**Prompts for Each Dataset**

**Malware_Incident_Response_Log**

Generate a dataset of cyber incident response process activities and communication logs for one type of cyber incident based on the attached file

---

**Augmented_Incident_Response_Log_Phishing**

Using the excel file attached and the following playbook, create an augmented version of the excel file including incident response processing chat and activities for this phishing scenario:

Phishing Attack Response Playbook

1. Detection

Automated Email Scanning:

- Tools Used: Email filtering solutions (e.g., Proofpoint, Mimecast), Threat Intelligence Platforms (TIPs).
- Criteria: Scan incoming emails for indicators of phishing such as:
    - Suspicious senders: Emails from domains that are newly registered or similar to legitimate domains.
    - Malicious links: URLs that lead to known phishing sites or use obfuscation techniques (e.g., URL shortening).
    - Malicious attachments: Files containing macros, executables, or other known malware signatures.
- Machine Learning Models: Utilize models trained on past phishing incidents to improve detection of evolving threats.

False Positive Reduction:

- Implement whitelisting of trusted domains and senders.
- Cross-reference against internal email metadata to identify anomalies.

2. Alert

SOC Notification:

- Medium: Automated alerts through SIEM (Security Information and Event Management) systems, such as Splunk or QRadar.
- Content: The alert includes:
    - Sender information: Display name, email address, and originating IP.
    - Email subject: Highlight any social engineering tactics used.
    - Threat Indicators: Details of suspicious links or attachments.
    - User Engagement: Whether the email was opened, and any links clicked.

Escalation Protocol:

- Priority 1 alerts (high-confidence phishing attempts) trigger immediate SOC response.
- Priority 2 alerts are reviewed within an hour, with potential escalation.

3. Isolation

- Email Quarantine:

    - Action: Automatically quarantine the email in the recipient's inbox, making it inaccessible.
    - Retroactive Action: Search for and quarantine the same email across the organization if multiple recipients were targeted.
- Endpoint Isolation: If the email was opened and a link clicked or attachment opened, isolate the affected endpoint from the network.
- Tools Used: EDR (Endpoint Detection and Response) solutions like CrowdStrike, Carbon Black.

4. Investigation

Automated Email Analysis:

- Sender Verification: Check if the sender's domain is spoofed or compromised.
- Link Analysis: Use a sandbox environment to analyze URLs and attached files for malicious behavior.
- Cross-Reference with Threat Intelligence:
    - Compare with known phishing campaigns.
    - Check against blacklisted IPs/domains in threat intelligence

Forensic Analysis:

- Extract metadata from the email (headers, routing information) to identify any anomalies.
- Examine the payload of attachments using static and dynamic analysis techniques.

5. Remediation

Email Removal:

- Action: Automatically remove the phishing email from all inboxes across the organization.
- Notification: Notify SOC and affected users that the email has been removed and instruct them not to interact with it.

Endpoint Remediation:

Malware Scanning: Initiate a comprehensive scan on affected endpoints.

- Patch Management: Apply any necessary patches if vulnerabilities were exploited.

User Awareness:

- Training Module: Trigger a short, mandatory phishing awareness training for affected users.
- Reporting Protocol: Reinforce the importance of reporting suspicious emails immediately.

6. User Notification

Communication Template:

- Content: Explain the phishing attempt, what actions were taken, and how the user can protect themselves in the future.

- Method: Automated email with embedded training materials or links to internal security portals.

Phishing Reporting Reinforcement:

- Encourage users to use the built-in "Report Phishing" button in their email client for future incidents.

7. Update Defenses

Threat Intelligence Feed Update:

- Action: Automatically update TIPs with new indicators of compromise (IOCs) identified during the incident.
- Filtering Rules Update: Adjust email filtering rules to detect and block similar phishing attempts in the future.

Machine Learning Model Retraining:

- Incorporate data from the phishing attempt to refine ML models for better detection.

Reporting

Incident Report Generation:

- Content: Include a detailed timeline, actions taken, user engagement statistics, and the final outcome.
- Automated Distribution: Send the report to relevant stakeholders (CISO, IT management, and legal/compliance teams).
- Integration with SIEM: Ensure the incident report is logged in the SIEM for future reference.

Lessons Learned:

- Conduct an after-action review to discuss what worked, what didn't, and how processes can be improved.
- Document and integrate these lessons into future playbook iterations.

---

**Augmented_Incident_Response_Positive_Chat**

Using the excel file attached and the following playbook, create an augmented version of the excel file including incident response processing chat with positive sentiment and activities for this phishing scenario: Phishing Attack Response Playbook

1. Detection

Automated Email Scanning:

- Tools Used: Email filtering solutions (e.g., Proofpoint, Mimecast), Threat Intelligence Platforms (TIPs).
- Criteria: Scan incoming emails for indicators of phishing such as:
    - Suspicious senders: Emails from domains that are newly registered or similar to legitimate domains.

    - Malicious links: URLs that lead to known phishing sites or use obfuscation techniques (e.g., URL shortening).
    - Malicious attachments: Files containing macros, executables, or other known malware signatures.
    - Machine Learning Models: Utilize models trained on past phishing incidents to improve detection of evolving threats.

False Positive Reduction:

- Implement whitelisting of trusted domains and senders.
- Cross-reference against internal email metadata to identify anomalies.

2. Alert

SOC Notification:

- Medium: Automated alerts through SIEM (Security Information and Event Management) systems, such as Splunk or QRadar.
- Content: The alert includes:
    - Sender information: Display name, email address, and originating IP.
    - Email subject: Highlight any social engineering tactics used.
    - Threat Indicators: Details of suspicious links or attachments.
    - User Engagement: Whether the email was opened, and any links clicked.

Escalation Protocol:

- Priority 1 alerts (high-confidence phishing attempts) trigger immediate SOC response.
- Priority 2 alerts are reviewed within an hour, with potential escalation.

3. Isolation

Email Quarantine:

- Action: Automatically quarantine the email in the recipient's inbox, making it inaccessible.
- Retroactive Action: Search for and quarantine the same email across the organization if multiple recipients were targeted.

Endpoint Isolation:

- If the email was opened and a link clicked or attachment opened, isolate the affected endpoint from the network.
- Tools Used: EDR (Endpoint Detection and Response) solutions like CrowdStrike, Carbon Black.

4. Investigation

Automated Email Analysis:

- Sender Verification: Check if the sender's domain is spoofed or compromised.
- Link Analysis: Use a sandbox environment to analyze URLs and attached files for malicious behavior.
- Cross-Reference with Threat Intelligence:
    - Compare with known phishing campaigns.

