AI-Based Threat Intelligence Platform

Introduction

Building an AI-Based Threat Intelligence Platform: In an era marked by an ever-expanding digital landscape and increasingly sophisticated cyber threats, the need for robust and intelligent cybersecurity solutions has never been more pressing. The "AI-Based Threat Intelligence Platform" project is a pioneering endeavour that seeks to fortify organizations' defenses against a multitude of cyber adversaries. By harnessing the power of artificial intelligence, this platform aims to provide real-time threat detection, rapid incident response, and proactive defense mechanisms to safeguard critical assets and data.

Challenges: Cyber threats have become more diverse and elusive, with attackers employing advanced techniques to infiltrate systems, steal sensitive data, disrupt operations, and exploit vulnerabilities. Traditional security measures are often insufficient in the face of these evolving threats, necessitating a proactive, adaptive, and intelligence-driven approach.

Vision: This project envisions an AI-based Threat Intelligence Platform that not only identifies known threats but also uncovers emerging and zero-day threats before they can inflict harm. By collecting, normalizing, and analyzing vast quantities of data from various sources, the platform will provide an all-encompassing view of an organization's threat landscape. Using advanced machine learning algorithms, it will separate benign anomalies from malicious activities and enable rapid incident response, ultimately empowering organizations to stay one step ahead of cyber adversaries.

Significance: The AI-Based Threat Intelligence Platform stands to redefine the landscape of cybersecurity by offering a proactive defense strategy, enhanced visibility, and the ability to swiftly respond to threats, reducing the risk of data breaches, financial losses, and reputational damage for organizations of all sizes and sectors.

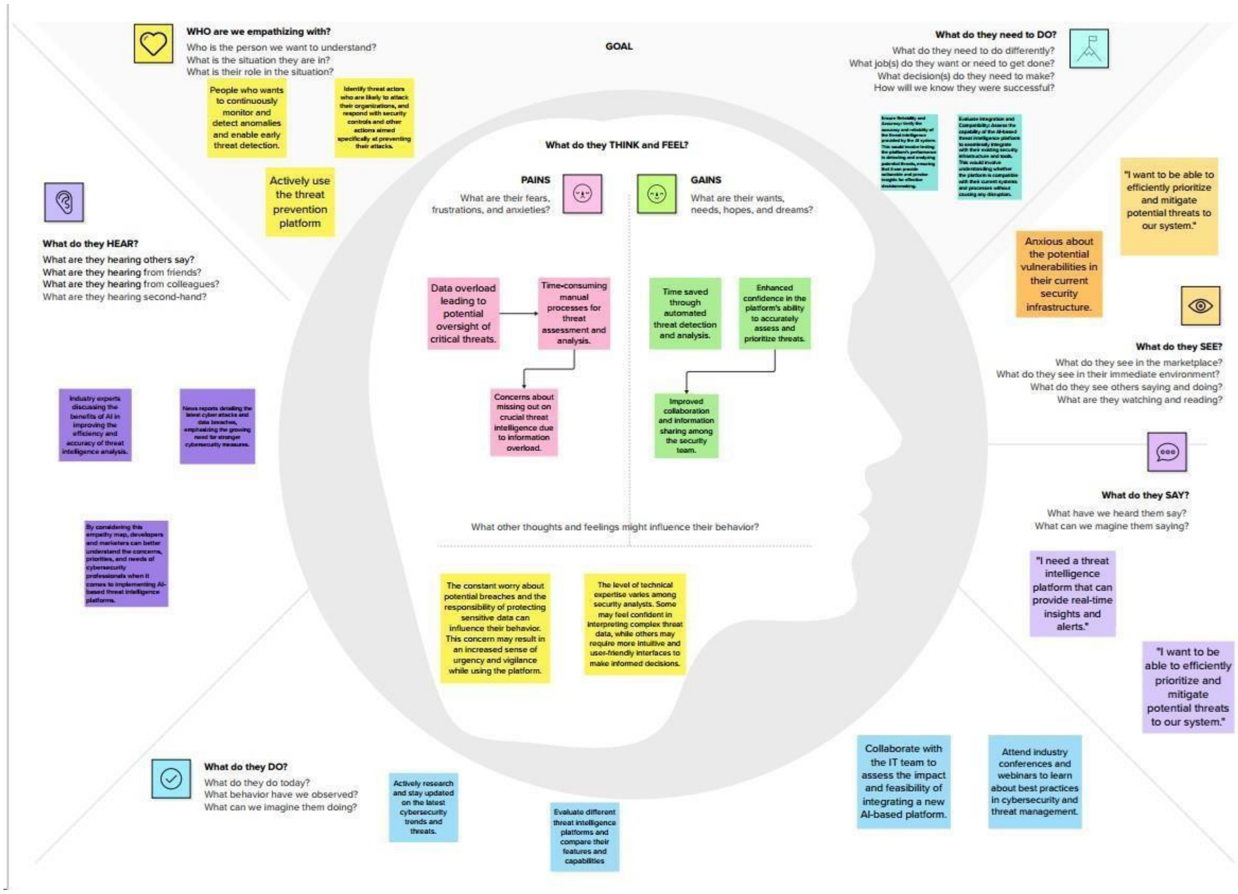
Objectives:

