HANDLING & IDENTIFYING FALSE POSITIVE ALERTS

BY IZZMIER IZZUDDIN

False Positive Detection 1: Suspicious PowerShell Activity

1. Detection

Example Alert:

Alert Name: Suspicious PowerShell Activity
Source: SIEM System
Time: 2023-06-15 12:34:56 UTC
Severity: High
Description: Detected execution of a PowerShell script on a user workstation, which matches a pattern commonly used in malicious activities.

2. Initial Triage

Steps:

1. **Receive and Acknowledge Alert**:
   - **Action**: Confirm receipt of the alert in the SIEM system.
   - **Responsible**: SOC Analyst.
2. **Preliminary Analysis**:
   - **Review Alert Details**: Examine the alert's metadata (time, source IP, user account, script details).
   - **Correlate with Other Alerts**: Check if similar alerts have been triggered recently.
   - **Determine Severity and Priority**: Based on the criticality of the affected system and potential impact.

Example Analysis:

- **Source Host**: 192.168.1.20 (internal IP of a user workstation).
- **User Account**: izzmier@manchesterunited.com.
- **Script Details**: PowerShell script attempting to access a network share and modify files.
- **Recent Alerts**: No other similar alerts from this host or user account.

3. Containment

Steps:

1. **Isolate Affected Systems** (if deemed necessary):
   - **Action**: Monitor the system closely but do not isolate yet to avoid disrupting normal operations.
   - **Responsible**: SOC Analyst.
2. **Check for Immediate Threats**:
   - **Action**: Verify if there are any immediate signs of compromise or ongoing malicious activity.
   - **Responsible**: SOC Analyst.

4. Investigation

Steps:

1. **Collect Evidence**:
    - **Action**: Gather logs from the SIEM, EDR, and network monitoring tools related to the PowerShell activity.
    - **Responsible**: SOC Analyst.
2. **Analyse Logs**:
    - **Check User Activity**: Determine if the user, izzmier, has a legitimate reason for running the script.
    - **Correlate with Threat Intelligence**: Verify if the script or behaviour matches any known malicious activity patterns.

Example Investigation:

- **Logs**: Showed that the PowerShell script was executed manually by izzmier during normal working hours.
- **User Activity**: Verified that izzmier is part of the IT department, which often runs scripts for maintenance tasks.
- **Script Analysis**: The script in question is a standard maintenance script used to update software on networked machines.
- **Threat Intelligence**: No matches found for the script content or behaviour in known malicious activity databases.

5. Eradication (if necessary)

Steps:

1. **Remove Malicious Artifacts** (if any are found):
    - **Action**: Scan the system for malware or unauthorized changes and remove any identified threats.
    - **Responsible**: SOC Analyst/IR Team.
2. **Patch and Update Systems** (if applicable):
    - **Action**: Ensure the system is fully patched and updated to prevent exploitation of known vulnerabilities.
    - **Responsible**: IT Support.

Example Eradication:

- **System Scan**: Confirmed no malicious artifacts or unauthorized changes were present.
- **Patching**: No additional action required as the system was already up-to-date.

6. Recovery

Steps:

1. **Restore Systems to Operational State** (if any actions were taken):

   - **Action**: No restoration needed as no isolation or significant changes were made.
   - **Responsible**: IT Support.
2. **Monitor for Recurrence**:
   - **Action**: Set up enhanced monitoring on the user account and similar script activities for the next 48 hours.
   - **Responsible**: SOC Analyst.

Example Recovery:

- **Enhanced Monitoring**: Activated for the next 48 hours on the user account and PowerShell activities.

7. Post-Incident Activity

Steps:

1. **Conduct a Post-Mortem**:
   - **Action**: Review the incident, determine why it was flagged as suspicious, and what can be improved to reduce false positives.
   - **Responsible**: IR Team.
2. **Update Documentation**:
   - **Action**: Update the playbooks and knowledge base with findings from the incident.
   - **Responsible**: SOC Analyst.
3. **User Awareness Training**:
   - **Action**: Inform the IT department about the incident and reinforce proper documentation and notification practices for maintenance scripts.
   - **Responsible**: IT Support/Security Awareness Team.

Example Post-Incident Activity:

- **Post-Mortem Meeting**: 2023-06-16 10:00:00 UTC.
- **Documentation Updated**: Incident report added to the knowledge base.
- **User Training**: Conducted a session with the IT department to ensure proper documentation of maintenance activities and communication with the SOC.