- Check against blacklisted IPs/domains in threat intelligence

Forensic Analysis:

- Extract metadata from the email (headers, routing information) to identify any anomalies.
- Examine the payload of attachments using static and dynamic analysis techniques.

5. Remediation

Email Removal:

- Action: Automatically remove the phishing email from all inboxes across the organization.
- Notification: Notify SOC and affected users that the email has been removed and instruct them not to interact with it.

Endpoint Remediation:

- Malware Scanning: Initiate a comprehensive scan on affected endpoints.
- Patch Management: Apply any necessary patches if vulnerabilities were exploited.

User Awareness:

- Training Module: Trigger a short, mandatory phishing awareness training for affected users.
- Reporting Protocol: Reinforce the importance of reporting suspicious emails immediately.

6. User Notification

Communication Template:

- Content: Explain the phishing attempt, what actions were taken, and how the user can protect themselves in the future.
- Method: Automated email with embedded training materials or links to internal security portals.

Phishing Reporting Reinforcement:

- Encourage users to use the built-in “Report Phishing” button in their email client for future incidents.

7. Update Defenses

Threat Intelligence Feed Update:

- Action: Automatically update TIPs with new indicators of compromise (IOCs) identified during the incident.
- Filtering Rules Update: Adjust email filtering rules to detect and block similar phishing attempts in the future.

Machine Learning Model Retraining:

- Incorporate data from the phishing attempt to refine ML models for better detection.

Reporting

Incident Report Generation:

- Content: Include a detailed timeline, actions taken, user engagement statistics, and the final outcome.
- Automated Distribution: Send the report to relevant stakeholders (CISO, IT management, and legal/compliance teams).
- Integration with SIEM: Ensure the incident report is logged in the SIEM for future reference.

Lessons Learned:

- Conduct an after-action review to discuss what worked, what didn't, and how processes can be improved.
- Document and integrate these lessons into future playbook iterations.

---

**Augmented_Incident_Response_Neutral_Chat**

Using the excel file attached and the following playbook, create an augmented version of the excel file including incident response processing chat with neutral sentiment and activities for this phishing scenario: Phishing Attack Response Playbook

1. Detection

Automated Email Scanning:

- Tools Used: Email filtering solutions (e.g., Proofpoint, Mimecast), Threat Intelligence Platforms (TIPs).
- Criteria: Scan incoming emails for indicators of phishing such as:
  - Suspicious senders: Emails from domains that are newly registered or similar to legitimate domains.
  - Malicious links: URLs that lead to known phishing sites or use obfuscation techniques (e.g., URL shortening).
  - Malicious attachments: Files containing macros, executables, or other known malware signatures.
  - Machine Learning Models: Utilize models trained on past phishing incidents to improve detection of evolving threats.

False Positive Reduction:

- Implement whitelisting of trusted domains and senders.
- Cross-reference against internal email metadata to identify anomalies.

2. Alert

SOC Notification:

- Medium: Automated alerts through SIEM (Security Information and Event Management) systems, such as Splunk or QRadar.
- Content: The alert includes:
  - Sender information: Display name, email address, and originating IP.
  - Email subject: Highlight any social engineering tactics used.

    - Threat Indicators: Details of suspicious links or attachments.
    - User Engagement: Whether the email was opened, and any links clicked.

Escalation Protocol:

- Priority 1 alerts (high-confidence phishing attempts) trigger immediate SOC response.
- Priority 2 alerts are reviewed within an hour, with potential escalation.

3. Isolation

Email Quarantine:

- Action: Automatically quarantine the email in the recipient's inbox, making it inaccessible.
- Retroactive Action: Search for and quarantine the same email across the organization if multiple recipients were targeted.
- Endpoint Isolation:
    - If the email was opened and a link clicked or attachment opened, isolate the affected endpoint from the network.
    - Tools Used: EDR (Endpoint Detection and Response) solutions like CrowdStrike, Carbon Black.

4. Investigation

Automated Email Analysis:

- Sender Verification: Check if the sender's domain is spoofed or compromised.
- Link Analysis: Use a sandbox environment to analyze URLs and attached files for malicious behavior.
- Cross-Reference with Threat Intelligence:
    - Compare with known phishing campaigns.
    - Check against blacklisted IPs/domains in threat intelligence

Forensic Analysis:

- Extract metadata from the email (headers, routing information) to identify any anomalies.
- Examine the payload of attachments using static and dynamic analysis techniques.

5. Remediation

Email Removal:

- Action: Automatically remove the phishing email from all inboxes across the organization.
- Notification: Notify SOC and affected users that the email has been removed and instruct them not to interact with it.

Endpoint Remediation:

- Malware Scanning: Initiate a comprehensive scan on affected endpoints.
- Patch Management: Apply any necessary patches if vulnerabilities were exploited.

User Awareness:

- Training Module: Trigger a short, mandatory phishing awareness training for affected users.
- Reporting Protocol: Reinforce the importance of reporting suspicious emails immediately.

6. User Notification

Communication Template:

- Content: Explain the phishing attempt, what actions were taken, and how the user can protect themselves in the future.
- Method: Automated email with embedded training materials or links to internal security portals.

Phishing Reporting Reinforcement:

- Encourage users to use the built-in "Report Phishing" button in their email client for future incidents.

7. Update Defenses

Threat Intelligence Feed Update:

- Action: Automatically update TIPs with new indicators of compromise (IOCs) identified during the incident.
- Filtering Rules Update: Adjust email filtering rules to detect and block similar phishing attempts in the future.

Machine Learning Model Retraining:

- Incorporate data from the phishing attempt to refine ML models for better detection.

Reporting

Incident Report Generation:

- Content: Include a detailed timeline, actions taken, user engagement statistics, and the final outcome.
- Automated Distribution: Send the report to relevant stakeholders (CISO, IT management, and legal/compliance teams).
- Integration with SIEM: Ensure the incident report is logged in the SIEM for future reference.

Lessons Learned:

- Conduct an after-action review to discuss what worked, what didn't, and how processes can be improved.
- Document and integrate these lessons into future playbook iterations.

