Project Design Phase-II
Data Flow Diagram & User Stories

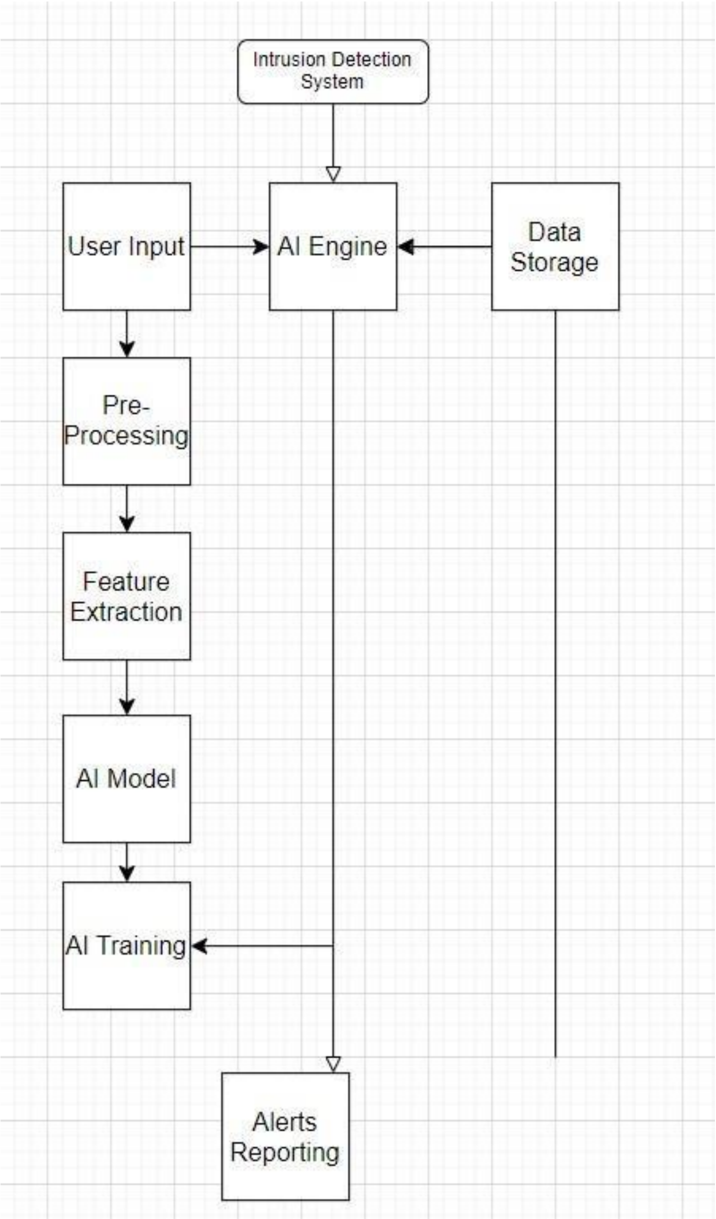
Date	25 October 2023
Team ID	9.2
Project Name	AI-powered threat hunting tool
Maximum Marks	4 Marks

Data Flow Diagrams:

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

Example: DFD Level 0 (Industry Standard)

Example: (Simplified)


Intrusion Detection System
User Input
AI Engine
Data Storage
Pre-Processing
Feature Extraction
AI Model
AI Training
Alerts Reporting

User Stories

Use the below template to list all the user stories for the product.

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Security Analyst	Threat Detection and Alerts	USN-1	Real-time Alerting	As a security analyst, I want to receive real-time alerts when the IDS detects a potential threat. The system should generate alerts for critical threats within one second of detection. Alerts should be delivered via email and a dashboard notification.	High	Sprint-1

Security Analyst	Threat Analysis and Reporting	USN-2	Alert Severity and Categorization	As a security analyst, I want to see the severity level and category of each alert. The system should assign a severity level (e.g., low, medium, high) to each alert based on the threat assessment. Alerts should be categorized (e.g., malware, DDoS, unauthorized access).	High	Sprint-1
Security Analyst		USN-3	Alert Investigation	As a security analyst, I want to investigate the details of an alert. Clicking on an alert should provide information about the source IP, destination IP, affected system, and a brief description of the threat.	Low	Sprint-3

Security Analyst	Automated Response and Mitigation	USN-4	Threat Intelligence Integration	As a security analyst, I want access to threat intelligence data related to detected threats. The system should display threat intelligence information for relevant alerts, including indicators of compromise (IoC) and known attack patterns.	Medium	Sprint-2
Security Analyst		USN-5	Automated Blocking	As a security analyst, I want to configure automated response actions for specific threat categories. The system should block traffic from known malicious IP addresses for alerts in the "high" severity category.	High	Sprint-1
Security Analyst	Reporting and Compliance	USN-6	Incident Escalation	As a security analyst, I want to escalate incidents to other team members when necessary.	Low	Sprint-4
				The system should provide a one-click option to escalate an incident to the incident response team with relevant details.		

Security Analyst		USN-7	Compliance Reporting	As a security analyst, I want the system to generate compliance reports. The system should generate daily, weekly, and monthly reports summarizing alerts, incident response times, and compliance with regulatory requirements	Low	Sprint-5
Security Analyst		USN-8	Dashboard and Visualization	As a security analyst, I want a dashboard with visualizations. The system should provide interactive charts and graphs to visualize the current threat landscape and historical data.	Low	Sprint-6