False Positive Detection 2: Unusual Outbound Traffic

1. Detection

Example Alert:
Alert Name: Unusual Outbound Traffic
Source: Network Monitoring Tool
Time: 2023-06-15 14:22:45 UTC
Severity: Medium
Description: Detected unusual outbound traffic from a workstation to an external IP address not commonly accessed by internal systems.

2. Initial Triage

Steps:

1. **Receive and Acknowledge Alert**:
   - **Action**: Confirm receipt of the alert in the SIEM system.
   - **Responsible**: SOC Analyst.
2. **Preliminary Analysis**:
   - **Review Alert Details**: Examine the alert’s metadata (time, source IP, destination IP, traffic type).
   - **Correlate with Other Alerts**: Check if similar alerts have been triggered recently.
   - **Determine Severity and Priority**: Based on the criticality of the affected system and potential impact.

Example Analysis:

- **Source Host**: 192.168.1.30 (internal IP of a user workstation).
- **Destination Host**: 198.51.100.12 (external IP).
- **Traffic Type**: HTTP traffic.
- **Recent Alerts**: No other similar alerts from this host.

3. Containment

Steps:

1. **Isolate Affected Systems** (if deemed necessary):
   - **Action**: Monitor the system closely but do not isolate yet to avoid disrupting normal operations.
   - **Responsible**: SOC Analyst.
2. **Check for Immediate Threats**:
   - **Action**: Verify if there are any immediate signs of compromise or ongoing malicious activity.
   - **Responsible**: SOC Analyst.

4. Investigation

Steps:

1. **Collect Evidence**:
   - **Action**: Gather logs from the SIEM, network monitoring tools, and check browser history on the workstation.
   - **Responsible**: SOC Analyst.
2. **Analyse Logs**:
   - **Check User Activity**: Determine if the user, izzmier, has a legitimate reason for accessing the external IP.
   - **Correlate with Threat Intelligence**: Verify if the external IP or traffic matches any known malicious activity patterns.

Example Investigation:

- **Logs**: Showed HTTP traffic from 192.168.1.30 to 198.51.100.12, consisting of data uploads.
- **User Activity**: Verified that izzmier is a marketing employee who recently uploaded files to a new third-party service for a project.
- **Traffic Analysis**: Confirmed the external IP belongs to a legitimate file-sharing service recently used by the marketing department.
- **Threat Intelligence**: No matches found for the external IP or traffic behaviour in known malicious activity databases.

5. Eradication (if necessary)

Steps:

1. **Remove Malicious Artifacts** (if any are found):
   - **Action**: Scan the system for malware or unauthorized changes and remove any identified threats.
   - **Responsible**: SOC Analyst/IR Team.
2. **Patch and Update Systems** (if applicable):
   - **Action**: Ensure the system is fully patched and updated to prevent exploitation of known vulnerabilities.
   - **Responsible**: IT Support.

Example Eradication:

- **System Scan**: Confirmed no malicious artifacts or unauthorized changes were present.
- **Patching**: No additional action required as the system was already up-to-date.

6. Recovery

Steps:

1. **Restore Systems to Operational State** (if any actions were taken):
   - **Action**: No restoration needed as no isolation or significant changes were made.
   - **Responsible**: IT Support.

2. **Monitor for Recurrence**:
    - **Action**: Set up enhanced monitoring on the user account and similar outbound traffic activities for the next 48 hours.
    - **Responsible**: SOC Analyst.

Example Recovery:

- **Enhanced Monitoring**: Activated for the next 48 hours on the user account and HTTP traffic.

7. Post-Incident Activity

Steps:

1. **Conduct a Post-Mortem**:
    - **Action**: Review the incident, determine why it was flagged as suspicious, and what can be improved to reduce false positives.
    - **Responsible**: IR Team.
2. **Update Documentation**:
    - **Action**: Update the playbooks and knowledge base with findings from the incident.
    - **Responsible**: SOC Analyst.
3. **User Awareness Training**:
    - **Action**: Inform the marketing department about the incident and reinforce proper documentation and notification practices for using new third-party services.
    - **Responsible**: IT Support/Security Awareness Team.

Example Post-Incident Activity:

- **Post-Mortem Meeting**: 2023-06-16 10:00:00 UTC.
- **Documentation Updated**: Incident report added to the knowledge base.
- **User Training**: Conducted a session with the marketing department to ensure proper documentation of third-party service usage and communication with the SOC.

