Project Design Phase-II
Technology Stack (Architecture & Stack)

Date	25 October 2023
Team ID	5.2
Project Name	AI-Enhanced Threat Intelligence Platform
Maximum Marks	4 Marks

Technical Architecture:

1. Data Ingestion:

Log Collection: Collect logs and data from various sources, such as firewalls, IDS/IPS, and network devices.

External Threat Feeds: Gather threat intelligence data from external sources.

2. **Data Processing:**

Data Normalization: Standardize incoming data to a common format for analysis.

Data Enrichment: Enhance data with additional information from threat feeds and other sources.

3. **Machine Learning and Analysis:**

Anomaly Detection: Utilize machine learning models for anomaly detection.

Behavioral Analysis: Analyze user and entity behavior for deviations.

Predictive Analysis: Predict potential threats based on historical data.

Threat Scoring: Assign threat scores to detected anomalies.

4. **Threat Intelligence Database:**

Store Threat Indicators: Maintain a database of known threats and indicators of compromise (IoCs).

Threat Feeds Integration: Continuously update threat intelligence from external sources.

5. **Alerting and Response:**

Alert Generation: Create alerts for detected threats based on predefined thresholds.

Incident Management: Manage and track security incidents.

Automated Response: Implement automated responses for known threats.

6. User Interface:

Dashboard: Provide a user-friendly dashboard for security analysts to monitor and respond to threats.

Visualization: Use visualizations to represent threat data and trends.

7. **Integration:**

Security Tools Integration: Integrate with other security tools like SIEM, IDS/IPS, and firewalls.

APIs: Provide APIs for external systems to interact with the platform.

8. **Scalability:**

Load Balancing: Implement load balancing for handling large volumes of data.

Scalable Infrastructure: Use scalable cloud or on-premises infrastructure.

9. **Security and Compliance:**

Data Encryption: Ensure data security with encryption.

Access Controls: Implement role-based access controls.

Regulatory Compliance: Adhere to data privacy regulations.

10. **Monitoring and Reporting:**

Logging and Auditing: Maintain logs for monitoring and auditing.

Reporting: Generate reports on threat detection and response.

11. **Continuous Learning:**

Feedback Loop: Establish a feedback loop for model improvement.

Model Training: Periodically retrain machine learning models.

12. **Ethical Considerations:**

Privacy Protection: Implement measures to protect user data.

Ethical AI: Ensure ethical AI practices in threat analysis.

This architectural outline provides a foundation for building an AI-powered Threat Intelligence Platform.

Working stages of the technology stack:

