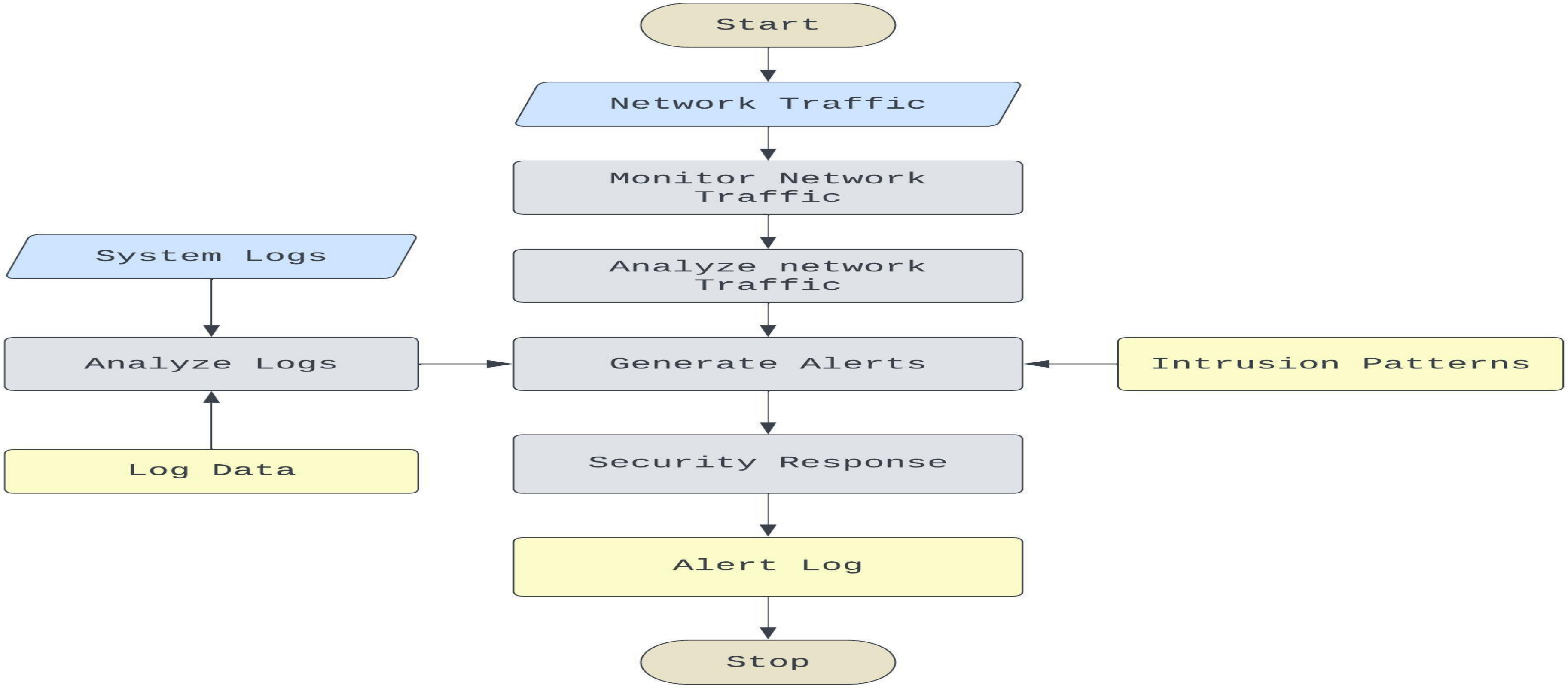
Team -1.4
TeamMembers-Asim Shikhar, R Gowtham, Love Yadav

Data Flow Diagram & User Stories

Date	31 October 2023
Team ID	Team-591527
Project Name	AI-Enhanced Intrusion Detection System (IDS)
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.



User Stories

User Story Number	User Story / Task	Acceptance Criteria	Priority	Release
USN-1	As a security administrator, I want to be able to train the AI-Enhanced IDS on my organization's network traffic data so that it can learn to detect anomalous and malicious activity.	The AI-Enhanced IDS must be able to be trained on a variety of network traffic data formats, including packet captures, NetFlow records, and security logs. The training process must be able to be completed within a reasonable amount of time, and the AI-Enhanced IDS must be able to learn to detect anomalous and malicious activity with a high degree of accuracy.	High	Sprint-1
USN-2	As a security administrator, I want to be able to deploy the AI-Enhanced IDS on my organization's network so that it can monitor traffic for anomalous and malicious activity in real time.	The AI-Enhanced IDS must be able to be deployed on a variety of network architectures, including cloud-based networks, on-premises networks, and hybrid networks. The deployment process must be straightforward and easy to follow. Once deployed, the AI-Enhanced IDS must be able to monitor network traffic for anomalous and malicious activity in real time and generate alerts when it detects suspicious activity.	High	Sprint-2

USN-3	As a security administrator, I want to be able to view alerts generated by the AI-Enhanced IDS so that I can investigate potential threats and take appropriate action.	The AI-Enhanced IDS must generate alerts that are clear, concise, and informative. The alerts must include information such as the time and date of the event, the source and destination IP addresses, the type of suspicious activity detected, and the severity of the threat. The AI-Enhanced IDS must also provide a way for security administrators to view and manage alerts.	Medium	Sprint-3
USN-4	As a security administrator, I want to be able to tune the AI-Enhanced IDS to reduce the number of false positives.	The AI-Enhanced IDS must provide a way for security administrators to tune its detection thresholds and other parameters to reduce the number of false positives. The AI-Enhanced IDS must also provide a way for security administrators to generate and test new detection rules.	Medium	Sprint-4
USN-5	As a security administrator, I want to be able to integrate the AI-Enhanced IDS with my organization's existing security infrastructure.	The AI-Enhanced IDS must provide a way for security administrators to integrate it with their organization's existing security infrastructure, such as security information and event management (SIEM) systems and security orchestration, automation, and response (SOAR) platforms. This integration should allow the AI-Enhanced IDS to share data with other security systems and to automate incident response tasks.	Low	Sprint-5