False Positive Detection 3: Possible Data Exfiltration

1. Detection

Example Alert:
Alert Name: Possible Data Exfiltration
Source: SIEM System
Time: 2023-06-15 15:12:30 UTC
Severity: High
Description: Detected large volumes of data being transferred from an internal server to an external IP address.

2. Initial Triage

Steps:

1. **Receive and Acknowledge Alert**:
   - **Action**: Confirm receipt of the alert in the SIEM system.
   - **Responsible**: SOC Analyst.
2. **Preliminary Analysis**:
   - **Review Alert Details**: Examine the alert's metadata (time, source IP, destination IP, data volume).
   - **Correlate with Other Alerts**: Check if similar alerts have been triggered recently.
   - **Determine Severity and Priority**: Based on the criticality of the affected system and potential impact.

Example Analysis:

- **Source Host**: 10.10.10.50 (internal server).
- **Destination Host**: 203.0.113.99 (external IP).
- **Data Volume**: 5 GB transferred within a short period.
- **Recent Alerts**: No other similar alerts from this host.

3. Containment

Steps:

1. **Isolate Affected Systems** (if deemed necessary):
   - **Action**: Monitor the server closely but do not isolate yet to avoid disrupting normal operations.
   - **Responsible**: SOC Analyst.
2. **Check for Immediate Threats**:
   - **Action**: Verify if there are any immediate signs of compromise or ongoing malicious activity.
   - **Responsible**: SOC Analyst.

4. Investigation

Steps:

1. **Collect Evidence**:
   - **Action**: Gather logs from the SIEM, EDR, and network monitoring tools related to the data transfer.
   - **Responsible**: SOC Analyst.
2. **Analyse Logs**:
   - **Check User Activity**: Determine if there is a legitimate reason for the data transfer.
   - **Correlate with Threat Intelligence**: Verify if the external IP or data transfer matches any known malicious activity patterns.

Example Investigation:

- **Logs**: Showed large data transfers from 10.10.10.50 to 203.0.113.99.
- **User Activity**: Verified that the data transfer was initiated by the backup service account, bkup_user.
- **Data Transfer Analysis**: Confirmed the external IP belongs to a cloud storage provider used for offsite backups.
- **Threat Intelligence**: No matches found for the external IP or data transfer behaviour in known malicious activity databases.

5. Eradication (if necessary)

Steps:

1. **Remove Malicious Artifacts** (if any are found):
   - **Action**: Scan the system for malware or unauthorized changes and remove any identified threats.
   - **Responsible**: SOC Analyst/IR Team.
2. **Patch and Update Systems** (if applicable):
   - **Action**: Ensure the system is fully patched and updated to prevent exploitation of known vulnerabilities.
   - **Responsible**: IT Support.

Example Eradication:

- **System Scan**: Confirmed no malicious artifacts or unauthorized changes were present.
- **Patching**: No additional action required as the system was already up-to-date.

6. Recovery

Steps:

1. **Restore Systems to Operational State** (if any actions were taken):
   - **Action**: No restoration needed as no isolation or significant changes were made.
   - **Responsible**: IT Support.
2. **Monitor for Recurrence**:

    - **Action**: Set up enhanced monitoring on the backup processes and data transfers for the next 48 hours.
    - **Responsible**: SOC Analyst.

Example Recovery:

- **Enhanced Monitoring**: Activated for the next 48 hours on the backup processes and data transfers.

7. Post-Incident Activity

Steps:

1. **Conduct a Post-Mortem**:
    - **Action**: Review the incident, determine why it was flagged as suspicious, and what can be improved to reduce false positives.
    - **Responsible**: IR Team.
2. **Update Documentation**:
    - **Action**: Update the playbooks and knowledge base with findings from the incident.
    - **Responsible**: SOC Analyst.
3. **User Awareness Training**:
    - **Action**: Inform the IT department about the incident and reinforce proper documentation and notification practices for large data transfers.
    - **Responsible**: IT Support/Security Awareness Team.

Example Post-Incident Activity:

- **Post-Mortem Meeting**: 2023-06-16 10:00:00 UTC.
- **Documentation Updated**: Incident report added to the knowledge base.
- **User Training**: Conducted a session with the IT department to ensure proper documentation of large data transfers and communication with the SOC.

