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

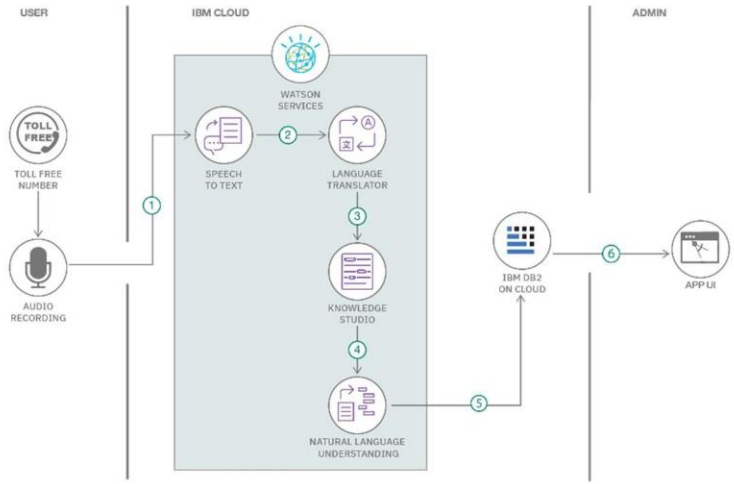
Date	25 October 2023
Team ID	9.2
Project Name	AI-powered threat hunting tool
Maximum Marks	4 Marks

Technical Architecture:

The Deliverable shall include the architectural diagram as below and the information as per the table1 & table 2

Example: Order processing during pandemics for offline mode

Reference: https://developer.ibm.com/patterns/ai-powered-backend-system-for-order-processing-during-pandemics/



Guidelines:

1. Include all the processes (As an applica on logic / Technology Block)
2. Provide infrastructural demarca on (Local / Cloud)
3. Indicate external interfaces (third party API's etc.)
4. Indicate Data Storage components / services
5. Indicate interface to machine learning models (if applicable)

Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	Data Sources	Data sources can include network traffic data, system logs, and security event data from various devices .	Network taps, sensors, log collectors, firewall logs, IDS/IPS devices, packet capture tools.
2.	Data Processing	This component is responsible for inges ng, preprocessing, and normalizing the data to make it suitable for analysis.	Apache Ka a, Logstash, Fluentd, data normaliza on scripts.
3.	Data Storage	A central repository for storing pre-processed data, enabling historical analysis and real- me access.	Elas csearch, Hadoop HDFS, AWS S3, SQL/NoSQL databases.
4.	Machine Learning Model	Machine learning models are used to iden fy anomalies and poten al intrusions by learning from historical data.	Python (Scikit-Learn, TensorFlow, PyTorch), Jupyter Notebooks, GPU for deep learning.
5.	Intrusion Detec on Rules Engine	This component includes predefined rules and signatures for known a ack pa erns, aiding in signaturebased detec on.	Snort, Suricata, YARA rules, custom signatures.
6.	Real-Time Analysis	This is where machine learning models and intrusion detec on rules are applied to the data for real- me analysis.	Real- me stream processing frameworks (e.g., Apache Flink, Apache Ka a Streams), Python for rule execu on.
7.	Alert Management	Alerts generated by the real- me analysis component are managed here, priori zed, and routed for further inves ga on.	SIEM systems, alert correla on tools, cke ng systems.
8.	User Interface (UI)	Provides a dashboard for security administrators and analysts to monitor the system's performance and respond to incidents.	Web-based UI (HTML, CSS, JavaScript), dashboard frameworks (e.g., Kibana, Grafana).

9.	Repor ng and Analy cs	Generates reports and provides analy cs on detected incidents, trends, and system performance.	Repor ng tools (e.g., Tableau, Power BI), data analy cs pla orms (e.g., Apache Spark), custom analy cs scripts.
10.	No fica on and Response	This component can automa cally trigger predefined responses when intrusions are detected, such as isola ng affected systems or blocking malicious traffic.	Automa on scripts, APIs for response ac ons, orchestra on tools (e.g., Ansible).
11.	Integra on APIs	APIs are used to integrate the intrusion detection system with other security tools and incident response platforms.	RESTful APIs, webhook integra ons, thirdparty security APIs.
12.	Scalability and Load Balancing	Ensures the system can handle high volumes of data and provides fault tolerance.	Load balancers, container orchestration (e.g., Kubernetes), cloud auto-scaling.
13.	Security and Compliance	Various security measures and compliance considerations should be integrated throughout the architecture to ensure data and system security.	Encryption (TLS/SSL), access control, auditing and monitoring tools, compliance frameworks (e.g., PCI DSS, HIPAA).

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Anomaly Detec on	AI-enhanced IDS can detect anomalies in network traffic and system behaviour by learning what is considered normal. When it iden fies devia ons from this baseline, it can trigger alerts or automa c responses	Machine learning algorithms, such as neural networks, clustering, and sta s cal analysis.
2.	Signature-Based Detec on	The system is equipped with predefined signatures or pa erns of known threats. When network traffic matches these signatures, it raises alarms or takes predefined ac ons.	Pa ern recogni on, rule-based systems.

3.	Real- me Monitoring	AI-enhanced IDS systems con nuously monitor network traffic in real- me, providing immediate threat detec on and response capabili es.	Con nuous packet analysis and traffic monitoring.
4.	Behaviour Analysis	It analyses user and system behaviour to iden fy suspicious ac vi es or devia ons from normal behaviour pa erns.	Machine learning, data analysis.
5.	Regular Updates and Training	The IDS con nuously updates its knowledge base and machine learning models to adapt to evolving threats.	Data collec on and model retraining.
6.	User-Friendly Interface	A user-friendly interface allows security analysts to interact with and configure the IDS efficiently, helping them make informed decisions.	User experience (UX) design principles.
7.	Threat Intelligence Integration	The IDS can stay updated with the latest threat intelligence, incorporating new threat signatures and indicators of compromise into its detection capabilities.	API integra ons with threat feeds and databases.
8.	Scalability	The system can be scaled horizontally and vertically to accommodate the needs of various network sizes and configurations	Distributed architecture, cloud-based solu ons.