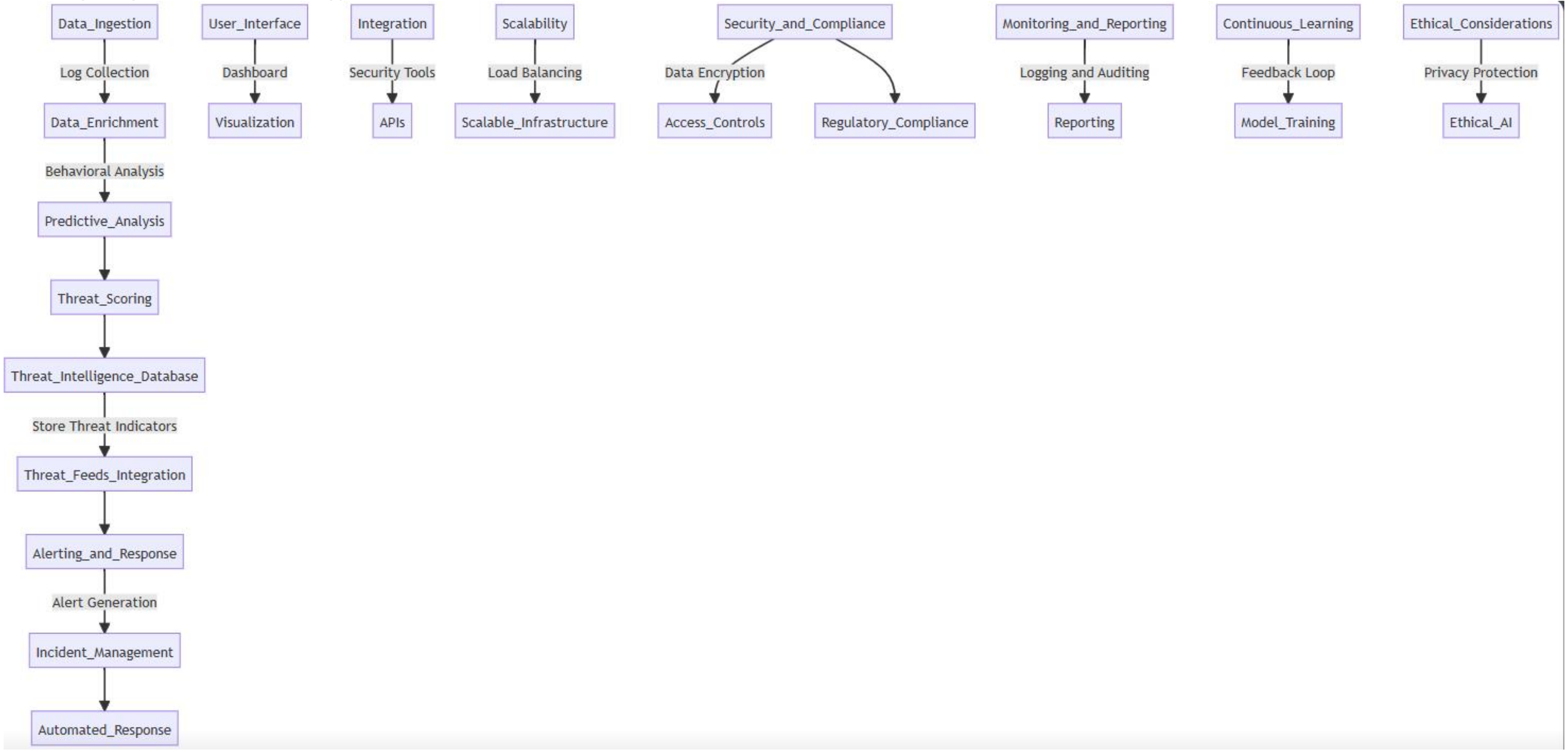

Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	Machine Learning Algorithms	Utilizes ML algorithms for anomaly detection and pattern recognition.	Python, TensorFlow, Scikit-Learn, XGBoost, PyTorch
2.	Behavioral Analysis	Analyzes user, device, and application behavior for identifying threats	Machine Learning Models, Anomaly Detection Algorithms
3.	Predictive Analysis	Predicts potential threats based on historical data and attack patterns.	Data Mining, Time Series Analysis
4.	Threat Detection	Automatically detects and responds to known threats and vulnerabilitie	AI-based Threat Detection Models, Signature-Based DetectionData Mining, Time Series Analysis
5.	Data Collection and Analysis	Aggregates and analyzes data from various sources, including logs and network traffic.	SIEM (Security Information and Event Management) Systems, Data Lakes
6.	Automation	Automates routine tasks, reducing the workload on security teams.	SOAR (Security Orchestration, Automation, and Response) Tools
7.	User and Entity Behavior Analytics	Creates baselines for normal behavior and detects deviations.	UEBA Solutions, Deep Learning Models
8.	Integration with Other Tools	Integrates with existing security tools for a comprehensive solution.	APIs, Webhooks, Integration Platforms
9.	Scalability	Scales to handle increasing data volumes and threats effectively.	Cloud Computing, Distributed Systems
10.	Challenges	Addresses challenges such as false positives and continuous learning	Natural Language Processing, Deep Learning for False Positive Reduction
11.	Regulatory Compliance	Helps organizations meet regulatory requirements for threat detection and response.	Compliance Tools, Data Encryption
12.	Ethical and Privacy Considerations	Considers ethical and privacy concerns, especially regarding user data.	Data Masking, Privacy-Preserving Techniques, Compliance Tools

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	Utilization of open-source frameworks for development, customization, and integration	Python, Django, Flask, Spring Boot, React.js, Angular, Node.js, Express.js, Elasticsearch, Kibana, etc.
2.	Security Implementations	Implementation of security measures and controls to safeguard the platform and data.	SSL/TLS, SHA-256, Encryption Algorithms, IAM (Identity and Access Management) Controls, Firewalls, OWASP (Open Web Application Security Project) guidelines, Security Information and Event Management (SIEM) Systems, Intrusion Detection Systems (IDS), etc.
3.	Scalable Architecture	Design and technology choices ensuring scalability to handle increasing data and users.	Microservices, Containers (Docker), Kubernetes, Load Balancers, Horizontal Scaling, Cloud Services (AWS, Azure, GCP), API Gateways, CDN (Content Delivery Network)

S.No	Characteristics	Description	Technology
4.	Availability	Measures taken to ensure the platform's availability, including redundancy and failover.	Load Balancers, Redundant Servers, Distributed Architecture, Disaster Recovery Plans, Failover Mechanisms, High Availability (HA) Clusters, Global Server Load Balancing (GSLB)
5.	Performance	Considerations for optimizing application performance, including caching and content delivery.	Caching Mechanisms, Content Delivery Networks (CDN), Load Testing Tools, In-Memory Databases (Redis), Application Performance Monitoring (APM) Tools, Horizontal Scaling