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
Moving to the establishing persistence phase on day seven, the attackers initiated command and control (C2) activities. They success
In the lateral movement and reconnaissance phase during weeks two through four, attackers leveraged compromised credentials to move
During the data exfiltration phase in weeks five and six, the APT group focused on identifying and exfiltrating sensitive customer f
```

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

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

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