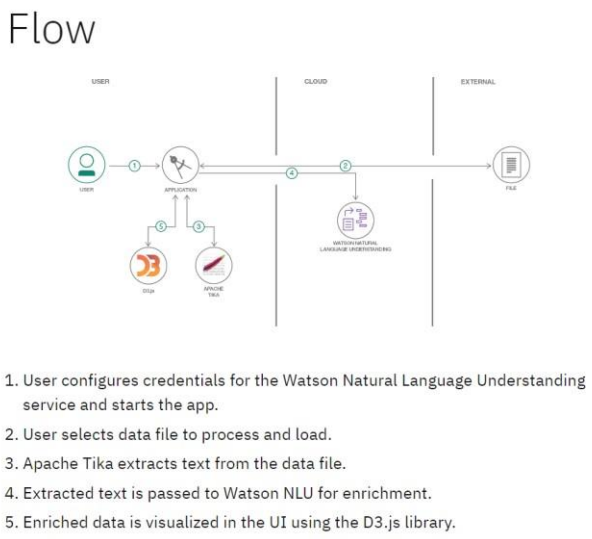
Project Design Phase-II
Data Flow Diagram & User Stories

Date	03 October 2022
Team ID	PNT2022TMIDxxxxxx
Project Name	Project - 6
Maximum Marks	4 Marks

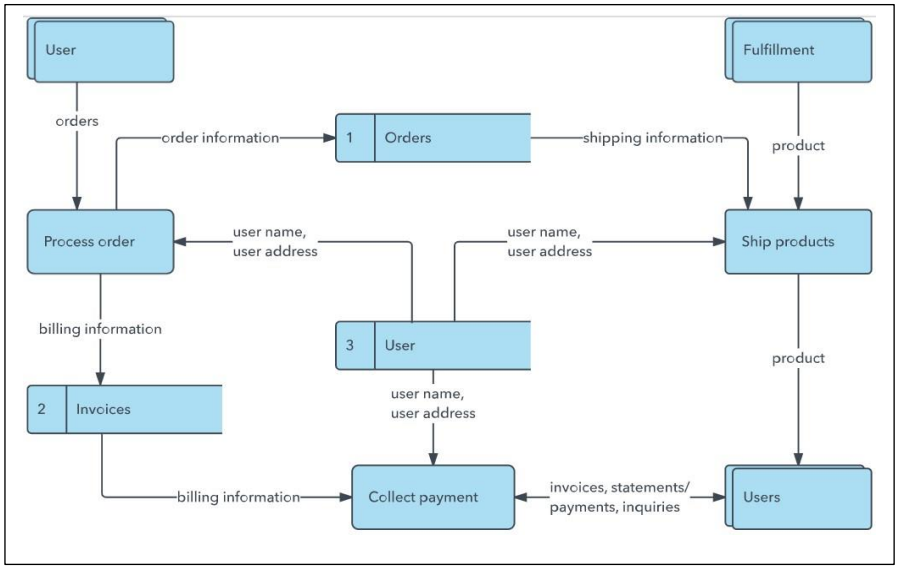
Data Flow Diagrams:

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.

