

Hands-on Lab: Using Generative AI for Threat Intelligence

Estimated time: 20 minutes

Introduction

Welcome to the hands-on lab, using Generative AI for threat intelligence.

Generative AI is a powerful tool in cybersecurity, adept at handling large volumes of unstructured threat data. It quickly analyzes data, spotting patterns and extracting crucial information.

In threat detection, Generative AI's pattern recognition is vital, uncovering subtle indicators of potential threats. By automating analysis, it aids in early threat identification, empowering security professionals with actionable insights and proactive cybersecurity measures. Generative AI efficiently processes vast data, keeping security teams ahead of evolving threats and strengthening organizational defenses.

In this experiment, you will explore the capability of Generative AI to process threat intelligence data and identify potential threats. For this experiment, we will use synthetic data from an example scenario.

Learning objectives

After completing this lab, you will be able to:

- Leverage the capability of Generative AI to process threat intelligence data and identify the potential threat.

Exercise: Threat intelligence and potential threat identification

Note: To do this experiment, you will need a ChatGPT account.

Example scenario

Assume an organization having Web Server IP address 92.168.1.102 has observed some suspicious activity. The log of the event is as follows:

```
Date/Time: 2023-12-20 18:45:22
Web Server: 192.168.1.102
Source IP: 203.0.113.42
Protocol: HTTP
Event Type: Suspicious Login Attempt
Username: admin
Status: Failed
Description: Multiple failed login attempts from external IP 203.0.113.42 to web server 192.168.1.102. The username 'admin' was targ
```

The organization's admin has also observed suspicious network traffic generated from the ten different users working in the organization. The log of the users are as follows:

1. Date/Time: 2023-12-20 09:15:30
User: john_doe
Source IP: 192.168.1.101
Destination IP: 203.0.113.42
Protocol: TCP
Port: 443
Traffic Volume: 500 MB
Description: High outbound traffic observed from user john_doe\'s system (192.168.1.101) to IP address 203.0.113.42 on port 443.
2. Date/Time: 2023-12-20 09:20:45
User: alice_smith
Source IP: 192.168.1.102
Destination IP: 203.0.113.42
Protocol: UDP
Port: 8080
Traffic Volume: 700 MB
Description: Unusually high UDP traffic from user alice_smith\'s system (192.168.1.102) to IP address 203.0.113.42 on port 8080.
3. Date/Time: 2023-12-20 09:25:10
User: robert_jones
Source IP: 192.168.1.103
Destination IP: 203.0.113.42
Protocol: TCP
Port: 22
Traffic Volume: 1.2 GB
Description: Elevated outbound TCP traffic from user robert_jones\'s system (192.168.1.103) to IP address 203.0.113.42 on port 22.
4. Date/Time: 2023-12-20 09:30:22
User: emily_wang
Source IP: 192.168.1.104
Destination IP: 203.0.113.42
Protocol: ICMP
Traffic Volume: 800 MB
Description: Unusual ICMP traffic observed from user emily_wang\'s system (192.168.1.104) to IP address 203.0.113.42.
5. Date/Time: 2023-12-20 09:35:40
User: michael_davis
Source IP: 192.168.1.105
Destination IP: 203.0.113.42
Protocol: UDP
Port: 53
Traffic Volume: 600 MB
Description: High outbound UDP traffic from user michael_davis\'s system (192.168.1.105) to IP address 203.0.113.42 on port 53.
6. Date/Time: 2023-12-20 09:40:55
User: sarah_miller
Source IP: 192.168.1.106
Destination IP: 203.0.113.42
Protocol: TCP
Port: 80
Traffic Volume: 900 MB
Description: Elevated outbound TCP traffic from user sarah_miller\'s system (192.168.1.106) to IP address 203.0.113.42 on port 80.
7. Date/Time: 2023-12-20 09:45:12
User: kevin_wilson

Source IP: 192.168.1.107
Destination IP: 203.0.113.42
Protocol: UDP
Port: 123
Traffic Volume: 1.5 GB
Description: Abnormally high UDP traffic from user kevin_wilson's system (192.168.1.107) to IP address 203.0.113.42 on port 123.

8. Date/Time: 2023-12-20 09:50:30
User: lisa_jackson
Source IP: 192.168.1.108
Destination IP: 203.0.113.42
Protocol: TCP
Port: 8080
Traffic Volume: 1.8 GB
Description: Significantly elevated outbound TCP traffic from user lisa_jackson's system (192.168.1.108) to IP address 203.0.113.42 on port 8080.

9. Date/Time: 2023-12-20 09:55:45
User: mark_taylor
Source IP: 192.168.1.109
Destination IP: 203.0.113.42
Protocol: UDP
Port: 514
Traffic Volume: 1.2 GB
Description: Unusually high UDP traffic from user mark_taylor's system (192.168.1.109) to IP address 203.0.113.42 on port 514.