---

**Incident_Response_Log_Phishing_Augmented_Negative**

Using the excel file attached and the following playbook, create an augmented version of the excel file including incident response processing chat with negative sentiment and activities for this phishing scenario: Phishing Attack Response Playbook

1. Detection

Automated Email Scanning:

- Tools Used: Email filtering solutions (e.g., Proofpoint, Mimecast), Threat Intelligence Platforms (TIPs).
- Criteria: Scan incoming emails for indicators of phishing such as:
    - Suspicious senders: Emails from domains that are newly registered or similar to legitimate domains.
    - Malicious links: URLs that lead to known phishing sites or use obfuscation techniques (e.g., URL shortening).
    - Malicious attachments: Files containing macros, executables, or other known malware signatures.
    - Machine Learning Models: Utilize models trained on past phishing incidents to improve detection of evolving threats.

False Positive Reduction:

- Implement whitelisting of trusted domains and senders.
- Cross-reference against internal email metadata to identify anomalies.

2. Alert

SOC Notification:

- Medium: Automated alerts through SIEM (Security Information and Event Management) systems, such as Splunk or QRadar.
- Content: The alert includes:
    - Sender information: Display name, email address, and originating IP.
    - Email subject: Highlight any social engineering tactics used.
    - Threat Indicators: Details of suspicious links or attachments.
    - User Engagement: Whether the email was opened, and any links clicked.

Escalation Protocol:

- Priority 1 alerts (high-confidence phishing attempts) trigger immediate SOC response.
- Priority 2 alerts are reviewed within an hour, with potential escalation.

3. Isolation

Email Quarantine:

- Action: Automatically quarantine the email in the recipient's inbox, making it inaccessible.
- Retroactive Action: Search for and quarantine the same email across the organization if multiple recipients were targeted.

Endpoint Isolation:

- If the email was opened and a link clicked or attachment opened, isolate the affected endpoint from the network.
- Tools Used: EDR (Endpoint Detection and Response) solutions like CrowdStrike, Carbon Black.

4. Investigation

Automated Email Analysis:

- Sender Verification: Check if the sender's domain is spoofed or compromised.
- Link Analysis: Use a sandbox environment to analyze URLs and attached files for malicious behavior.

Cross-Reference with Threat Intelligence:

- Compare with known phishing campaigns.
- Check against blacklisted IPs/domains in threat intelligence

Forensic Analysis:

- Extract metadata from the email (headers, routing information) to identify any anomalies.
- Examine the payload of attachments using static and dynamic analysis techniques.

5. Remediation

Email Removal:

- Action: Automatically remove the phishing email from all inboxes across the organization.
- Notification: Notify SOC and affected users that the email has been removed and instruct them not to interact with it.

Endpoint Remediation:

- Malware Scanning: Initiate a comprehensive scan on affected endpoints.
- Patch Management: Apply any necessary patches if vulnerabilities were exploited.

User Awareness:

- Training Module: Trigger a short, mandatory phishing awareness training for affected users.
- Reporting Protocol: Reinforce the importance of reporting suspicious emails immediately.

6. User Notification

Communication Template:

- Content: Explain the phishing attempt, what actions were taken, and how the user can protect themselves in the future.
- Method: Automated email with embedded training materials or links to internal security portals.

Phishing Reporting Reinforcement:

- Encourage users to use the built-in “Report Phishing” button in their email client for future incidents.

7. Update Defenses

Threat Intelligence Feed Update:

- Action: Automatically update TIPs with new indicators of compromise (IOCs) identified during the incident.
- Filtering Rules Update: Adjust email filtering rules to detect and block similar phishing attempts in the future.

Machine Learning Model Retraining:

- Incorporate data from the phishing attempt to refine ML models for better
- detection.

Reporting

Incident Report Generation:

- Content: Include a detailed timeline, actions taken, user engagement statistics, and the final outcome.
- Automated Distribution: Send the report to relevant stakeholders (CISO, IT management, and legal/compliance teams).
- Integration with SIEM: Ensure the incident report is logged in the SIEM for future reference.

Lessons Learned:

- Conduct an after-action review to discuss what worked, what didn't, and how processes can be improved.
- Document and integrate these lessons into future playbook iterations.

---

**Incident_Response_Log_Phishing_Negative_Sentiment**

Using the excel file attached and the following playbook, create an augmented version of the excel file including incident response processing chat with negative sentiment and activities for this phishing scenario: Phishing Attack Response Playbook

1. Detection

Automated Email Scanning:

- Tools Used: Email filtering solutions (e.g., Proofpoint, Mimecast), Threat Intelligence Platforms (TIPs).
- Criteria: Scan incoming emails for indicators of phishing such as:
    - Suspicious senders: Emails from domains that are newly registered or similar to legitimate domains.
    - Malicious links: URLs that lead to known phishing sites or use obfuscation techniques (e.g., URL shortening).
    - Malicious attachments: Files containing macros, executables, or other known malware signatures.
    - Machine Learning Models: Utilize models trained on past phishing incidents to improve detection of evolving threats.

False Positive Reduction:

- Implement whitelisting of trusted domains and senders.
- Cross-reference against internal email metadata to identify anomalies.

2. Alert

SOC Notification:

- Medium: Automated alerts through SIEM (Security Information and Event Management) systems, such as Splunk or QRadar.
- Content: The alert includes:
    - Sender information: Display name, email address, and originating IP.
    - Email subject: Highlight any social engineering tactics used.
    - Threat Indicators: Details of suspicious links or attachments.
    - User Engagement: Whether the email was opened, and any links clicked.

Escalation Protocol:

- Priority 1 alerts (high-confidence phishing attempts) trigger immediate SOC response.
- Priority 2 alerts are reviewed within an hour, with potential escalation.

3. Isolation

Email Quarantine:

- Action: Automatically quarantine the email in the recipient's inbox, making it inaccessible.
- Retroactive Action: Search for and quarantine the same email across the organization if multiple recipients were targeted.

Endpoint Isolation:

- If the email was opened and a link clicked or attachment opened, isolate the affected endpoint from the network.
- Tools Used: EDR (Endpoint Detection and Response) solutions like CrowdStrike, Carbon Black.

4. Investigation

Automated Email Analysis:

- Sender Verification: Check if the sender's domain is spoofed or compromised.
- Link Analysis: Use a sandbox environment to analyze URLs and attached files for malicious behavior.
- Cross-Reference with Threat Intelligence:
    - Compare with known phishing campaigns.
    - Check against blacklisted IPs/domains in threat intelligence

Forensic Analysis:

- Extract metadata from the email (headers, routing information) to identify any anomalies.
- Examine the payload of attachments using static and dynamic analysis techniques.

5. Remediation

Email Removal:

- Action: Automatically remove the phishing email from all inboxes across the organization.
- Notification: Notify SOC and affected users that the email has been removed and instruct them not to interact with it.

