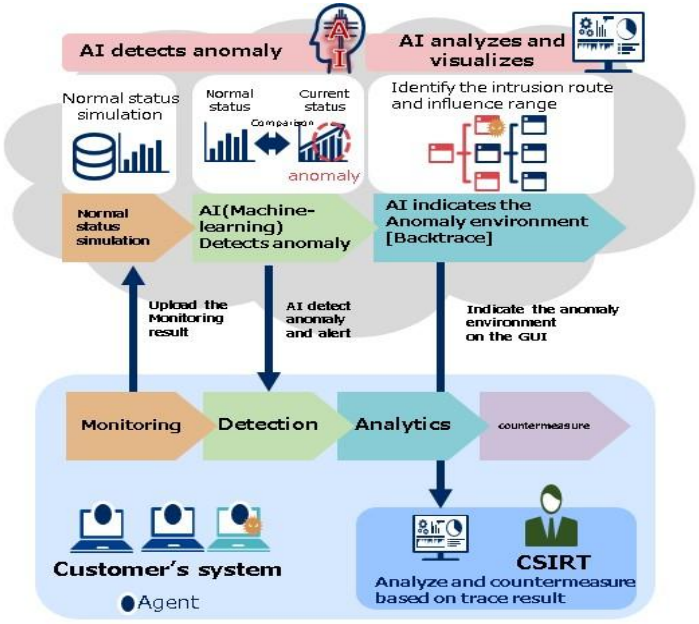
Project Design Phase-II
Technology Stack (Architecture & Stack)

Date	03 October 2022
Team ID	10.4
Project Name	Project - AI-enhanced security analytics dashboard
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: Vulnerability scanning and analyzing it through dashboard along with the remedies.



Guidelines:

1. Include all the processes (As an application logic / Technology Block)
2. Provide infrastructural demarcation (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	Log Collection	Efficient log collection	Fluentd (open source)
	Log Forwarding	Lightweight log forwarding	Filebeat (open source) or Custom Scripts
	Data Storage	Scalable storage and indexing	Elasticsearch (open source and free)
2	Data Processing and Analysis : Big Data Processing	Big data processing	Apache Spark (open source)
	Real-time Data Streaming	Real-time data streaming	Apache Kafka (open source)
3	Data Visualization	Data visualization and analytics	Kibana (open source and designed for Elasticsearch)

4	Security and Authentication : User Authentication	User authentication	Open-source solutions like Keycloak or Auth0
	Data Encryption	Data encryption	SSL/TLS (built-in and low cost)
	Access Control	Role-based access control	Implement custom role-based access control
5	Infrastructure and Deployment : Containerization	Containerization	Docker (open source and cost-effective)
	Orchestration	Orchestration	Kubernetes (open source)
	Hosting	Hosting options	Affordable cloud services (AWS Free Tier, Google Cloud "Always Free" tier) or on-premises servers
6	Primary Language	Primary programming language	Python (open source)

	ML Libraries	Machine learning libraries	Scikit-learn (open source)
7	Alerting Services	Integration with alerting services	Free services like Slack or email
8	Reporting Tools	Custom reporting tools and dashboards	Open-source tools like Grafana or Metabase
9	User Interface	User interface development	HTML, CSS, and JavaScript (keep it simple)
10	Version Control	Version control	Git (open source)
	Collaboration Tools	Collaboration and project management tools	Free or low-cost tools like GitHub or GitLab
11	Documentation Platform	Documentation and knowledge sharing	Open-source platforms like DokuWiki

12	Automated Testing Tools	Testing tools and frameworks	Open-source tools like Selenium, JUnit, or pytest
13	System Monitoring	System monitoring	Open-source tools like Prometheus and Grafana
	Centralized Logging	Centralized logging and error tracking	ELK Stack (Elasticsearch, Logstash, Kibana)
14	Data Backup and Recovery	Basic data backup and recovery solutions	Implemented on chosen infrastructure

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1	Open-Source Frameworks	Open-source frameworks used	Utilizes open-source frameworks where applicable

2	Security Implementations	Security and access controls	Basic security measures: SSL/TLS, IAM controls
3	Scalable Architecture	Scalability of architecture	Microservices architecture
4	Availability	Availability of application	Load balancers, distributed servers (budget-friendly options)
5	Performance	Design for performance	High request rate considerations, basic caching

References:

https://images.google.com/