Project Design Phase-I

Date	23 October 2023
Team ID	PNT2023TMIDxxxxxx
Project Name	AI-Based Threat Intelligence Platform
Maximum Marks	2 Marks

Proposed Solution Template:

Project team shall fill the following information in proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	How might we enrich data sources, streamline data preprocessing, implement effective behavioral analysis methods, enable real-time monitoring and analysis, and conduct regular red team testing to improve threat intelligence and enhance platform security and resilience?
		• Expand data sources and implement advanced data preprocessing techniques to improve data quality and reduce false positives. • Incorporate behavioral analysis to detect advanced threats like insider

2.	Idea / Solution description	threats and zero-day attacks. ● Enable real-time monitoring and analysis of threat data to allow for immediate response to emerging threats. ● Promote information sharing and collaboration among organizations to enhance collective threat intelligence. ● Integrate the Threat Intelligence Platform with SIEM systems and implement machine learning models to provide a holistic view of security events and enable faster threat response. ● Invest in user education and training, continuously update threat intelligence feeds, and establish a feedback loop with users to refine detection rules and models. ● Develop algorithms for prioritizing threats and integrate incident response automation to reduce response time and ensure efficient threat mitigation. ● Ensure that the platform complies with relevant cybersecurity regulations and standards.

3.	Novelty / Uniqueness	The novelty and uniqueness of the proposed problem statement and solution for improving threat intelligence platforms lies in its holistic and integrated approach. By addressing all of the key areas of threat intelligence in a comprehensive and coordinated manner, the proposed solution can help organizations to achieve a significant step forward in their threat detection and prevention capabilities. ● Support for information sharing and collaboration: Threat intelligence sharing is essential for organizations to stay ahead of the threat curve. The proposed solution promotes information sharing and collaboration by providing a platform for organizations to share threat intelligence and learn from each other's experiences. ● Integration with SIEM systems: Integrating the Threat Intelligence Platform with SIEM systems can provide organizations with a holistic view of their security posture and enable faster threat response. The proposed solution is designed to be easily integrated with SIEM systems. ● Use of machine learning for

		continuous learning: Machine learning can be used to continuously improve the accuracy and effectiveness of threat intelligence platforms. The proposed solution implements machine learning models to learn from new threat data and evolving attack patterns. ● Alignment with cybersecurity regulations and standards: Ensuring that the Threat Intelligence Platform complies with relevant cybersecurity regulations and standards is essential for maintaining a secure and compliant security posture. The proposed solution is designed to meet the requirements of key cybersecurity regulations and standards.
4.	Social Impact / Customer	Improved threat intelligence platforms can have a significant social impact by helping organizations to protect their critical infrastructure, intellectual property, and customer data from cyberattacks. This can help to reduce financial losses, prevent disruptions to essential services, and

	Satisfaction	safeguard the privacy of individuals. Additionally, improved threat intelligence can help to raise awareness of cybersecurity threats and enable organizations to take steps to mitigate these risks.
5.	Business Model (Revenue Model)	Subscription-based revenue model for threat intelligence platform: Subscription: Customers pay a monthly or annual fee to access the threat intelligence platform and its features. This model is well-suited for businesses of all sizes, as it provides them with a predictable source of revenue.
		The scalability of the proposed solution for improving threat intelligence platforms is dependent on the specific technologies and architectures that are used. However, in general, the proposed solution is designed to be scalable to meet the needs of organizations of all sizes.

6.	Scalability of the Solution	Here are some specific ways in which the proposed solution can be scaled: ● Data ingestion and processing: The proposed solution can be scaled to ingest and process large volumes of data from a variety of sources by using distributed computing and storage technologies. ● Real-time monitoring and analysis: The proposed solution can be scaled to perform real-time monitoring and analysis of threat data by using advanced machine learning techniques and distributed computing architectures. ● Information sharing and collaboration: The proposed solution can be scaled to facilitate information sharing and collaboration among organizations by using a cloud-based platform and standard communication protocols. ● Integration with SIEM systems: The proposed solution can be scaled to integrate with SIEM systems of all sizes by using standard APIs and data formats. ● Compliance and regulation

		adherence: The proposed solution can be scaled to meet the compliance and regulation requirements of organizations of all sizes by implementing a robust security and compliance framework.