- Real-Time Threat Detection: Implement AI models capable of continuously monitoring and analyzing network traffic, logs, and security events to detect threats in real time.
- Threat Feed Integration: Integrate a comprehensive range of threat intelligence feeds from trusted sources, enriching internal data with the latest threat indicators.
- Automated Alerting: Develop an alerting system that provides timely notifications to security analysts when a potential threat is detected.
- Incident Response Integration: Seamlessly connect with existing incident response processes and tools to expedite mitigation.
- User-Friendly Interface: Create an intuitive user interface with interactive dashboards and reports to enable security analysts to make informed decisions.

Abstract

The AI-Based Threat Intelligence Platform employs artificial intelligence for real-time threat detection, anomaly identification, and rapid incident response. It integrates diverse data sources, providing a proactive defence strategy. This initiative aims to strengthen cybersecurity across industries, reducing the risk of data breaches and financial losses.

Empathy Map


WHO are we empathizing with?
Who is the person we want to understand?
What is the situation they are in?
What is their role in the situation?
GOAL
What do they need to DO?
What do they need to do differently?
What job(s) do they want or need to get done?
What decision(s) do they need to make?
How will we know they were successful?
What do they THINK and FEEL?
PAINS
What are their fears, frustrations, and anxieties?
GAINS
What are their wants, needs, hopes, and dreams?
What other thoughts and feelings might influence their behavior?
What do they HEAR?
What are they hearing others say?
What are they hearing from friends?
What are they hearing from colleagues?
What are they hearing second-hand?
What do they SEE?
What do they see in the marketplace?
What do they see in their immediate environment?
What do they see others saying and doing?
What are they watching and reading?
What do they SAY?
What have we heard them say?
What can we magine them saying?
What do they DO?
What do they do today?
What behavior have we observed?
What can we imagine them doing?

People who wants to continuously monitor and detect anomalies and enable early threat detection.

Identify threat actors who are likely to attack their organizations, and respond with security controls and other actions aimed specifically at preventing their attacks.

Actively use the threat prevention platform

Ensure Reliability and Accuracy: Verify the accuracy and reliability of the threat intelligence provided by the AI system. This would involve testing the platform's performance in detecting and analyzing potential threats, ensuring that it can provide actionable and precise insights for effective decisionmaking.

Evaluate Integration and Compatibility: Assess the capability of the AI-based threat intelligence platform to seamlessly integrate with their existing security infrastructure and tools. This would involve understanding whether the platform is compatible with their current systems and processes without causing any disruption.

"I want to be able to efficiently prioritize and mitigate potential threats to our system."

Anxious about the potential vulnerabilities in their current security infrastructure.

Data overload leading to potential oversight of critical threats.

Time-consuming manual processes for threat assessment and analysis.

Concerns about missing out on crucial threat intelligence due to information overload.

Time saved through automated threat detection and analysis.

Enhanced confidence in the platform's ability to accurately assess and prioritize threats.

Improved collaboration and information sharing among the security team.

The constant worry about potential breaches and the responsibility of protecting sensitive data can influence their behavior. This concern may result in an increased sense of urgency and vigilance while using the platform.

The level of technical expertise varies among security analysts. Some may feel confident in interpreting complex threat data, while others may require more intuitive and user-friendly interfaces to make informed decisions.

Industry experts discussing the benefits of AI in improving the efficiency and accuracy of threat intelligence analysis.

