Hands-on Lab: Incident Response and Alert Generation Using Generative AI

Estimated time needed: 25 minutes

Introduction

In incident response, quickly sorting and prioritizing alerts is crucial. Generative AI helps speed up this process by swiftly analyzing security alerts and categorizing them based on their severity and relevance to the environment.

Automating this triage process is significant because it streamlines security team workflows. By having alerts sorted, security professionals can concentrate on tackling the most urgent threats first, saving time and bolstering overall security.

Generative AI's automated triage capabilities are invaluable in cybersecurity, strengthening defenses and protecting digital environments from emerging threats. In this experiment, you will learn how to use generative AI for alert prioritization and communication with administrators using synthetic data from a sample scenario.

Learning objective

After completing this lab, you will be able to:

- Leverage the capability of generative AI to aid in the automated triage of security incidents

Log analysis and prioritization

Example scenario: Imagine a bank equipped with a fully IT-enabled system. You are a security analyst in the bank and have received five different cyberattack alerts corresponding to five types of cyberattacks.

1. SQL injection attack alert: alert message: `SQL injection attempt detected in web server logs. Suspicious input: ‘; DROP TABLE Users–`
2. Zero-day exploit alert: alert message: `Unusual system behavior detected on Server X. Possible zero-day exploit. Investigate abnormal code execution patterns.`
3. Man-in-the-middle (MitM) attack alert: alert message: `Anomalous SSL/TLS certificate changes during secure communication. Potential Man-in-the-Middle attack detected. Investigate immediately`
4. Advanced persistent threat (APT) alert: alert message: `Persistent unauthorized access attempts across multiple systems. Possible APT campaign detected. Implement enhanced monitoring and investigate further.`
5. Cross-site scripting (XSS) attack alert: alert message: `Client-side script injection detected in web application logs. Malicious script found in user input. Possible Cross-Site Scripting (XSS) attack. Investigate and mitigate.`

   Note: These examples are generic and do not contain real-world data. Detailed investigation, correlation with other logs, and additional context would be required to confirm and respond to such alerts appropriately in a real scenario.

Now, with the help of generative AI, let's accomplish the following tasks:

1. Analyze the logs and prioritize them (high, medium, low) based on the severity of the incident.
2. Email the administrators about the high priority incident.

Exercise 1: Log alert prioritization

Step 1:- Copy and paste the following prompt in the message input box.

```
Assign the three priorities "Low” “Medium” and “High” to the logs generated by the security system
```

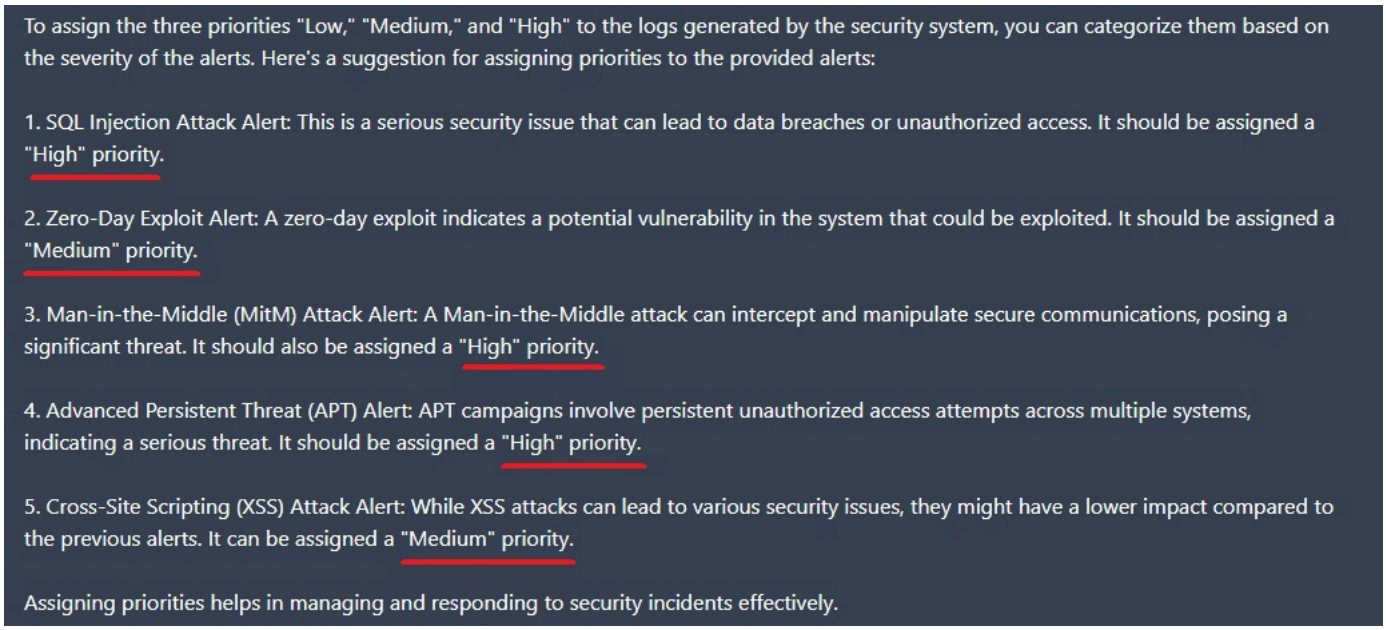
Step 2: Copy and paste the following security system logs in the message input box following the prompt instructions.

```
1. SQL injection attack alert: alert message: SQL injection attempt detected in web server logs. Suspicious input: ‘; DROP TABLE Use
2. Zero-day exploit alert: alert message: Unusual system behavior detected on Server X. Possible zero-day exploit. Investigate abnor
3. Man-in-the-middle (MitM) attack alert: alert message: Anomalous SSL/TLS certificate changes during secure communication. Potentia
4. Advanced persistent threat (APT) alert: alert message: Persistent unauthorized access attempts across multiple systems. Possible
5. Cross-site scripting (XSS) attack alert: alert message: Client-side script injection detected in web application logs. Malicious
```

Step 3: Select **Start Chat**

Step 4: Examine the response.