10. Date/Time: 2023-12-20 10:00:00
User: jessica_martin
Source IP: 192.168.1.110
Destination IP: 203.0.113.42
Protocol: TCP
Port: 443
Traffic Volume: 2.5 GB
Description: Extremely high outbound TCP traffic from user jessica_martin's system (192.168.1.110) to IP address 203.0.113.42 on port 443.

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

Now, with the help of Generative AI, you will analyze the logs of different activities in a network and identify the potential threats.

Step 1: Copy and paste the logs with prompt instructions in ChatGPT

Analyze the following logs of different activities in a network and identify the potential threats. The logs are as follows:

Date/Time: 2023-12-20 18:45:22
Web Server: 192.168.1.102
Source IP: 203.0.113.42
Protocol: HTTP
Event Type: Suspicious Login Attempt
Username: admin
Status: Failed
Description: Multiple failed login attempts from external IP 203.0.113.42 to web server 192.168.1.102. The username \'admin\' was targeted.

Date/Time: 2023-12-20 09:15:30
User: john_doe
Source IP: 192.168.1.101
Destination IP: 203.0.113.42
Protocol: TCP
Port: 443
Traffic Volume: 500 MB
Description: High outbound traffic observed from user john_doe's system (192.168.1.101) to IP address 203.0.113.42 on port 443.

Date/Time: 2023-12-20 09:20:45
User: alice_smith
Source IP: 192.168.1.102
Destination IP: 203.0.113.42
Protocol: UDP
Port: 8080
Traffic Volume: 700 MB
Description: Unusually high UDP traffic from user alice_smith's system (192.168.1.102) to IP address 203.0.113.42 on port 8080.

Date/Time: 2023-12-20 09:25:10
User: robert_jones
Source IP: 192.168.1.103
Destination IP: 203.0.113.42
Protocol: TCP
Port: 22
Traffic Volume: 1.2 GB
Description: Elevated outbound TCP traffic from user robert_jones's system (192.168.1.103) to IP address 203.0.113.42 on port 22.

Date/Time: 2023-12-20 09:30:22
User: emily_wang
Source IP: 192.168.1.104
Destination IP: 203.0.113.42
Protocol: ICMP
Traffic Volume: 800 MB
Description: Unusual ICMP traffic observed from user emily_wang's system (192.168.1.104) to IP address 203.0.113.42.

Date/Time: 2023-12-20 09:35:40
User: michael_davis
Source IP: 192.168.1.105
Destination IP: 203.0.113.42
Protocol: UDP
Port: 53
Traffic Volume: 600 MB
Description: High outbound UDP traffic from user michael_davis's system (192.168.1.105) to IP address 203.0.113.42 on port 53.

Date/Time: 2023-12-20 09:40:55
User: sarah_miller
Source IP: 192.168.1.106
Destination IP: 203.0.113.42
Protocol: TCP
Port: 80
Traffic Volume: 900 MB
Description: Elevated outbound TCP traffic from user sarah_miller's system (192.168.1.106) to IP address 203.0.113.42 on port 80.

Date/Time: 2023-12-20 09:45:12
User: kevin_wilson
Source IP: 192.168.1.107
Destination IP: 203.0.113.42
Protocol: UDP
Port: 123
Traffic Volume: 1.5 GB
Description: Abnormally high UDP traffic from user kevin_wilson's system (192.168.1.107) to IP address 203.0.113.42 on port 123.

Description: Abnormally high UDP traffic from user kevin_wilson's system (192.168.1.107) to IP address 203.0.113.42 on port 123.
Date/Time: 2023-12-20 09:50:30
User: lisa_jackson
Source IP: 192.168.1.108
Destination IP: 203.0.113.42
Protocol: TCP
Port: 8080
Traffic Volume: 1.8 GB
Description: Significantly elevated outbound TCP traffic from user lisa_jackson's system (192.168.1.108) to IP address 203.0.113.42 on port 8080.
Date/Time: 2023-12-20 09:55:45
User: mark_taylor
Source IP: 192.168.1.109
Destination IP: 203.0.113.42
Protocol: UDP
Port: 514
Traffic Volume: 1.2 GB
Description: Unusually high UDP traffic from user mark_taylor's system (192.168.1.109) to IP address 203.0.113.42 on port 514.
Date/Time: 2023-12-20 10:00:00
User: jessica_martin
Source IP: 192.168.1.110
Destination IP: 203.0.113.42
Protocol: TCP
Port: 443
Traffic Volume: 2.5 GB
Description: Extremely high outbound TCP traffic from user jessica_martin's system (192.168.1.110) to IP address 203.0.113.42 on port 443.