Endpoint Remediation:

- Malware Scanning: Initiate a comprehensive scan on affected endpoints.
- Patch Management: Apply any necessary patches if vulnerabilities were exploited.

User Awareness:

- Training Module: Trigger a short, mandatory phishing awareness training for affected users.
- Reporting Protocol: Reinforce the importance of reporting suspicious emails immediately.

6. User Notification

Communication Template:

- Content: Explain the phishing attempt, what actions were taken, and how the user can protect themselves in the future.
- Method: Automated email with embedded training materials or links to internal security portals.

Phishing Reporting Reinforcement:

- Encourage users to use the built-in "Report Phishing" button in their email client for future incidents.

7. Update Defenses

Threat Intelligence Feed Update:

- Action: Automatically update TIPs with new indicators of compromise (IOCs) identified during the incident.
- Filtering Rules Update: Adjust email filtering rules to detect and block similar phishing attempts in the future.

Machine Learning Model Retraining:

- Incorporate data from the phishing attempt to refine ML models for better detection.

Reporting

Incident Report Generation:

- Content: Include a detailed timeline, actions taken, user engagement statistics, and the final outcome.
- Automated Distribution: Send the report to relevant stakeholders (CISO, IT management, and legal/compliance teams).

- Integration with SIEM: Ensure the incident report is logged in the SIEM for future reference.

Lessons Learned:

- Conduct an after-action review to discuss what worked, what didn't, and how processes can be improved.
- Document and integrate these lessons into future playbook iterations.

---

**Augmented_Incident_Response_Log**

Instruction: Augment a dataset attached named: *Incident_Event_Log_Samples* to include the same fields and generate Cyber Incident Response Process Activities and Communication Logs for enrichment

Context: The dataset should closely simulate the IR process approach presented in the attached sample IR Playbook and Chat Log containing different IR Case types named: *IR-Playbooks* This will aid you in populating the new dataset fields to be augmented to an existing dataset. The dataset should include variations of IR cases for various Incident Types both from the IR Playbook and additional Incidents types

Input Data: The existing dataset fields, and their values are presented in the attached dataset named: *Incident_Event_Log_Samples* The new enhanced dataset fields attributes to be included are described in the attached file named: *Fields*

Output Indicator: Generate the new dataset output in CSV format where each row is a unique incident response case

---

**Enhanced_Incident_Response_Log_With_Communications**

Instruction: Augment a dataset attached named: *Incident_Event_Log_Samples* to generate Cyber Incident Response Process Activities and Communication Logs. Include additional fields as described in the attached file named: *Fields*, closely simulate the Incident Response process approach presented in the attached Incident Response playbooks and chat logs samples file named: *IR-Playbooks* which contains different IR Case types

Context: The dataset should closely simulate the Incident Response process approach presented in the attached Incident Response playbooks and chat logs samples file named: *IR-Playbooks* which contains different IR Case types. This will aid you in populating the new dataset fields to be augmented to the existing dataset. The dataset should include variations of Incident Response cases for various Incident Types both from the Incident Response Playbook and additional Incidents types

Input Data: The existing dataset fields, and their values are presented in the attached dataset named: *Incident_Event_Log_Samples* The new enhanced dataset fields attributes to be included are described in the attached file named: *Fields*

Output Indicator: Generate the new dataset output in CSV format where each row is a unique incident response case

---

**Phishing_Incident_Response_Dataset**

Instruction: Using the dataset attached named: *Incident_Event_Log_Samples* generate a new dataset of Cyber Incident Response Process Activities and Communication Logs. Augment the information to include the same fields as outlined in the dataset attached named: *Incident_Event_Log_Samples* and additional fields as described in the attached file named: *Fields*, closely simulate the Incident Response process approach to a phishing attack and chat logs sample as described in the file attached named: *Phishing Attack Response Playbook* which contains an Incident Response approach to a phishing attack and chat logs sample.

Context: The dataset should closely simulate the Incident Response process approach to a phishing attack and chat logs sample as described in the file attached named: *Phishing Attack Response Playbook* which contains an Incident Response approach to a phishing attack and chat logs sample. This will aid you in populating the new dataset fields to be augmented to the existing dataset. The dataset should include an Incident Response case for a phishing incident.

Input Data: The existing dataset fields, and their values are presented in the attached dataset named: *Incident_Event_Log_Samples* The new enhanced dataset fields attributes to be included are described in the attached file named: *Fields*

Output Indicator: Generate the new dataset output in CSV format where each row is a unique incident response case

---

**Augmented_Phishing_Incident_Dataset**

Instruction: Augment the attached dataset named: *Incident_Event_Log_Samples* to generate a dataset of cyber incident response activities and communication logs for phishing attacks.

Context: Augment the fields in the current dataset and include all additional fields as described in the attached file named: *Fields*. Ensure to create the fields Incident Response Case and Observables Analysis in array format containing the information listed. Place all information in two columns with the first column being the fields and second column being the values, group each incident. The dataset should closely simulate the incident response process approach for a phishing attack presented in the file attached named: *Phishing Attack Response Playbook*, this is a sample playbook and chat log for an incident response phishing case. This will aid you in populating the new dataset fields to be augmented to the existing dataset. The dataset should include variations of phishing cases for various incidents.

Input Data: The existing dataset fields, and their values are presented in the attached dataset named: *Incident_Event_Log_Samples* The new enhanced dataset fields attributes to be included are described in the attached file named: *Fields*

Output Indicator: Generate the new dataset output in CSV format including multiple unique incident response cases

---

**Simulated_Incident_Response_Data**

Attached is a dataset of incident response activities logs related to various cybersecurity cases named: *Incident_Event_Log_Samples.xlsx*. Augment this to simulate a dataset of cyber incident response activities and communication logs for multiple incidents.

Attached are two supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case, Observables Analysis, and Event Analysis.
- IR-Playbooks.pdf: This provides sample playbooks and chat logs describing realistic incident response steps for various cyber-attacks.

Instructions:

1. Understand the sample incident response processes described in the file IR-Playbooks.pdf.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include variations of incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of incident response and chat log data.

---

**Simulated_Incident_Response_Logs**

Attached is a dataset of incident response activities logs related to various cybersecurity cases named: *Incident_Event_Log_Samples.xlsx*. Augment this to simulate a dataset of cyber incident response activities and communication logs for 5 incidents.

Attached are two supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- IR-Playbooks.pdf: This provides sample playbooks and chat logs describing realistic incident response steps for various cyber-attacks.

