PROJECT DESIGN PHASE

SOLUTION ARCHITECTURE TEMPLATE

DATE	19 September 2023
TEAM ID	5.1
PROJECT NAME	Project – AI based threat intelligence platform

SOLUTION ARCHITECTURE TEMPLATE

The solution architecture of an AI-based threat intelligence platform typically consists of the following components:

- Data ingestion: This component is responsible for collecting security data from a variety of sources, such as system logs, network traffic, user behaviour, and external threat intelligence feeds. The data is then normalized and stored in a centralized location for analysis.

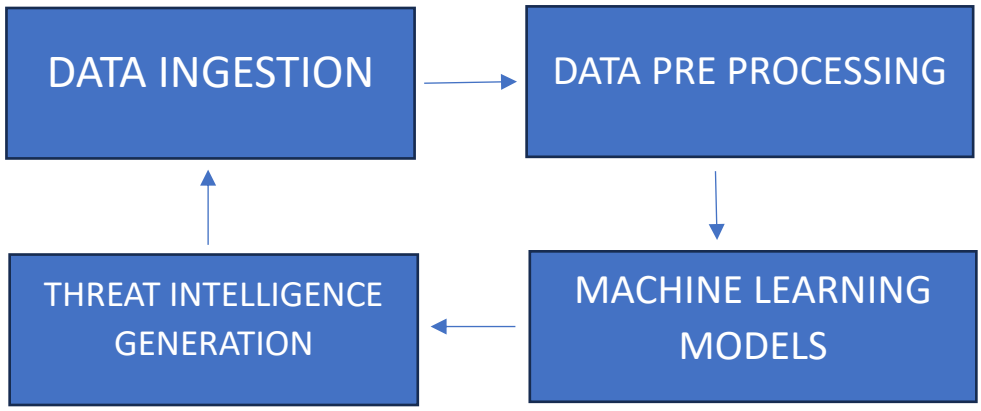
- Data preprocessing: This component prepares the ingested data for machine learning by cleaning, transforming, and feature engineering.

- Machine learning models: This component uses machine learning algorithms to analyse the pre-processed data and identify patterns and anomalies that may indicate potential threats.

- Threat intelligence generation: This component converts the output of the machine learning models into human-readable and actionable threat intelligence reports.

- Threat intelligence dissemination: This component distributes the threat intelligence reports to security analysts and other stakeholders across the organization.

DIAGRAM



Data ingestion

The data ingestion component collects security data from a variety of sources, such as:

- System logs (e.g., firewall logs, application logs, operating system logs).
- Network traffic (e.g., NetFlow data, packet captures).
- User behaviour data (e.g., login data, file access data, web browsing data).
- External threat intelligence feeds (e.g., feeds from security vendors, government agencies, and open-source sources).

Data preprocessing

The data preprocessing component prepares the ingested data for machine learning by cleaning, transforming, and feature engineering. This may involve:

- Removing noise and outliers from the data
- Transforming the data into a format that is compatible with the machine learning algorithms
- Creating new features from the existing data that may be more predictive of potential threats.

Machine learning models:

The machine learning models component uses machine learning algorithms to analyse the pre-processed data and identify patterns and anomalies that may indicate potential threats. There are a variety of machine learning algorithms that can be used for this purpose, such as supervised learning, unsupervised learning, and deep learning.

Threat intelligence generation:

The threat intelligence generation component converts the output of the machine learning models into human-readable and actionable threat intelligence reports. This may involve:

- Correlating data from multiple sources to get a more complete picture of a threat
- Enriching the data with additional information, such as the threat actor's motivations and capabilities
- Prioritizing the threats based on their severity and impact to the organization