Project title : AI-powered threat hunting tool

Abstract

The goal of this project is to develop a tool that proactively hunts for threats in network data, employing AI algorithms to identify potential vulnerabilities. The tool will be designed to be scalable, efficient, and effective in detecting a wide range of threats, including known vulnerabilities, zero-day vulnerabilities, and emerging threats.

The tool will work by collecting network data from a variety of sources, such as firewalls, intrusion detection systems, and network monitoring tools. The data will then be preprocessed to clean it up and make it consistent. Next, an AI model will be used to identify potential vulnerabilities in the data. The model will be trained on a dataset of known vulnerabilities, as well as data from real-world networks.

Once the AI model has identified potential vulnerabilities, the tool will prioritize them based on their severity and exploitability. The tool will then generate alerts for the security team to investigate. The alerts will include information about the vulnerability, the severity of the vulnerability, and the steps that the security team can take to mitigate the vulnerability.

Key components of this project include:

1. **Data Collection and Preprocessing**: Gathering and preprocessing network traffic data to create a clean and representative dataset for training AI models.

2. **AI Model Development**: Designing and training machine learning and deep learning models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and clustering algorithms, to identify patterns and anomalies in network traffic.

3. **Real-Time Monitoring**: Implementing a real-time monitoring system that continuously assesses network traffic for potential threats, providing immediate alerts and automated responses when anomalies are detected.

4. **Adaptability**: Ensuring that the system can self-learn and adapt to new attack vectors and variations over time, reducing false positives and increasing detection accuracy.

User-Friendly Interface: Creating a user-friendly dashboard for security administrators to monitor and manage the IDS, configure policies, and respond to alerts effectively.

The Proactive Threat Hunting Tool is a valuable tool for security analysts who are struggling to keep up with the increasing volume and complexity of network data and the sophistication of cyberattacks. By automating the process of threat hunting and providing security analysts with insights into the latest threats and vulnerabilities, the Proactive Threat Hunting Tool can help security analysts to identify and respond to threats more quickly and effectively.