Abstract

Cyber threats are constantly evolving, making it challenging for security teams to stay ahead of the curve. An AI-based threat intelligence platform can help security teams by automating the collection, aggregation, and analysis of threat data from a variety of sources. This provides security teams with actionable insights to help them detect, prevent, and respond to cyber-attacks more effectively.

This project aims to develop and deploy an AI-based threat intelligence platform. The platform will collect and analyse threat data from a variety of sources, including open-source feeds, dark web monitoring, and proprietary feeds. It will then use machine learning and AI algorithms to identify patterns and insights in the data. This information will be used to generate actionable alerts and reports for security analysts.

The project will be completed in four phases: Planning: This phase will involve defining the project scope, objectives, and deliverables. Key stakeholders will be identified and their roles assigned. A detailed project plan will be created, including timelines and resource allocation. Data Collection and Preprocessing: This phase will involve identifying and selecting relevant threat intelligence sources. Data collection mechanisms will be developed and implemented. Collected data will be pre-processed to clean and normalize it. Machine Learning Model Development and Deployment: This phase will involve choosing appropriate machine learning algorithms for threat detection and emerging threat identification. Models will be trained and fine-tuned using historical threat data. Models will then be deployed to production. User Interface Design, Development, and Deployment: This phase will involve designing and developing a user-friendly interface for security analysts and users to access threat intelligence data. Customizable dashboards and reports will be created for different user roles. Collaboration features will be implemented to facilitate information sharing among security teams. The user interface will be deployed to production and made available to users.

Once the platform is deployed, it will be thoroughly tested for functionalities and security measures. It will then be deployed in a controlled environment and gradually rolled out to production. A maintenance plan will be established for ongoing updates, bug fixes, and improvements.