Project Design Phase-I
Proposed Solution Template

Date	27 October 2023
Team ID	10.2
Project Name	AI-enhanced security analytics dashboard that provides real-time insights into security events, trends, and risks
Maximum Marks	2 Marks

Proposed Solution:

S. No	**Parameter**	**Description**
1.	Problem Statement (Problem to be solved)	In the current digital landscape, the absence of a centralized, real-time security analytics dashboard that incorporates AI-driven insights impedes organizations ability to swiftly detect, analyze and respond to emerging security threats. This gap leads to delayed threat identification, inefficient resource allocation, and increased vulnerability to potential breaches. Therefore, there is a pressing need for an AI-enhanced security analytics dashboard that can consolidate diverse security data sources, deliver real-time insights, and empower proactive security measures. This project aims to develop a user-friendly and scalable solution that integrates cutting-edge AI algorithms for predictive analysis, anomaly detection, and trend forecasting ,facilitating robust security management and safeguarding critical data assets
2.	Idea / Solution description	The proposed solution is a scalable security analytics dashboard that leverages leading-edge AI techniques such as: • **Statistical analysis and machine learning** for baseline modeling and anomaly detection from network, endpoint, and user activity data • **Natural language processing** to parse through unstructured threat intelligence and log data • **Scene graph analytics** to identify relationships between threats, users, and infrastructure • **Graph neural networks** to detect suspicious behavioral patterns and trends

		The dashboard will provide security analysts with real-time visibility through customizable alerting, dynamic visualizations, and role-based access controls. Users can prioritize and investigate security events, perform root cause analysis, and initiate automated response workflows. Built-in reporting capabilities will facilitate risk monitoring and communication across stakeholders. The solution will ingest data from existing security tools via API integrations and normalize/enrich data for AI analytics. The platform will be scalable to accommodate large enterprises and offer robust data protection compliant with industry standards. An intuitive, responsive UI will provide users a simple yet powerful security analytics experience.
3.	Novelty / Uniqueness	• It takes an AI-first approach to security analytics, unlike most solutions that apply AI as an afterthought. Advanced AI algorithms are deeply integrated for automated threat detection, analysis, and response. • The dashboard uniquely combines statistical, NLP, graph-based, and computer vision AI to extract insights from diverse data types in a holistic manner. This overcomes the limitations of point analytics tools. • A key innovation is the use of scene graph analytics to model relationships between security entities. This enables complex threat hunting and risk monitoring across the attack surface.
4.	Social Impact / Customer Satisfaction	• Improved cybersecurity and reduced data breaches through proactive threat detection can build public trust and reputation for organizations using the dashboard. • Faster incident response enabled by the dashboard translates to minimizing customer data and privacy violations in the event of attacks. • By detecting insider threats and cyber risks, the dashboard helps companies avoid IP theft and maintains shareholder value. • Scalable architecture and cloud deployment ensure affordable access to

		advanced analytics, especially for smaller businesses or non-profits.
5.	Business Model (Revenue Model)	The dashboard will be offered as a Software-as-a-Service (SaaS) model to provide easy access without extensive setup and maintenance overhead for customers. **Target Customers** The platform is designed for organizations of all sizes across industries looking to augment their security operations through AI automation and actionable insights from data. **Revenue Streams** • Subscription plans for dashboard access based on number of users, data sources, and platform features • Professional services for onboarding, training, and ongoing enhancement • Ongoing customer support and maintenance contracts **Key Metrics** • Number of customers across tiers and segments • Data sources and events processed per customer • Renewal and retention rates • Customer lifetime value • Customer acquisition cost • Cost per incident detected/prevented
6.	Scalability of the Solution	Here is a concise overview of how the proposed security analytics dashboard solution scales: • Distributed microservices architecture spreads workload across servers as data volumes grow. Just add more servers. • Cloud deployment provides unlimited computing power for storage, processing, and analysis as needed. • Modular components can be independently scaled - ex: scale AI modelling servers separately from app servers. • Stateless design prevents bottlenecks. No single point of failure.