Sample output



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: Automatic email communication for high priority alerts

After prioritizing the threat alerts, it may be necessary to convey the high-priority alert to the system administrator for appropriate action. This process can be automated using a generative AI model.

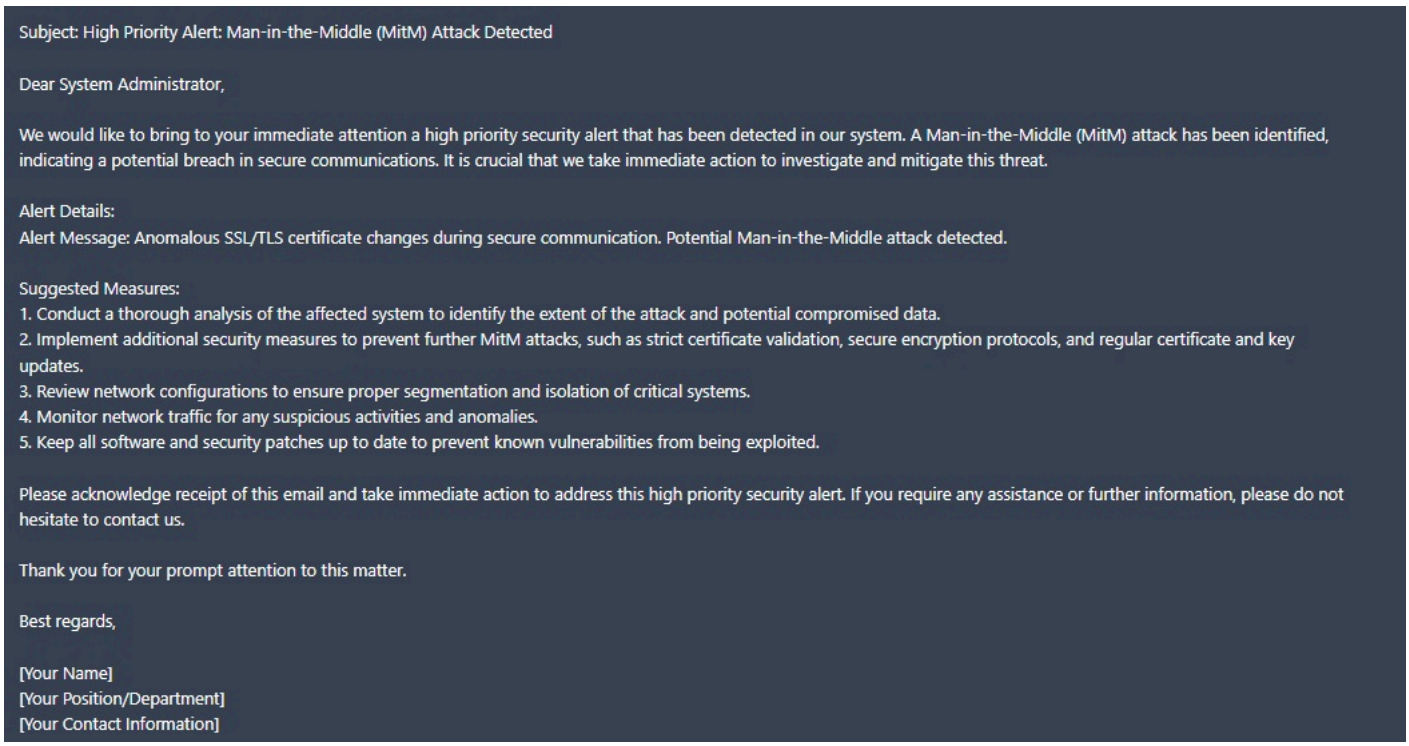
Continuing the experiment, we will attempt to generate an automated email using a generative AI platform. The goal is to create an email that effectively communicates the high-priority alert to the system administrator. The email should include details of the high-priority alert and suggest appropriate measures to address it.

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

```
Generate an email to communicate the high-priority alert to the system admin. The email message should contain the priority alert de
```

Step 2: Review the response.

Sample output



Exercises

Do the following exercise based on the system logs used in the hands-on exercise:

1. Determine the alert indicating a potential security breach requiring immediate communication with the web server administrator.

▼ Click here for an example solution
Identify the critical alert triggering an immediate notification to the web server administrator due to a potential security breach in the system log.

2. Identify the security incident alert that must be communicated to the network administrator.

▼ Click here for an example solution
Specify the security incident alert necessitating communication to the network administrator in the system logs.

3. Prioritize the security alerts into categories of High, Medium, and Low, and arrange them chronologically from highest to lowest priority. Generate the email communication to send the list of alerts in chronological order from highest to lowest priority to the system administrator.

▼ Click here for an example solution
Prioritize security alerts into 'High, Medium, and Low' categories and arrange them chronologically by priority. Then, compose an email to send the list of alerts, starting with the highest priority, to the system administrator based on the given system logs.

Summary

Congratulations on completing the hands-on lab, Incident Response and Alert Generation Using Generative AI.

In this lab:

- You have explored the capabilities of the generative AI platform for incident analysis and prioritization.
- You can train the generative AI model specifically to the need of the organization to automate security incident triage by swiftly analyzing data, generating alerts for potential threats, and prioritizing them based on severity and relevance.
- This action accelerates response times, allowing security teams to promptly address the most critical issues and strengthen overall cybersecurity defenses.

Author(s)

Manish Kumar