False Positive Detection 4: Unauthorized Software Installation

1. Detection

Example Alert:
Alert Name: Unauthorized Software Installation
Source: Endpoint Detection and Response (EDR) Tool
Time: 2023-06-15 16:05:20 UTC
Severity: High
Description: Detected installation of software on a user workstation that matches a pattern commonly associated with unauthorized or potentially malicious applications.

2. Initial Triage

Steps:

1. **Receive and Acknowledge Alert**:
   - **Action**: Confirm receipt of the alert in the SIEM system.
   - **Responsible**: SOC Analyst.
2. **Preliminary Analysis**:
   - **Review Alert Details**: Examine the alert's metadata (time, source IP, user account, software details).
   - **Correlate with Other Alerts**: Check if similar alerts have been triggered recently.
   - **Determine Severity and Priority**: Based on the criticality of the affected system and potential impact.

Example Analysis:

- **Source Host**: 192.168.1.40 (internal IP of a user workstation).
- **User Account**: izzmier@manchesterunited.com.
- **Software Details**: Installation of a file-sharing application.
- **Recent Alerts**: No other similar alerts from this host or user account.

3. Containment

Steps:

1. **Isolate Affected Systems** (if deemed necessary):
   - **Action**: Monitor the system closely but do not isolate yet to avoid disrupting normal operations.
   - **Responsible**: SOC Analyst.
2. **Check for Immediate Threats**:
   - **Action**: Verify if there are any immediate signs of compromise or ongoing malicious activity.
   - **Responsible**: SOC Analyst.

4. Investigation

Steps:

1. **Collect Evidence**:
    - **Action**: Gather logs from the EDR, SIEM, and check installed software list on the workstation.
    - **Responsible**: SOC Analyst.
2. **Analyse Logs**:
    - **Check User Activity**: Determine if the user, izzmier, has a legitimate reason for installing the software.
    - **Correlate with Threat Intelligence**: Verify if the software or behaviour matches any known malicious activity patterns.

Example Investigation:

- **Logs**: Showed the installation of a file-sharing application from a reputable vendor.
- **User Activity**: Verified that izzmier is part of the marketing team, which often uses file-sharing applications to collaborate with external partners.
- **Software Analysis**: Confirmed the software is a legitimate application used by the marketing department for project collaboration.
- **Threat Intelligence**: No matches found for the software or installation behaviour in known malicious activity databases.

5. Eradication (if necessary)

Steps:

1. **Remove Malicious Artifacts** (if any are found):
    - **Action**: Scan the system for malware or unauthorized changes and remove any identified threats.
    - **Responsible**: SOC Analyst/IR Team.
2. **Patch and Update Systems** (if applicable):
    - **Action**: Ensure the system is fully patched and updated to prevent exploitation of known vulnerabilities.
    - **Responsible**: IT Support.

Example Eradication:

- **System Scan**: Confirmed no malicious artifacts or unauthorized changes were present.
- **Patching**: No additional action required as the system was already up-to-date.

6. Recovery

Steps:

1. **Restore Systems to Operational State** (if any actions were taken):
    - **Action**: No restoration needed as no isolation or significant changes were made.
    - **Responsible**: IT Support.
2. **Monitor for Recurrence**:

  - **Action**: Set up enhanced monitoring on the user account and software installations for the next 48 hours.
  - **Responsible**: SOC Analyst.

Example Recovery:

- **Enhanced Monitoring**: Activated for the next 48 hours on the user account and software installations.

7. Post-Incident Activity

Steps:

1. **Conduct a Post-Mortem**:
   - **Action**: Review the incident, determine why it was flagged as suspicious, and what can be improved to reduce false positives.
   - **Responsible**: IR Team.
2. **Update Documentation**:
   - **Action**: Update the playbooks and knowledge base with findings from the incident.
   - **Responsible**: SOC Analyst.
3. **User Awareness Training**:
   - **Action**: Inform the marketing department about the incident and reinforce proper documentation and notification practices for software installations.
   - **Responsible**: IT Support/Security Awareness Team.

Example Post-Incident Activity:

- **Post-Mortem Meeting**: 2023-06-16 10:00:00 UTC.
- **Documentation Updated**: Incident report added to the knowledge base.
- **User Training**: Conducted a session with the marketing department to ensure proper documentation of software installations and communication with the SOC.