News reports detailing the latest cyber attacks and data breaches, emphasizing the growing need for stronger cybersecurity measures.

By considering this empathy map, developers and marketers can better understand the concerns, priorities, and needs of cybersecurity professionals when it comes to implementing AI-based threat intelligence platforms.

"I need a threat intelligence platform that can provide real-time insights and alerts."

"I want to be able to efficiently prioritize and mitigate potential threats to our system."

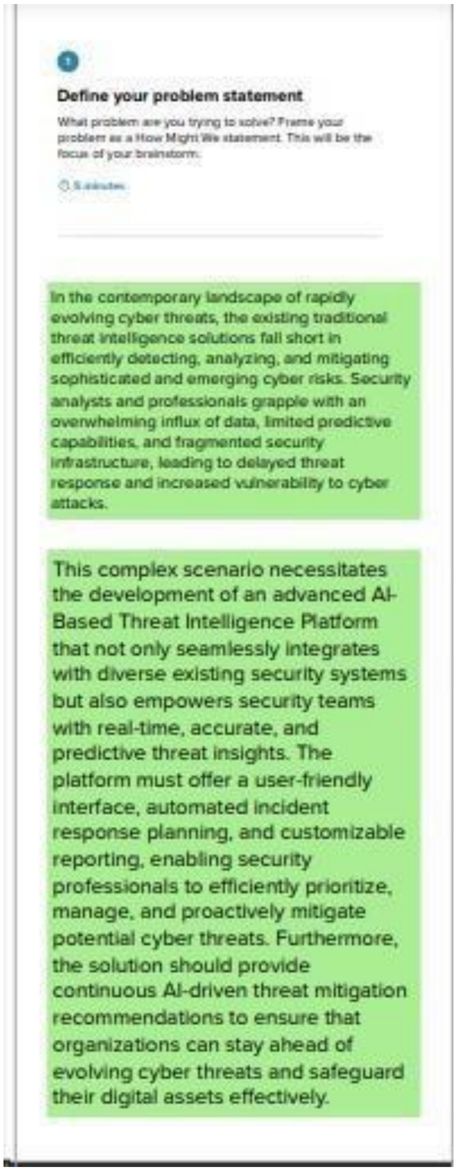
Actively research and stay updated on the latest cybersecurity trends and threats.

Evaluate different threat intelligence platforms and compare their features and capabilities

Collaborate with the IT team to assess the impact and feasibility of integrating a new AI-based platform.

Attend industry conferences and webinars to learn about best practices in cybersecurity and threat management.

Brainstorming Map

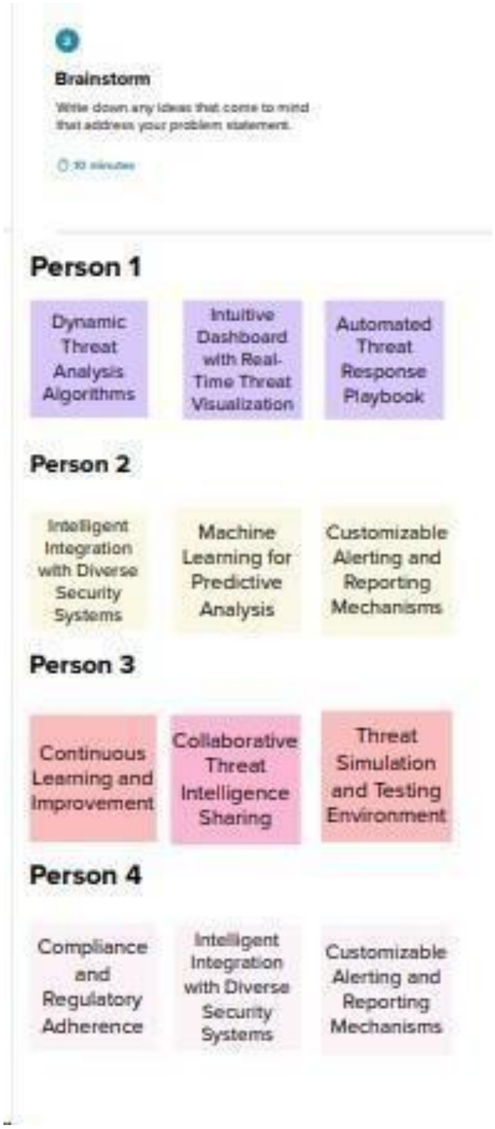


Define your problem statement

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

In the contemporary landscape of rapidly evolving cyber threats, the existing traditional threat intelligence solutions fall short in efficiently detecting, analyzing, and mitigating sophisticated and emerging cyber risks. Security analysts and professionals grapple with an overwhelming influx of data, limited predictive capabilities, and fragmented security infrastructure, leading to delayed threat response and increased vulnerability to cyber attacks.