Instructions:

1. Understand the sample incident response processes described in the file IR-Playbooks.pdf.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.

5. Include 5 variations of incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of incident response and chat log data.

---

**Simulated_Phishing_Incidents**

Attached is a dataset of incident response activities logs related to various cybersecurity cases in an Excel file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for three phishing incidents.

Attached are two supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic phishing case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include three variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

**Simulated_Phishing_Incidents_10**

Can you generate 10 examples in a CSV file

---

**Simulated_Phishing_Incidents_Additional_10**

10 more

---

**Simulated_Phishing_Incidents_Additional_20**

20 more

---

**Simulated_Phishing_Incidents_Final_10**

10 more

---

**Simulated_50_Phishing_Incidents**

Attached is a dataset of incident response activities logs related to various cybersecurity cases in an Excel file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for 50 phishing incidents.

Attached are two supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic phishing case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include three variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

**Simulated_Additional_5_Phishing_Incidents**

5 more

---

**Phishing_Incident_Response_Simulation**

Attached is a dataset of incident response activities logs related to various cybersecurity cases in an Excel file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for 50 phishing incidents.

Attached are two supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic phishing case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include three variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

**Phishing_Incident_Simulation**

Attached is a dataset of incident response activities logs related to various cybersecurity cases in an Excel file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for 50 phishing incidents.

Attached are two supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic phishing case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include 50 variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

**Phishing_Incident_Simulation_Additional50**

50 more

---

**Phishing_Incident_Simulation_Extra25_Varied**

25 more and have them with more variation

---

**Simulated_Phishing_Incidents (1)**

Attached is a dataset of incident response activities logs related to various cybersecurity cases in a file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for three phishing incidents.

Attached are three supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.
- CompleteExample.xlsx: This defines the preferred format of the final dataset.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic phishing case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include three variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

**Enhanced_Phishing_Incidents**

Attached is a dataset of incident response activities logs related to various cybersecurity cases in a file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for three phishing incidents.

Attached are two supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.

- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic phishing case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include three variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

Phishing_Incident_Response_Simulation (1)

Attached is a dataset of incident response activities logs related to various cybersecurity cases in a file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for three phishing incidents.

Attached are three supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.
- CompleteExample.xlsx: This defines the preferred format of the final dataset.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.
2. Use the fields listed in Fields.xlsx to augment the existing dataset in Incident_Event_Log_Samples.xlsx.
3. For each incident, simulate a realistic phishing case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.

5. Include three variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

**Augmented_Incident_Response_Log (1)**

Generate a dataset of Cyber Incident Response Process Activities and Communication Log.

The dataset should closely simulate the IR process approach presented in the attached incident response and chat log sample: *CompleteExample* This will aid you in populating the new dataset fields to be augmented to an existing dataset attached * Incident_Event_Log_Samples*. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for three phishing incidents.

The new dataset fields to be included and their values are presented in the attached file * Fields*. The attached file *Phishing Attack Response Playbook* provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.

Generate the new dataset output in CSV format where each row is a unique incident response case.

---

**phishing_incident_case**

Generate a dataset of cyber incident response process activities and a communication log for a phishing incident.

The dataset should closely simulate the Incident response process approach.

Generate the dataset output in CSV format where each row is a unique incident response case.

---

**Simulated_Phishing_Incident_Response**

Attached is a dataset of incident response activities logs related to various cybersecurity cases in a file named Incident_Event_Log_Samples.xlsx. Augment and enhance this dataset to simulate a cyber incident response dataset specifically for two phishing incidents. Use all the fields in this file and augment the values.

Attached are three supporting files:

- Fields.xlsx: This defines additional fields to be included in the new dataset, including structured array fields like Incident Response Case and Observables Analysis.
- Phishing Attack Response Playbook.docx: This provides a sample playbook and chat log describing realistic incident response steps for phishing attacks.
- CompleteExample.xlsx: This defines the preferred format of the final dataset.

Instructions:

1. Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.

2. Use the fields listed in Fields.xlsx to add to the existing fields in Incident_Event_Log_Samples.xlsx.
3. Simulate a realistic phishing incident response case ensuring to include:
    - A detailed array for the fields Incident Response Case and Observables Analysis containing the information as outlined for these fields in Fields.xlsx
    - Include a simulated chat log field (e.g., Chat Log) with time-stamped, realistic communications between SOC analysts handling the case
4. Format the output as a two-column dataset with Field and Value, grouping entries per incident and inserting a blank row between each case.
5. Include two variations of phishing incidents, using user-reported cases and automated detections.
6. Output the final dataset in CSV format for download.

Ensure the output closely reflects a structured, professional simulation of phishing incident response and chat log data.

---

**Complete_Simulated_Phishing_Incident_Response**

This time include all of the fields as listed in CompleteExample.xlsx and augment the values to match the scenario you create

---

**Non_Anonymized_Complete_Phishing_Incident_Response**

This time do not leave any data anonymised such as ?, make sure this value is augmented, rfc means request for change

---

**Structured_Complete_Phishing_Incident_Response**

Ensure to include a structure array field for Case Tasks and Observables Analysis keeping the structure of those values as outlined in the attached file and augment to this scenario

---

**Structured_Phishing_CaseTasks_Exact**

You need to include all information exactly how the following is structured for Case Tasks: [{"Case Tasks Title": "Email Filtering", "Case Task Start Date": "29/02/2016 01:30", "Case Task Assignee": "user_789", "Case Task Status": "Completed", "Case Task Duration": "30 minutes", "Case Attribute Data": "{ 'email': 'suspicious@example.com', 'reason': 'unknown sender' }"}, {"Case Tasks Title": "Quarantine Email", "Case Task Start Date": "29/02/2016 01:40", "Case Task Assignee": "user_789", "Case Task Status": "Completed", "Case Task Duration": "20 minutes", "Case Attribute Data": "{ 'email_id': '12345', 'status': 'quarantined' }"}, {"Case Tasks Title": "Endpoint Isolation", "Case Task Start Date": "29/02/2016 01:45", "Case Task Assignee": "user_789", "Case Task Status": "Completed", "Case Task Duration": "40 minutes", "Case Attribute Data": "{ 'endpoints': ['PC001', 'PC002'], 'status': 'isolated' }"}, {"Case Tasks Title": "Analyzing IoCs", "Case Task Start Date": "29/02/2016 02:00", "Case Task Assignee": "user_456", "Case Task Status": "Completed", "Case Task Duration": "1 hour", "Case Attribute Data": "{ 'data_collected': 'sender_info, email_content, IP_address' }"}, {"Case Tasks Title": "Email Removal", "Case Task Start Date": "29/02/2016 02:15", "Case Task Assignee": "user_789", "Case Task Status": "Completed", "Case Task Duration": "25 minutes", "Case Attribute Data": "{ 'removed_emails': ['suspicious@example.com'] }"}, {"Case Tasks Title": "Apply Patches", "Case Task Start Date": "29/02/2016 02:45", "Case Task Assignee": "user_789", "Case Task Status": "Completed", "Case Task Duration": "1 hour", "Case Attribute Data": "{ 'patches_applied': 'Security_patch_1, Security_patch_2' }"}, {"Case Tasks Title": "Filtering Criteria Review", "Case

