

Hands-on Lab: Cybersecurity Incident Reports and Playbook Generation using Generative AI



Estimated time needed: 30 minutes

Introduction

Welcome to the hands-on lab, Cybersecurity Incident Reports and Playbook Generation using Generative AI.

A cybersecurity report and playbook are essential for an organization's efforts to manage and respond to cybersecurity incidents.

A cybersecurity incident report is a comprehensive document that provides an overview of the organization's current cybersecurity posture, incidents, and the steps to address them. It serves as a tool for internal and external communication and is often used to inform stakeholders about the state of cybersecurity within the organization.

Learning objectives

After completing this lab, you will be able to:

- Apply Generative AI in comprehensive incident report generation.
- Customize cybersecurity playbooks with Generative AI assistance.

Let's get started with prompting and experimenting with the models.

Exercise 1: Cybersecurity Incident Report Generation Using Generative AI

In this lab, we will use a Generative AI platform to generate a cybersecurity incident report in standard format.

We will use the below hypothetical scenario of a cyber attack incident in the organization:

The cyber attack unfolded in a multi-stage timeline, starting with the initial compromise on day one. During this phase, the threat actors employed a malicious attachment carrying a custom-designed trojan, carefully crafted to bypass traditional antivirus detection mechanisms. Moving to the establishing persistence phase on day seven, the attackers initiated command and control (C2) activities. They successfully established a covert communication channel to external servers, providing them with remote control capabilities over the compromised system. In the lateral movement and reconnaissance phase during weeks two through four, attackers leveraged compromised credentials to move laterally across the network. They meticulously mapped the organization's infrastructure and executed privilege escalation strategies, exploiting vulnerabilities in unpatched systems. This strategy allowed the threat actors to elevate their privileges, gaining access to critical servers and databases. During the data exfiltration phase in weeks five and six, the APT group focused on identifying and exfiltrating sensitive customer financial data. The attackers utilized encrypted channels to avoid detection and adopted a subtle approach, slowly exfiltrating data in small, inconspicuous quantities.

Now, let's generate an incident report in a standard format for this scenario.

Step 1: Copy and paste the prompt Instruction in 'message' input box.

Generate a cyber incident report in the standard format for the given cyber attack incident.

Step 2: Copy and paste the incident report in 'message' input box just after the prompt instructions within double quotes.

The cyber attack unfolded in a multi-stage timeline, starting with the initial compromise on day one. During this phase, the threat actors employed a malicious attachment carrying a custom-designed trojan, carefully crafted to bypass traditional antivirus detection mechanisms. Moving to the establishing persistence phase on day seven, the attackers initiated command and control (C2) activities. They successfully established a covert communication channel to external servers, providing them with remote control capabilities over the compromised system. In the lateral movement and reconnaissance phase during weeks two through four, attackers leveraged compromised credentials to move laterally across the network. They meticulously mapped the organization's infrastructure and executed privilege escalation strategies, exploiting vulnerabilities in unpatched systems. This strategy allowed the threat actors to elevate their privileges, gaining access to critical servers and databases. During the data exfiltration phase in weeks five and six, the APT group focused on identifying and exfiltrating sensitive customer financial data. The attackers utilized encrypted channels to avoid detection and adopted a subtle approach, slowly exfiltrating data in small, inconspicuous quantities.

Step 3: Click on **Start Chat** and examine the response. The system will generate a detailed incident report with Timeline and Recommendations.

Cyber Incident Report:

Title: The Cyber Attack Incident

Summary: The cyber attack unfolded in a multi-stage timeline, starting with the initial compromise on day one. During this phase, the threat actors employed a malicious attachment carrying a custom-designed trojan, carefully crafted to bypass traditional antivirus detection mechanisms. Moving to the establishing persistence phase on day seven, the attackers initiated command and control (C2) activities. They successfully established a covert communication channel to external servers, providing them with remote control capabilities over the compromised system.

Timeline:

- Day 1: Initial Compromise
 - Threat actors used a malicious attachment carrying a custom-designed trojan.
 - Trojan bypassed traditional antivirus detection mechanisms.
- Day 7: Establishing Persistence
 - Attackers initiated command and control (C2) activities.
 - Covert communication channel to external servers was established.
 - Remote control capabilities over the compromised system were obtained.
- Weeks 2-4: Lateral Movement and Reconnaissance
 - Attackers leveraged compromised credentials to move laterally across the network.
 - Meticulous mapping of the organization's infrastructure took place.
 - Privilege escalation strategies were executed, exploiting vulnerabilities in unpatched systems.
 - Access to critical servers and databases was gained.
- Weeks 5-6: Data Exfiltration
 - APT group focused on identifying and exfiltrating sensitive customer financial data.
 - Encrypted channels were utilized to avoid detection.
 - Data was slowly exfiltrated in small, inconspicuous quantities.