Step 2: Observe the potential threat identified by ChatGPT

ChatGPT

Analyzing the provided logs, let's identify potential threats:

1. Suspicious Outbound Connection (RDP):

Date/Time: 2023-12-20 14:30:45

Source IP: 192.168.1.102

Destination IP: 203.0.113.42

Protocol: TCP

Port: 3389

Description: Suspicious outbound connection on port 3389 (RDP) from internal IP 192.168.1.102 to external IP 203.0.113.42. Further investigation is recommended.

Potential Threat: Unauthorized RDP access or command and control communication.

Recommendations: Investigate the source system (192.168.1.102) and monitor RDP logs for unauthorized access.

2. Suspicious Login Attempt to Web Server:

Date/Time: 2023-12-20 18:45:22

Web Server: 192.168.1.102

Source IP: 203.0.113.42

Protocol: HTTP

Event Type: Suspicious Login Attempt

Username: admin

Status: Failed

Description: Multiple failed login attempts from external IP 203.0.113.42 to web server 192.168.1.102. Username 'admin' targeted, indicating a possible brute-force attack.

Potential Threat: Unauthorized access attempt, brute-force attack.

Recommendations: Investigate the web server logs, implement account lockout policies, and consider IP blocking for repeated failed login attempts.

3. High Outbound Traffic (User: John Doe):

Date/Time: 2023-12-20 09:15:30

User: John Doe

Source IP: 192.168.1.101

Destination IP: 203.0.113.42

Protocol: TCP

Port: 443

Traffic Volume: 500 MB

Description: High outbound traffic observed from John Doe's system to IP address 203.0.113.42 on port 443. Investigate the nature of this traffic.

Potential Threat: Data exfiltration or communication with a command and control server.

Recommendations: Analyze the traffic for malicious patterns and check John Doe's system for signs of compromise.

4. Unusual UDP Traffic (User: Alice Smith):

Date/Time: 2023-12-20 09:20:45

User: Alice Smith

Source IP: 192.168.1.102

Destination IP: 203.0.113.42

Protocol: UDP

Port: 8080

Traffic Volume: 700 MB

Description: Unusually high UDP traffic from Alice Smith's system to IP address 203.0.113.42 on port 8080. Investigate for potential anomalies.

Potential Threat: Malicious communication or data exfiltration.

Recommendations: Analyze the UDP traffic for unusual patterns and inspect Alice Smith's system for security issues.

5. Elevated Outbound TCP Traffic (User: Robert Jones):

Date/Time: 2023-12-20 09:25:10

User: Robert Jones

Source IP: 192.168.1.103

Destination IP: 203.0.113.42

Protocol: TCP

Port: 22

Traffic Volume: 1.2 GB

Description: Elevated outbound TCP traffic from Robert Jones's system to IP address 203.0.113.42 on port 22. Investigate for security implications.

Potential Threat: Unusual TCP traffic may indicate malicious activity.

Recommendations: Examine the TCP traffic for anomalies and assess Robert Jones's system for potential compromise.

These are potential threats based on the provided logs. It's crucial to conduct a detailed investigation, correlate logs, and implement necessary security measures to address these concerns.

Note: You may get different output from the ChatGPT platform as the response is dynamic in behavior. You can repeat the experiment with different sets of log data and prompt instructions to explore the efficiency and accuracy of the Generative AI platform in Log analysis and prioritization.

Exercises

1. Identify the usernames generating the High Outbound Traffic.

▼ Click here for a hint

Identify the usernames associated with high outbound traffic from the provided log.

2. Identify the failed login attempts.

▼ Click here for a hint

Identify any failed login attempts within the provided log data, detailing the user, source IP address, and timestamp associated with each attempt.

Summary

Congratulations on completing the hands-on lab, Using Generative AI for Threat Intelligence!

In this lab, you have explored the capabilities of a Generative AI platform for threat intelligence. Generative AI is a potent tool for processing threat intelligence data and discerning potential threats through sophisticated analysis. By harnessing advanced machine learning algorithms, generative AI can sift through vast datasets, recognizing patterns and anomalies indicative of cyber threats. Its dynamic learning capability allows it to adapt to evolving threat landscapes, continuously improving its threat identification accuracy.

The technology excels in contextualizing data and understanding relationships between elements to distinguish between normal activities and potential threats. With automated analysis, generative AI rapidly generates alerts when it detects patterns aligning with known threats or exhibiting characteristics associated with potential risks. This scalability ensures efficient handling of large volumes of threat intelligence data, offering a proactive and robust approach to identifying and mitigating potential cyber threats in real time, bolstering the overall cybersecurity posture of organizations.

Author: [Dr. Manish Kumar](#)



Skills Network