False Positive Detection 5: Suspicious Email Activity

1. Detection

Example Alert:
Alert Name: Suspicious Email Activity
Source: SIEM System
Time: 2023-06-15 17:45:10 UTC
Severity: High
Description: Detected a large number of outbound emails from an internal email account within a short period, which may indicate potential spam or phishing activity.

2. Initial Triage

Steps:

1. **Receive and Acknowledge Alert**:
   - **Action**: Confirm receipt of the alert in the SIEM system.
   - **Responsible**: SOC Analyst.
2. **Preliminary Analysis**:
   - **Review Alert Details**: Examine the alert's metadata (time, source IP, user account, email volume).
   - **Correlate with Other Alerts**: Check if similar alerts have been triggered recently.
   - **Determine Severity and Priority**: Based on the criticality of the affected system and potential impact.

Example Analysis:

- **Source Host**: 192.168.1.50 (internal IP of the mail server).
- **User Account**: izzmier@manchesterunited.com.
- **Email Volume**: 500 emails sent in 10 minutes.
- **Recent Alerts**: No other similar alerts from this host or user account.

3. Containment

Steps:

1. **Isolate Affected Systems** (if deemed necessary):
   - **Action**: Monitor the email account closely but do not disable it yet to avoid disrupting normal operations.
   - **Responsible**: SOC Analyst.
2. **Check for Immediate Threats**:
   - **Action**: Verify if there are any immediate signs of compromise or ongoing malicious activity.
   - **Responsible**: SOC Analyst.

4. Investigation

Steps:

1. **Collect Evidence**:
   - **Action**: Gather logs from the SIEM, EDR, and email server related to the outbound email activity.
   - **Responsible**: SOC Analyst.
2. **Analyse Logs**:
   - **Check User Activity**: Determine if the user, izzmier, has a legitimate reason for sending the large volume of emails.
   - **Correlate with Threat Intelligence**: Verify if the email activity or content matches any known spam or phishing patterns.

Example Investigation:

- **Logs**: Showed 500 emails sent by izzmier@manchesterunited.com to various external recipients.
- **User Activity**: Verified that izzmier is part of the sales team, which often sends mass emails to clients for marketing campaigns.
- **Email Content Analysis**: Confirmed that the emails contained legitimate marketing material related to a new product launch.
- **Threat Intelligence**: No matches found for the email content or sending behaviour in known spam or phishing databases.

5. Eradication (if necessary)

Steps:

1. **Remove Malicious Artifacts** (if any are found):
   - **Action**: Scan the system for malware or unauthorized changes and remove any identified threats.
   - **Responsible**: SOC Analyst/IR Team.
2. **Patch and Update Systems** (if applicable):
   - **Action**: Ensure the email server and user workstation are fully patched and updated to prevent exploitation of known vulnerabilities.
   - **Responsible**: IT Support.

Example Eradication:

- **System Scan**: Confirmed no malicious artifacts or unauthorized changes were present.
- **Patching**: No additional action required as the systems were already up-to-date.

6. Recovery

Steps:

1. **Restore Systems to Operational State** (if any actions were taken):
   - **Action**: No restoration needed as no isolation or significant changes were made.
   - **Responsible**: IT Support.

2. **Monitor for Recurrence**:
    - **Action**: Set up enhanced monitoring on the email account and outbound email activities for the next 48 hours.
    - **Responsible**: SOC Analyst.

Example Recovery:

- **Enhanced Monitoring**: Activated for the next 48 hours on the user account and outbound email activities.

7. Post-Incident Activity

Steps:

1. **Conduct a Post-Mortem**:
    - **Action**: Review the incident, determine why it was flagged as suspicious, and what can be improved to reduce false positives.
    - **Responsible**: IR Team.
2. **Update Documentation**:
    - **Action**: Update the playbooks and knowledge base with findings from the incident.
    - **Responsible**: SOC Analyst.
3. **User Awareness Training**:
    - **Action**: Inform the sales team about the incident and reinforce proper documentation and notification practices for large email campaigns.
    - **Responsible**: IT Support/Security Awareness Team.

Example Post-Incident Activity:

- **Post-Mortem Meeting**: 2023-06-16 10:00:00 UTC.
- **Documentation Updated**: Incident report added to the knowledge base.
- **User Training**: Conducted a session with the sales team to ensure proper documentation of email campaigns and communication with the SOC.