Task Start Date": "29/02/2016 03:15", "Case Task Assignee": "user_789", "Case Task Status": "Completed", "Case Task Duration": "45 minutes", "Case Attribute Data": "{ 'new_criteria': 'Updated filters to include recent phishing patterns' }"}, {"Case Tasks Title": "Incident Report", "Case Task Start Date": "29/02/2016 04:00", "Case Task Assignee": "user_456", "Case Task Status": "Completed", "Case Task Duration": "1 hour", "Case Attribute Data": "{ 'report_summary': 'Phishing attack successfully contained and remediated.' }"}]

---

**Augmented_Structured_Phishing_CaseTasks**

now augment this data to suit the scenario

---

**Final_Augmented_Phishing_CaseTasks**

yes but change all of  the data in the field case tasks to match the scenario you created

---

**Final_Observables_Augmented_Phishing**

You need to include all information exactly how the following is structured for Observables Analysis: [{"Analysis Type": "File", "Analysis ID": "file-2016-001", "Timestamp": "2016-02-29 02:00:10 UTC", "Data Value": "MD5 Hash: e99a18c428cb38d5f260853678922e03", "Details": "Detected by 7/60 antivirus engines, flagged as Trojan:Win32/Generic and Ransomware:Win32/Locky", "Status": "Success"}, {"Analysis Type": "URL", "Analysis ID": "url-2016-002", "Timestamp": "2016-02-29 02:01:10  UTC", "Data Value": "URL: http://malicious-site.com", "Details": "Reputation score is 0 (High risk), associated with known phishing campaigns", "Status": "Success"}, {"Analysis Type": "IP Address", "Analysis ID": "ip-2016-003", "Timestamp": "2016-02-29 02:01:130  UTC", "Data Value": "IP Address: 192.168.1.100", "Details": "IP is listed in threat intelligence feeds as associated with phishing activities, has been involved in 5 previous incidents", "Status": "Success"}, {"Analysis Type": "Domain", "Analysis ID": "domain-2016-004", "Timestamp": "2016-02-29 02:02:10  UTC", "Data Value": "Domain: example-malicious.com", "Details": "Domain is associated with multiple known phishing campaigns, reputation score is 0 (High risk)", "Status": "Success"}, {"Analysis Type": "Email Header", "Analysis ID": "email-2016-005", "Timestamp": "2016-02-29 02:02:50 UTC", "Data Value": "Header Analysis: Received: from mail.example.com", "Details": "Header indicates the email was sent from a known suspicious IP, associated with previous phishing attempts", "Status": "Success"}, {"Analysis Type": "Process", "Analysis ID": "process-2016-006", "Timestamp": "2016-02-29 02:03:04  UTC", "Data Value": "Process ID: 1234, Process Name: suspicious.exe", "Details": "Process is flagged by multiple security tools as malicious, showing behavior consistent with ransomware", "Status": "Success"}]

---

**Final_Scenario_Observables_Phishing**

yes but change all of  the data in the field observables analysis to match the scenario you created

---

**Final_Scenario_Timestamps_Aligned**

Can you make sure all date and timestamps are correct and in alignment for the phishing scenario you created in the attached excel

I attached the excel from the last prompt: Final Scenario Observables Phishing

---

**Final_ChatLog_Timestamps_Aligned**

Can you make sure all date and timestamps are correct in the chat log also and in alignment for the phishing scenario you created in the attached excel

I attached the excel from the last prompt: Final Scenario Timestamps Aligned

---

**Final_ChatLog_Timestamps_Corrected**

Can you fix the timestamps in the chat log there are format errors

---

**Final_ChatLog_HHMM_Timestamps**

No make the timestamp in the chat log HH:MM

---

**Final_Updated_ChatLog_Scenario**

Can you update the chat log to replicate the following and then adjust to your scenario: User_789 [01:16 AM]: "Received a report of a suspicious email from Caller 2403. The email seems to be a phishing attempt. We should start by filtering and quarantining it immediately." User_456 [01:20 AM]: "The email has been flagged as containing potentially malicious links. Will update once they respond." User_789 [01:30 AM]: "Email has been quarantined. Iâ€™ve initiated a malware scan on the affected endpoints. Itâ€™s quite a frustrating issue, but we should resolve it quickly." User_456 [01:45 AM]: "Confirmed, the malware scan is in progress. The situation is critical, but Iâ€™m confident weâ€™ll handle it effectively. Letâ€™s keep the communication flowing." User_789 [02:00 AM]: "Collected data on the email sender and IP address. The sender is flagged in our threat database. The scan didnâ€™t find any immediate threats on the endpoints, but weâ€™re still monitoring." User_456 [02:15 AM]: "Removing the phishing email from all inboxes. Users are notified with guidance on recognizing phishing attempts. The support from the team has been excellent." User_789 [02:30 AM]: "Applied security patches to address potential vulnerabilities. This should mitigate similar threats in the future. Overall, the situation was managed well, despite the initial difficulties." User_456 [03:00 AM]: "Reviewed filtering criteria to include the new phishing patterns. The incident is resolved quickly. The quick response and team support were crucial." User_789 [03:30 AM]: "Incident report is being drafted. Summary: Phishing attack successfully contained with no major impact. We acted swiftly and effectively." User_456 [04:00 AM]: "Final report completed and shared. Good job to everyone involved. It was a challenging situation, but we resolved it efficiently."