This complex scenario necessitates the development of an advanced AI-Based Threat Intelligence Platform that not only seamlessly integrates with diverse existing security systems but also empowers security teams with real-time, accurate, and predictive threat insights. The platform must offer a user-friendly interface, automated incident response planning, and customizable reporting, enabling security professionals to efficiently prioritize, manage, and proactively mitigate potential cyber threats. Furthermore, the solution should provide continuous AI-driven threat mitigation recommendations to ensure that organizations can stay ahead of evolving cyber threats and safeguard their digital assets effectively.



Brainstorm

Write down any ideas that come to mind that address your problem statement.

Person 1

Dynamic Threat Analysis Algorithms

Intuitive Dashboard with Real-Time Threat Visualization

Automated Threat Response Playbook

Person 2

Intelligent Integration with Diverse Security Systems

Machine Learning for Predictive Analysis

Customizable Alerting and Reporting Mechanisms

Person 3

Continuous Learning and Improvement

Collaborative Threat Intelligence Sharing

Threat Simulation and Testing Environment

Person 4

Compliance and Regulatory Adherence

Intelligent Integration with Diverse Security Systems

Customizable Alerting and Reporting Mechanisms

3

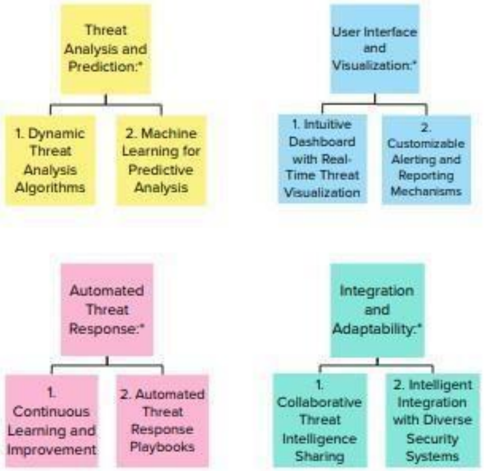
Group ideas

Take turns sharing your ideas while clustering similar or related notes as you go. Once all sticky notes have been grouped, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you and break it up into smaller sub-groups.

20 minutes

TIP

Add customizable tags to sticky notes to make it easier to find, browse, organize, and categorize important ideas as themes within your mural.



Threat Analysis and Prediction:*

1. Dynamic Threat Analysis Algorithms

2. Machine Learning for Predictive Analysis

User Interface and Visualization:*

1. Intuitive Dashboard with Real-Time Threat Visualization

2. Customizable Alerting and Reporting Mechanisms

Automated Threat Response:*

1. Continuous Learning and Improvement

2. Automated Threat Response Playbooks

Integration and Adaptability:*

1. Collaborative Threat Intelligence Sharing

2. Intelligent Integration with Diverse Security Systems

4

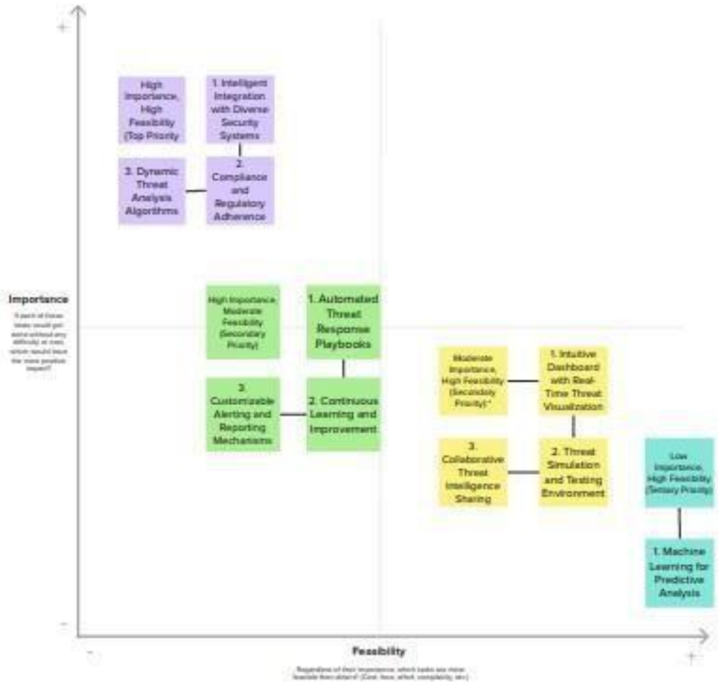
Prioritize

Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

20 minutes

TIP

Participants can use their cursors to point at where sticky notes should go on the grid. The facilitator can confirm the spot by using the laser pointer holding the H key on the keyboard.



High Importance, High Feasibility (Top Priority

1. Intelligent Integration with Diverse Security Systems

2. Compliance and Regulatory Adherence

3. Dynamic Threat Analysis Algorithms

High Importance, Moderate Feasibility (Secondary Priority)

1. Automated Threat Response Playbooks

2. Continuous Learning and Improvement

3. Customizable Alerting and Reporting Mechanisms

Moderate Importance, High Feasibility (Secondary Priority):*

1. Intuitive Dashboard with Real-Time Threat Visualization

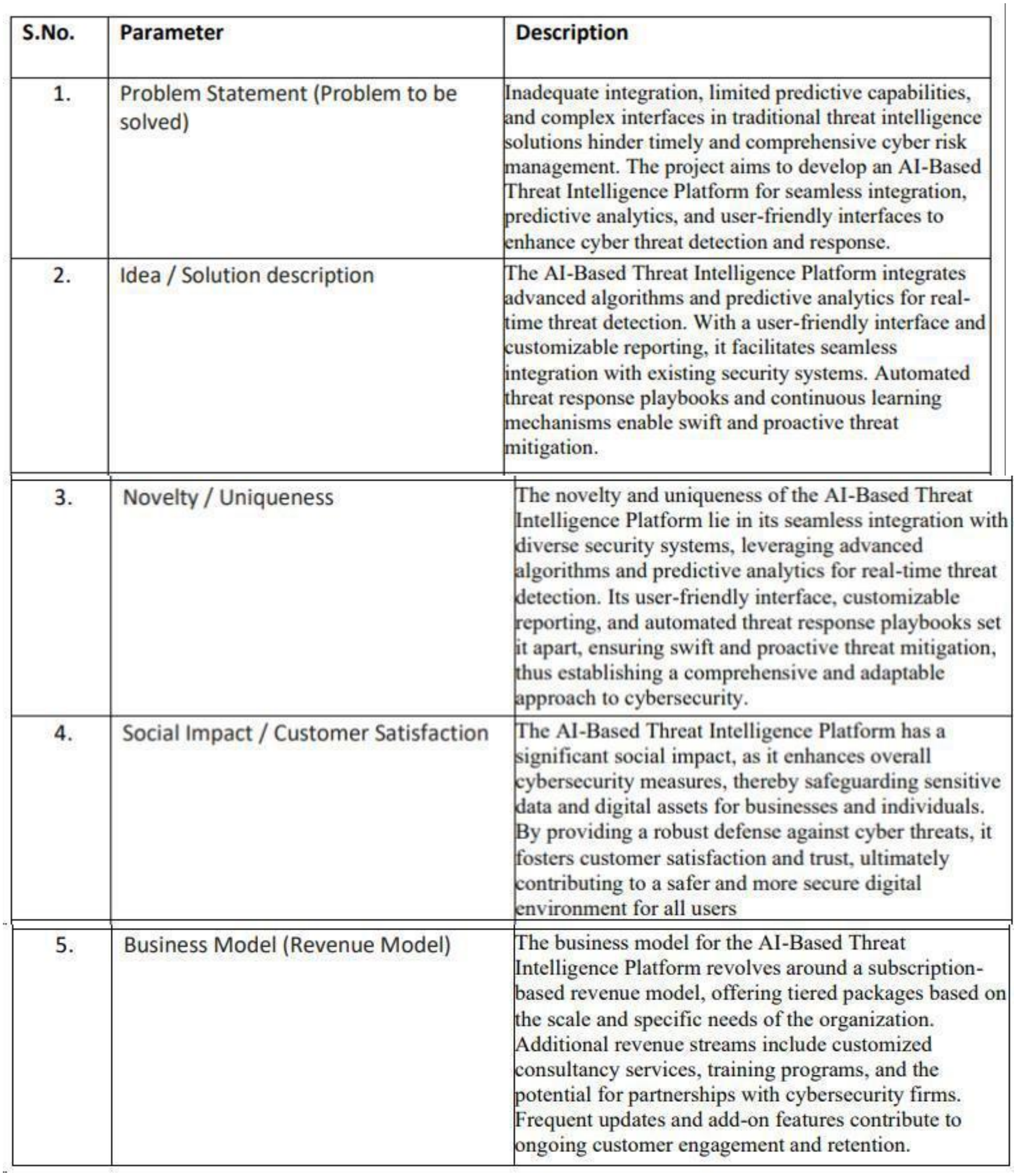
2. Threat Simulation and Testing Environment

3. Collaborative Threat Intelligence Sharing

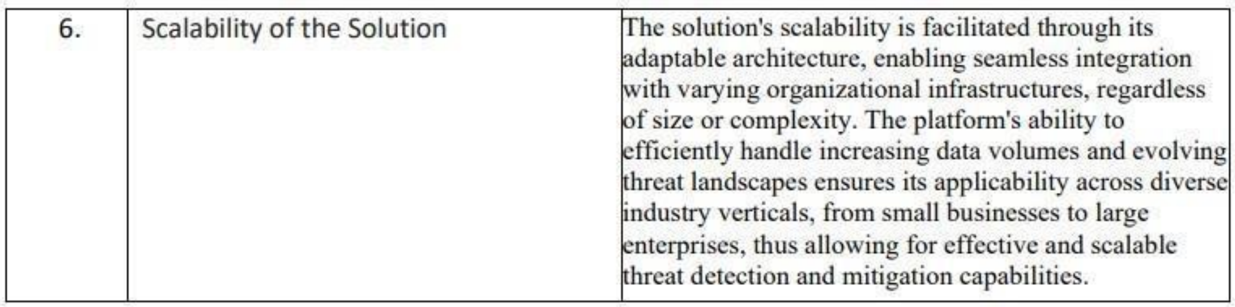
Low Importance, High Feasibility (Tertiary Priority)

1. Machine Learning for Predictive Analysis

Proposed solution



S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Inadequate integration, limited predictive capabilities, and complex interfaces in traditional threat intelligence solutions hinder timely and comprehensive cyber risk management. The project aims to develop an AI-Based Threat Intelligence Platform for seamless integration, predictive analytics, and user-friendly interfaces to enhance cyber threat detection and response.
2.	Idea / Solution description	The AI-Based Threat Intelligence Platform integrates advanced algorithms and predictive analytics for real-time threat detection. With a user-friendly interface and customizable reporting, it facilitates seamless integration with existing security systems. Automated threat response playbooks and continuous learning mechanisms enable swift and proactive threat mitigation.
3.	Novelty / Uniqueness	The novelty and uniqueness of the AI-Based Threat Intelligence Platform lie in its seamless integration with diverse security systems, leveraging advanced algorithms and predictive analytics for real-time threat detection. Its user-friendly interface, customizable reporting, and automated threat response playbooks set it apart, ensuring swift and proactive threat mitigation, thus establishing a comprehensive and adaptable approach to cybersecurity.
4.	Social Impact / Customer Satisfaction	The AI-Based Threat Intelligence Platform has a significant social impact, as it enhances overall cybersecurity measures, thereby safeguarding sensitive data and digital assets for businesses and individuals. By providing a robust defense against cyber threats, it fosters customer satisfaction and trust, ultimately contributing to a safer and more secure digital environment for all users
5.	Business Model (Revenue Model)	The business model for the AI-Based Threat Intelligence Platform revolves around a subscription-based revenue model, offering tiered packages based on the scale and specific needs of the organization. Additional revenue streams include customized consultancy services, training programs, and the potential for partnerships with cybersecurity firms. Frequent updates and add-on features contribute to ongoing customer engagement and retention.



6.	Scalability of the Solution	The solution's scalability is facilitated through its adaptable architecture, enabling seamless integration with varying organizational infrastructures, regardless of size or complexity. The platform's ability to efficiently handle increasing data volumes and evolving threat landscapes ensures its applicability across diverse industry verticals, from small businesses to large enterprises, thus allowing for effective and scalable threat detection and mitigation capabilities.

Solution architecture

The solution architecture of an AI-based threat intelligence platform typically consists of the following components:

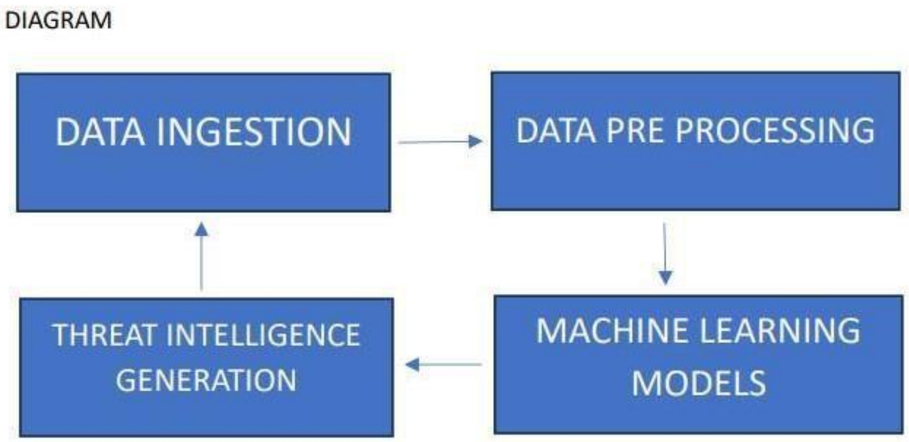
Data ingestion: This component is responsible for collecting security data from a variety of sources, such as system logs, network traffic, user behaviour, and external threat intelligence feeds. The data is then normalized and stored in a centralized location for analysis.

Data preprocessing: This component prepares the ingested data for machine learning by cleaning, transforming, and feature engineering.

Machine learning models: This component uses machine learning algorithms to analyse the pre-processed data and identify patterns and anomalies that may indicate potential threats.

Threat intelligence generation: This component converts the output of the machine learning models into human-readable and actionable threat intelligence reports.

Threat intelligence dissemination: This component distributes the threat intelligence reports to security analysts and other stakeholders across the organization.



Data ingestion:
The data ingestion component collects security data from a variety of sources, such as:

- System logs (e.g., firewall logs, application logs, operating system logs).
- Network traffic (e.g., NetFlow data, packet captures).
- User behaviour data (e.g., login data, file access data, web browsing data).
- External threat intelligence feeds (e.g., feeds from security vendors, government agencies, and open-source sources).

Data preprocessing:
The data preprocessing component prepares the ingested data for machine learning by cleaning, transforming, and feature engineering. This may involve:

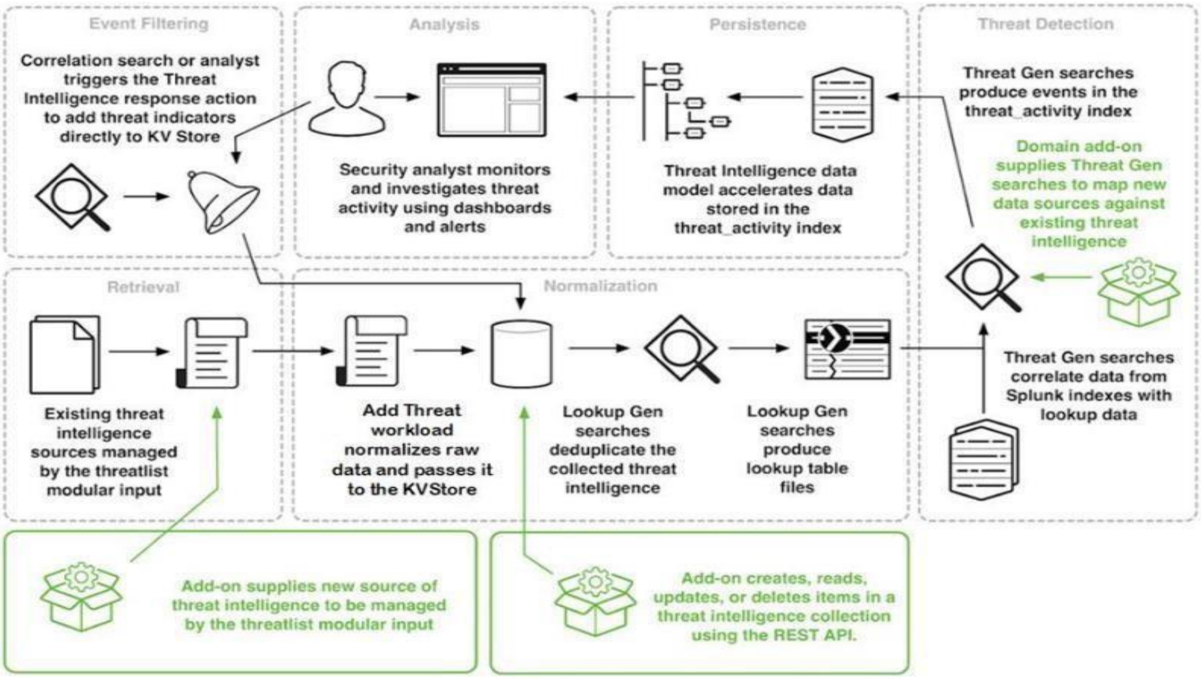
- Removing noise and outliers from the data.
- Transforming the data into a format that is compatible with the machine learning algorithms.
- Creating new features from the existing data that may be more predictive of potential threats.