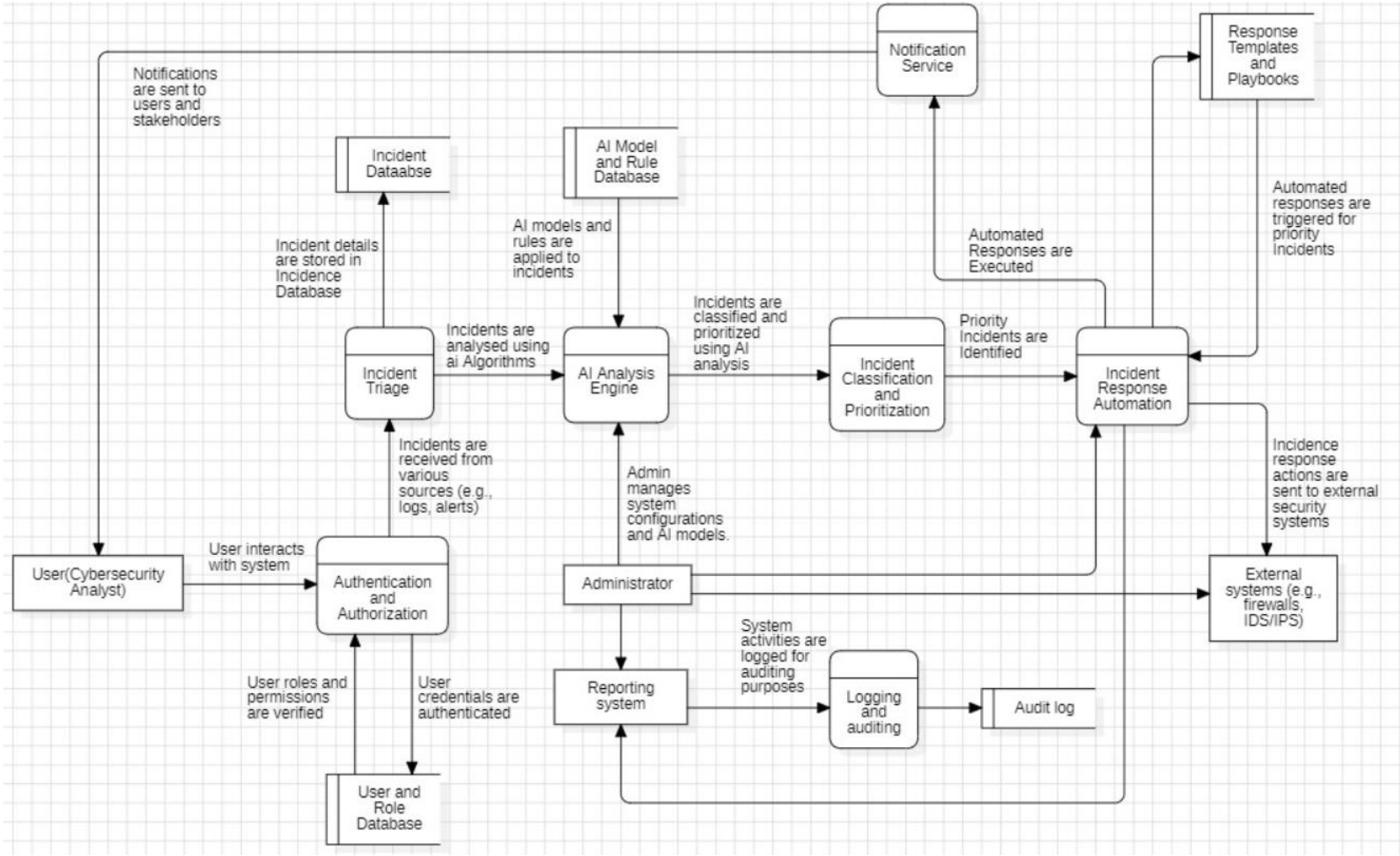
Example: (Simplified)



Example: DFD Level 0 (Industry Standard)



DFD:


Notification Service
Response Templates and Playbooks
Notifications are sent to users and stakeholders
Incident Dataabse
AI Model and Rule Database
Automated responses are triggered for priority Incidents
AI models and rules are applied to incidents
Incident details are stored in Incidence Database
Automated Responses are Executed
Incidents are classified and prioritized using AI analysis
Priority Incidents are Identified
Incident Triage
Incidents are analysed using ai Algorithms
AI Analysis Engine
Incident Classification and Prioritization
Incident Response Automation
Incidence response actions are sent to external security systems
Incidents are received from various sources (e.g., logs, alerts)
Admin manages system configurations and AI models.
User interacts with system
User(Cybersecurity Analyst)
Authentication and Authorization
Administrator
External systems (e.g., firewalls, IDS/IPS)
System activities are logged for auditing purposes
User roles and permissions are verified
User credentials are authenticated
Reporting system
Logging and auditing
Audit log
User and Role Database

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
Cybersecurity Analyst	Incident Triage and Response	US001	As a cybersecurity analyst, I want to log in securely to access the system	User can enter valid credentials. Authentication is successful. User roles and permissions are verified.	HIGH	Sprint-1
Cybersecurity Analyst	Incident Triage and Response	US002	As a cybersecurity analyst, I want to receive incidents from various sources, including logs and alerts.	Incidents are received from external sources. Incidents are stored in the incident database.	HIGH	Sprint-1
Cybersecurity Analyst	AI Analysis	US003	As a cybersecurity analyst, I want to leverage AI analysis to understand incident details.	Incidents are analysed using AI algorithms. AI models and rules are applied to incidents.	HIGH	Sprint-2
Cybersecurity Analyst	Incident classification and prioritization.	US004	As a cybersecurity analyst, I want to classify and prioritize incidents based on AI analysis.	Incidents are classified and prioritized based on AI analysis.	HIGH	Sprint-2
Cybersecurity Analyst	Incident response Automation.	US005	As a cybersecurity analyst, I want to trigger automated responses for priority incidents.	Automated response actions are executed for priority incidents. Responses are based on predefined templates and playbooks.	HIGH	Sprint-3
Cybersecurity Analyst	Notification service	US006	As a cybersecurity analyst, I want to receive notifications about incident status and actions taken.	Notifications are sent to users and stakeholders.	HIGH	Sprint-3
Cybersecurity Analyst	Logging and Auditing	US007	As a cybersecurity analyst, I want system activities to be logged for auditing purposes.	System activities are logged in the Audit log.	HIGH	Sprint-4

Administrator	System management	US008	As and administrator, I want to manage system configurations and AI models.	The admin interface allows configuration management.	HIGH	Sprint-4
External system	External System integration	US009	As and external system, I want to receive incident response actions from the platform.	The platform can send incident response actions to external systems.	HIGH	Sprint-5
Reporting user	Reporting	US010	As a reporting user, I want to generate and receive detailed incident reports	Incident reports are generated and transmitted to the reporting system.	LOW	Sprint-5