Project Design Phase-I
Solution Architecture

Date	19 october 2023
Team ID	5.2
Project Name	AI-Enhanced Threat Intelligence Platform
Maximum Marks	4 Marks

Solution Architecture:

Data Analysis: AI is used to analyze large volumes of data from various sources, including network logs, user behavior, and external threat feeds. Machine learning models can identify anomalies and potential threats in real-time.

Pattern Recognition: ML algorithms can identify patterns in historical threat data. This helps in predicting and preventing future attacks based on similarities with past incidents.

Behavior Analysis: AI can monitor user and system behavior, looking for deviations that may indicate a security breach. It can learn what "normal" behavior looks like and raise alerts when anomalies occur.

Automation: AI-driven threat intelligence platforms can automate responses to certain types of threats. For example, they can block specific IP addresses, quarantine compromised devices, or perform other predefined actions.

Threat Feed Analysis: AI can sift through massive threat data feeds and prioritize potential threats. This helps security analysts focus on the most critical issues.

Natural Language Processing (NLP): NLP is used for analyzing textual data like security reports, blogs, and news articles. It helps in understanding and categorizing threats and vulnerabilities.

Predictive Analytics: Machine learning models can predict potential threats by analyzing historical data and current trends, allowing organizations to proactively strengthen their security posture.

Adaptive Learning: AI can continuously adapt and improve its threat detection capabilities. As it encounters new threats, it can learn to identify them and incorporate this knowledge into its algorithms.

User and Entity Behavior Analytics (UEBA): AI-driven UEBA systems monitor and analyze user and entity behavior to detect insider threats and account compromise.

Incident Response: AI can assist in the automation of incident response processes, including isolating affected systems, notifying security teams, and providing initial recommendations for remediation.

Solution Architecture Diagram: