 is not involved in any known malicious activities.
   2. **Traffic Pattern Analysis**

  - The traffic consists mainly of large data transfers over HTTP and HTTPS.

5. Containment and Mitigation

1. **Block Malicious IPs**
   - Add 203.0.113.5 to the firewall block list.
2. **Enhance Network Security**
   - Implement network intrusion detection systems (NIDS) and additional monitoring tools.
3. **Identify Other Unusual Activities**
   - Searching network logs for other instances of high-volume traffic to 203.0.113.5.

6. Eradication

1. **Remove Malicious Connections**
   - Terminate any ongoing connections between 192.168.1.50 and 203.0.113.5.
2. **Verify Network Integrity**
   - Reviewing network logs and configurations to ensure there are no remaining issues.

7. Recovery

1. **Restore Operations**
   - Restoring network connectivity and monitoring for any signs of unusual activity.
2. **Communication**
   - Providing a detailed incident report to the IT and security teams, outlining the steps taken and any improvements made.

Raw Logs for Easy Understanding

Firewall Logs:

```
Jul 28 10:00:00 Firewall: High volume of traffic from 192.168.1.50 to 203.0.113.5
Jul 28 10:00:05 Firewall: Continued high volume of traffic from 192.168.1.50 to 203.0.113.5
Jul 28 10:00:10 Firewall: Blocked traffic from 192.168.1.50 to 203.0.113.5
```

Network Logs:

```
Jul 28 10:00:00 Network: Unusual network activity detected from 192.168.1.50 to 203.0.113.5
Jul 28 10:00:05 Network: Activity persists at high volume
Jul 28 10:00:10 Network: Blocked traffic from 192.168.1.50 to 203.0.113.5
```

OSINT Tools Results

1. **VirusTotal**
   - **Query**: 203.0.113.5
   - **Result**: IP associated with a known command and control server.
2. **Shodan**
   - **Query**: 203.0.113.5
   - **Result**: Ports 80 and 443 open.
3. **GreyNoise**
   - **Query**: 192.168.1.50
   - **Result**: No known malicious activities.

Isolation Steps

1. **Block the Malicious IP**
   - **Firewall Rule**: Add a rule to block traffic to and from 203.0.113.5.

     ```
     iptables -A INPUT -s 203.0.113.5 -j DROP
     iptables -A OUTPUT -d 203.0.113.5 -j DROP
     ```

2. **Terminate Ongoing Connections**
   - **Command**: Terminate any active sessions between 192.168.1.50 and 203.0.113.5.

     ```
     netstat -an | grep 203.0.113.5
     kill <PID>
     ```

Root Cause Analysis (RCA)

Incident Summary: On July 28, 2024, at 10:00:00, a suspicious network activity alert was triggered due to a high volume of outbound traffic from 192.168.1.50 to 203.0.113.5, suggesting potential data exfiltration or communication with a command and control server.

Root Cause

1. **Compromised Endpoint**
   - **Source**: The endpoint with IP 192.168.1.50 was compromised, possibly due to malware infection.
   - **Mechanism**: The compromised endpoint began communicating with a known command and control server at 203.0.113.5.
2. **Data Exfiltration**
   - **Impact**: High volume of data being transferred, indicating possible data exfiltration.

Contributing Factors

1. **Insufficient Endpoint Security**

   - Lack of advanced endpoint protection may have allowed the malware to compromise the system.
2. **Delayed Detection**
   - The suspicious activity was detected after a significant volume of data had already been transferred.

Corrective Actions

1. **Improve Endpoint Security**
   - **Action**: Deploy advanced endpoint protection solutions and conduct regular security audits.
   - **Timeline**: Immediate and ongoing.
2. **Enhance Network Monitoring**
   - **Action**: Implement network intrusion detection systems (NIDS) and continuous network traffic analysis.
   - **Timeline**: Immediate and ongoing.
3. **Conduct Security Awareness Training**
   - **Action**: Provide regular training to employees on recognising and responding to phishing attempts and other attack vectors.
   - **Timeline**: Quarterly.

Preventive Measures

1. **Regular Security Audits**
   - Conduct regular security audits and penetration testing to identify and mitigate vulnerabilities.
2. **Continuous Monitoring and Response**
   - Implement a continuous monitoring and incident response strategy to quickly detect and respond to suspicious activities.
3. **Update and Patch Management**
   - Ensure all systems and applications are regularly updated and patched to protect against known vulnerabilities.