---

**Final_ChatLog_RFC_Adjusted**

For the field RFC which means Request For Change identifier of a change request associated with the incident, can you make sure in the attached log that this is only filled in if there is a request for change in the scenario and adjust in the dataset according to the scenario you provided

I attached the previous file but named as: Final Updated ChatLog Scenario Almost Perfect but Errors

---

**Final_ChatLog_No_RFC_Field**

If there is no RFC then remove the field completely please

---

**Final_ChatLog_CaseID_Adjusted**

Can we adjust the Case ID field to be INC followed by the numbers

---

**Final_ChatLog_CaseID_CASE_Format**

That is perfect for the number field, for the Case ID field can you adjust the value to CASE followed by numbers

---

**Final_ChatLog_CaseID_Unique**

can you generate Case followed by a different number for the Case ID field please

---

**Final_ChatLog_Close_Code_Updated**

Using the following case closure codes augment the cose_code field to contain the appropriate value: Incident Response Case Closure Codes

- Resolved - True Positive: The reported incident was legitimate, and malicious activity or a security breach was confirmed. This indicates a successful detection and response to a real threat.
- Sub-categories (By Threat Vector):

Email-based Threats:

- Phishing (Credential Harvesting): User fell victim to a phishing attempt designed to steal login credentials, and the credentials were confirmed compromised.
- Phishing (Malware Attachment): User opened a malicious attachment from an email, leading to malware execution.
- Business Email Compromise (BEC): An attacker successfully impersonated a legitimate entity (e.g., executive, vendor) via email, leading to financial fraud or data compromise.
- Spear Phishing: A highly targeted phishing attack succeeded against a specific individual or group.
- Malicious URL Click: User clicked on a malicious link in an email, leading to compromise or attempted compromise.

Endpoint/Host-Based Threats:

- Malware Infection: A system was confirmed infected with malicious software.
- Ransomware Detected: Ransomware was identified and its activity (encryption, demand) confirmed.
- Remote Access Trojan (RAT): A RAT was detected and confirmed to have established control over an endpoint.
- Privilege Escalation: An attacker or malicious process successfully gained elevated privileges on a system.
- Unauthorized Software Execution: Unauthorized or malicious software was executed on an endpoint.
- Persistence Mechanism Installed: An attacker successfully established a method for maintaining access to a compromised system (e.g., creating a new service, modifying registry).

Network-Based Threats:

- Command and Control (C2) Traffic: Malicious C2 communication (beaconing, exfiltration) was detected and confirmed.

- Data Exfiltration Attempt: Confirmed attempt or success in transferring sensitive data out of the network.
- Port Scanning/Reconnaissance: Confirmed malicious reconnaissance activity (e.g., targeted port scans, vulnerability scans) from an attacker.
- Distributed Denial of Service (DDoS): A confirmed DDoS attack impacting network availability.
- Lateral Movement Detected: An attacker successfully moved from one compromised system to another within the internal network.
- Suspicious VPN Use or Traffic Routing: Confirmed unauthorized or malicious use of VPNs or abnormal traffic routing indicative of compromise.

Identity and Access Violations:

- Brute Force Login (Successful): An account was successfully compromised via brute-force attack.
- Suspicious Login (e.g., from foreign IP): A confirmed legitimate but unauthorized login from an unusual/suspicious location or device.
- Unauthorized Access to System/Data: General confirmation of unauthorized access to a system or specific data, not necessarily tied to a specific login method.
- Privilege Abuse: A legitimate user was confirmed to have abused their authorized privileges for malicious or unauthorized purposes.
- Account Compromise: A user account (not necessarily via brute-force) was confirmed compromised and used by an attacker.

Data Security:

- Sensitive Data Exposure: Confirmed exposure or leak of sensitive organizational or customer data.
- Unencrypted Data Transfer: Confirmed transfer of sensitive data over unencrypted channels where encryption was required.
- Data Loss Prevention (DLP) Policy Violation: A confirmed violation of DLP policies indicating sensitive data mishandling or attempted exfiltration.
- Shadow IT Detection (unsanctioned tools/services): Confirmed use of unsanctioned applications or services that expose the organization to risk.

Insider Threats / Internal Misuse:

- Deliberate Policy Violation: A confirmed incident where an internal user deliberately violated security policies, leading to a security event.
- Sabotage or Malicious Insider Activity: Confirmed malicious actions by an insider aimed at damaging systems, data, or operations.
- Use of Unauthorized USB or Devices: Confirmed incident of unauthorized external storage devices being connected and potentially compromising systems.

Others / Specialized:

- Zero-Day Exploitation: Confirmation that a previously unknown vulnerability without a patch available (zero-day) was exploited in an attack.
- Supply Chain Attack Detected: A confirmed compromise originating from a third-party vendor or software supply chain.

- Threat Intel Match (IOCs confirmed): An Indicator of Compromise (IOC) from threat intelligence was confirmed to be present in the environment.
- Confirmed Exploit Attempt (e.g., Log4Shell, ProxyShell): A specific, known vulnerability (e.g., Log4Shell, ProxyShell) was successfully exploited, or an attempt was confirmed.

1. False Positive: The alert or reported incident was investigated and determined not to be a real security event.
2. Benign: The activity was suspicious or triggered an alert but, upon investigation, was determined to be legitimate and non-malicious (e.g., a legitimate pentest, a false positive from a new application, expected administrative activity that looked suspicious).
3. Duplicate: The reported incident was found to be a duplicate of an already existing or previously closed incident.
4. User Error / Misconfiguration: The incident was a direct result of user action or a misconfiguration that can be corrected without indicating a malicious external threat.

I attached the previous file: Final ChatLog CaseID Unique

Augment the attached dataset to ensure the name in the opened_by field is unique in comparison to the name in the caller_id field and make sure to replace all occurrences of john.doe in the dataset with the new name that you assign in the opened_by field

I attached the file: Final ChatLog Close Code Updated

Then was given a file which I said:

No make sure the caller_id is different to the opened_by name

---

**Final_ChatLog_OpenedBy_EmailCorrected**

Then was given a file which I said:

No make sure name@company.com is a different name to the opened_by field please

---

**Final_ChatLog_CallerID_Email_Unique**

Augment the attached dataset to ensure the name in name@company.com in the caller_id field is unique in comparison to the opened_by field

I attached the file: Final ChatLog Close Code Updated

---

**Final_ChatLog_CallerID_Cleaned**

Make sure the format for the caller_id is Caller number such as Caller 2403, can you remove the nina.patel from the chat log please also

---

**Final_ChatLog_CallerID_Formatted_New**

Augment the attached dataset to ensure the caller_id field value is in the format caller number for example Caller 2341 but dont use this number

---

**Final_ChatLog_CallerID_Updated_Again**

Augment the attached dataset to ensure the caller_id field value is in the format caller number for example Caller 2341 but dont use this number