Recommendations:

1. Enhance Email Security:
 - Implement advanced email filtering mechanisms to detect and block malicious attachments.
 - Educate employees on identifying and avoiding phishing attempts.
2. Regular Patching and Vulnerability Management:
 - Establish a robust patch management process to ensure timely updates of software and systems.
 - Conduct regular vulnerability assessments and prioritize patching based on criticality.
3. Network Segmentation and Access Controls:
 - Implement network segmentation to limit lateral movement within the network.
 - Enforce strong access controls and regularly review user privileges.
4. Intrusion Detection and Monitoring:
 - Deploy intrusion detection systems to detect and alert on suspicious network activities.
 - Implement centralized logging and monitoring to identify potential security incidents.
5. Data Loss Prevention:
 - Implement data loss prevention mechanisms to detect and prevent unauthorized data exfiltration.
 - Encrypt sensitive customer data to protect it from unauthorized access.

Please note that this incident report is based on the information provided and may require further investigation and analysis for a comprehensive understanding of the cyber attack incident.

Note: The response generated by the Generative AI platform may vary as it is dynamic in behavior, and you may need to tweak your prompt instructions to get a better response.

Exercise 2: Cybersecurity Playbook Using Generative AI

A cybersecurity playbook is a detailed document outlining specific procedures and actions to respond to cybersecurity incidents. It provides a step-by-step guide for cybersecurity teams facing different threats or attacks. The playbook is a proactive approach to incident response, ensuring that the team is well-prepared to handle a variety of scenarios.

In this lab, you will generate a cybersecurity playbook for a malware attack.

Step 1: Copy and paste the prompt Instruction in 'message' input box.

A malware attack has compromised my organization. I have a lot of data related to customer and vendor information. Please help me wi

Step 2: Click on **Start Chat** and examine the response. The system has generated a playbook for responding to a Malware Attack. The sample response is shown below.

Sample Output

Playbook for Responding to a Malware Attack:

1. Activate Incident Response Team:
 - Immediately assemble a dedicated team of cybersecurity experts to respond to the malware attack.
 - Assign specific roles and responsibilities to team members, including incident coordinator, technical analysts, and communication liaison.
2. Isolate Infected Systems:
 - Identify and isolate the compromised systems from the network to prevent further spread of the malware.
 - Disconnect affected systems from the internet and other network resources.
3. Collect Forensic Evidence:
 - Preserve and collect evidence related to the malware attack for further analysis and potential legal actions.
 - Capture memory dumps, network traffic logs, and any other relevant artifacts.
4. Analyze Malware:
 - Conduct a thorough analysis of the malware to understand its behavior, capabilities, and potential impact.
 - Use sandbox environments or specialized tools to safely analyze the malware without risking further infections.
5. Remediate Infected Systems:
 - Remove the malware from infected systems using reputable antivirus or antimalware software.
 - Update all software and systems to the latest versions to patch vulnerabilities exploited by the malware.
6. Restore Systems from Backups:
 - Restore affected systems from clean backups to ensure their integrity and minimize the impact of the malware attack.
 - Verify the backups for any signs of compromise before restoring.
7. Enhance Security Measures:
 - Strengthen security controls and measures to prevent future malware attacks.
 - Implement advanced endpoint protection solutions, intrusion detection systems, and network monitoring tools.
8. Communicate with Stakeholders:
 - Notify relevant stakeholders, including customers and vendors, about the malware attack and its potential impact on their data.
 - Provide regular updates on the incident response progress and steps taken to mitigate the attack.
9. Conduct Post-Incident Analysis:
 - Perform a thorough post-incident analysis to identify the root cause of the malware attack and any vulnerabilities in the organization's security posture.
 - Implement necessary improvements and lessons learned from the incident response process.
10. Employee Awareness and Training:
 - Conduct regular cybersecurity awareness training for employees to educate them about malware threats, phishing attempts, and safe computing practices.
 - Encourage reporting of suspicious activities or potential security incidents.

It is important to note that this playbook provides general guidance and may need to be tailored based on the specific circumstances and requirements of your organization. Additionally, it is advisable to consult with cybersecurity professionals and legal experts to ensure a comprehensive and effective response to the malware attack.

Note: The response of the ChatGPT platform is dynamic in behavior and may sometimes show different results. You can repeat the query to get the most satisfying response.

Next Step

Complete the exercise provided in the following section to assess your skills.

Exercises

Do the following exercises:

1. Generate the Incident Summary with an impact assessment of the malware attack scenario discussed in hands-on exercise.
► [Click here for an example solution](#)
2. Generate a playbook for phishing attack .
► [Click here for an example solution](#)
3. Generate a playbook for Ransomware attack on critical infrastructure.
► [Click here for an example solution](#)

Summary

Generative AI can revolutionize cybersecurity incident reporting by automatically generating detailed and coherent reports.

- By analyzing incident data, AI models can provide concise summaries, enhance language clarity, and facilitate automated documentation of incident response processes.
- Moreover, in incident playbooks, Generative AI can craft scenario-specific, dynamic playbooks that adapt to evolving threats.
- Natural language interfaces and interactive guidance powered by AI can assist incident responders in real-time, offering valuable insights and recommendations.
- Additionally, Generative AI contributes to decision support through predictive analytics, risk assessment, and dynamic adaptation, empowering organizations to respond to cybersecurity threats proactively.

Author(s)

[Dr. Manish Kumar](#)

© IBM Corporation. All rights reserved.