I attached the file: Final ChatLog Close Code Updated

---

**Final_ChatLog_ChatUpdated_FromCaller**

Update the chat to reflect the suspicious email report came from the caller id

---

**Final_ChatLog_ChatUpdated_FromCallerID**

Augment the chat log in the attached file to reflect the suspicious email report came from the caller id

I attached the file: Final ChatLog CallerID Updated Again

---

**Augmented_Incident_Response_Data**

Augment the attached incident response dataset to ensure the opened_by and sys_created_by fields are in the format user_number, assign two unique values to each of these fields and update the assigned_to field to reflect one of them and also update the fields sys_updated_by, Case Tasks, Observables Analysis, Chat Log and resolved_by fields values where they are mentioned

I attached the file: Final ChatLog ChatUpdated FromCallerID

---

**Final Augmented Incident Data**

Augment the field name caller_id to be Reporting_User_ID and augment its value to be Reporting _User_Number

Change the value to be Reporting_User_2320 and replace anywhere that lists Caller 2320 with this

---

**Phishing_Incident_Dataset**

Create an incident response dataset using all fields from the attached dataset called Perfect_Dataset and augment the values to use the exact same format as in Perfect_Dataset but create a phishing scenario based off of the attached file Phishing Attack Response Playbook

make sure all fields names are the exact same and please provide download

I attached the file: Perfect_Dataset which is the previous file “Final Augmented Incident Data” renamed

---

**Phishing_Incident_Dataset_Complete**

you didnt use all the fields from Perfect_Dataset, remake with the exact same fields

---

**Phishing_Incident_Record**

Use the exact same field names and structure as in Perfect_Dataset.csv.

The output should be a two-column dataset with "Field" and "Value" headers.

Populate the values to reflect a realistic phishing attack based on best practices from the Phishing Attack Response Playbook.

Reuse the exact patterns for values from Perfect_Dataset.csv, such as how dates, usernames, states, and priority levels are formatted.

---

**Filled_Phoshing_Incident_Record**

fill in the values

---

**Phishing_Response_Incident**

Use all the same field names and structure from Perfect_Dataset.csv.

Match the style and format of values exactly as they appear in Perfect_Dataset.csv

Reflect a realistic phishing attack response as outlined in the Phishing Attack Response Playbook.

Output as a two-column table: "Field" and "Value".

If the original dataset contains N/A or empty values, use realistic substitutes based on the scenario.

---

**Phishing_Incident_Augmented**

Use the exact same field names and structure from Perfect_Dataset.csv.

Match the style and format of values precisely (e.g., usernames like user_123, date formats like YYYY-MM-DD HH:MM:SS, values like "2 - High", "FALSE").

Populate values to reflect a new phishing attack based on best practices described in the Phishing Attack Response Playbook.

Output the result as a two-column table with headers "Field" and "Value".

If any fields were "N/A" or empty in the original dataset, fill them in with realistic values relevant to a phishing scenario.

---

**phishing_incident_response_dataset (2)**

Using all of the following fields create a cyber incident response dataset specifically for a phishing incident.

Field Descriptions

number Identifier for the incident

incident_state Current status of the incident

active Boolean (true/false) indicating if the incident is still active

reassignment_count Number of times the incident has been reassigned to different teams or analysts

reopen_count Number of times the incident was reopened after being resolved or closed, due to the incident resolution being rejected by the caller

sys_mod_count Number of times the incident record has been updated up until that moment

made_sla Boolean indicating whether the Service Level Agreement (SLA) target was met

Reporting_User_ID Identifier of the user who reported the incident

opened_by Identifier of the user who reported the incident

opened_at Date/time when the incident was opened

sys_created_by Identifier of the user who registered the incident

sys_created_at Incident system creation date and time

sys_updated_by Identifier of the user who updated the incident

sys_updated_at Date and time of when the incident was last updated

contact_type Means by which the incident was reported

category Identifier of incident category

subcategory Identifier of incident subcategory

u_symptom Description of the user perception about service availability

impact Description of the impact caused by the incident

urgency How urgently the incident must be resolved

priority Calculated by the system based on “impact” and “urgency”

assigned_to Identifier of the user handling the incident

knowledge Boolean attribute that shows whether a knowledge base document was used to resolve the incident

notify Description of whether notifications were sent to user who should be informed of notifications for the incident

rfc Request for change identifier of the change request if there is one associated with the incident

caused_by Cause of the incident (could be a problem or change)

resolved_by Identifier of the user who marked the incident as resolved

resolved_at Incident resolution date and time

closed_at Final date and time when the incident was closed (after resolution confirmation)

Case ID The case number that is a unique identifier for each case

Case Title Title or brief description of the case

Creation Date Date when the case was created

Description Detailed description of the case

Incident Response Case (Array) This field contains several attributes of a single IR case instance. Subject: Brief summary such as “Malware detected on endpoint 1234”; Summary: Detailed narrative or executive summary of the incident; Case Tasks Title: Title or brief description of the task within the case; Case Task Start Date: Start date of the task; Case Task Assignee: User assigned to the task; Case Task Status: Current status of the task; Case Task

Duration: Duration of the task; Case Attribute Data: Additional attributes or metadata associated with the case

Observables Analysis (Array) This field contains several analysis for a single IR case instance. Analysis Type: Specifies the type of analysis conducted; Analysis ID: A unique identifier for this specific analysis; Timestamp: The date and time when the analysis was performed; Data Value: The specific data being analysed; Details: Additional information or results of analysis; Status: The final outcome of analysis

Chat Log Ticketing system chat response data

Chat Keywords Keywords extracted from chat response data

Chat Sentiment Determination Optimism: Most interactions show motivation, and high responsiveness, reflecting positivity; or Confidence: Most interactions reflect assurance, clear decision-making, and composed communication; or Frustration: Most interactions show misunderstanding, dissatisfaction or challenges with problem solving; or Urgency: Most interactions show a need for immediate action, time sensitivity, and critical importance; or Conflict: Most interactions show disagreement and differing perspectives

Event ID Unique identifier for each event

Distribution How the information within an event or attribute is shared with other organisations or participants in the MISP community

Threat Level Assessed threat level of the event

Read and understand the sample phishing response process described in the file Phishing Attack Response Playbook.docx.

Use the exact same field names and structure from Perfect_Dataset.csv. Match the style and format of values precisely.

Format the output as a two-column dataset with Field and Value.

Output the final dataset in CSV format for download.