Machine learning models:
The machine learning models component uses machine learning algorithms to analyse the pre-processed data and identify patterns and anomalies that may indicate potential threats. There are a variety of machine learning algorithms that can be used for this purpose, such as supervised learning, unsupervised learning, and deep learning.

Threat intelligence generation:
The threat intelligence generation component converts the output of the machine learning models into human-readable and actionable threat intelligence reports. This may involve:

- Correlating data from multiple sources to get a more complete picture of a threat.
- Enriching the data with additional information, such as the threat actor's motivations and capabilities.
- Prioritizing the threats based on their severity and impact to the organization.

Technology stack


Event Filtering
Correlation search or analyst triggers the Threat Intelligence response action to add threat indicators directly to KV Store
Analysis
Security analyst monitors and investigates threat activity using dashboards and alerts
Persistence
Threat Intelligence data model accelerates data stored in the threat_activity index
Threat Detection
Threat Gen searches produce events in the threat_activity index
Domain add-on supplies Threat Gen searches to map new data sources against existing threat intelligence
Retrieval
Existing threat intelligence sources managed by the threatlist modular input
Normalization
Add Threat workload normalizes raw data and passes it to the KVStore
Lookup Gen searches deduplicate the collected threat intelligence
Lookup Gen searches produce lookup table files
Threat Gen searches correlate data from Splunk indexes with lookup data
Add-on supplies new source of threat intelligence to be managed by the threatlist modular input
Add-on creates, reads, updates, or deletes items in a threat intelligence collection using the REST API.

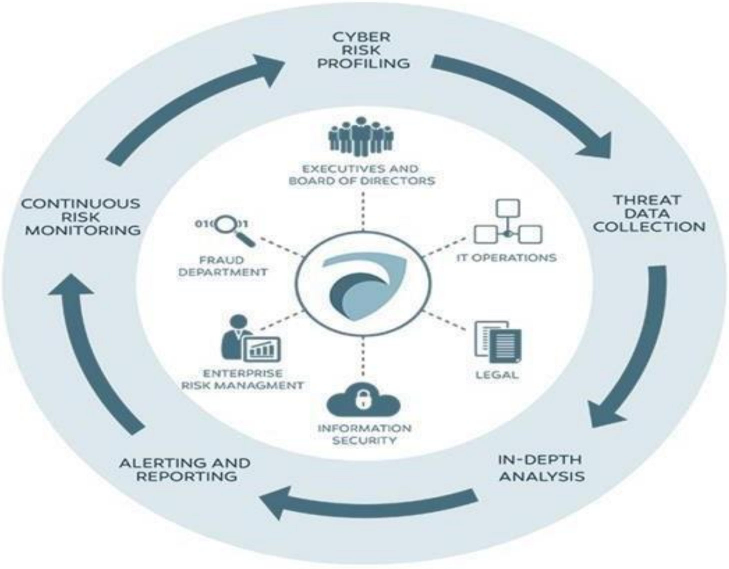
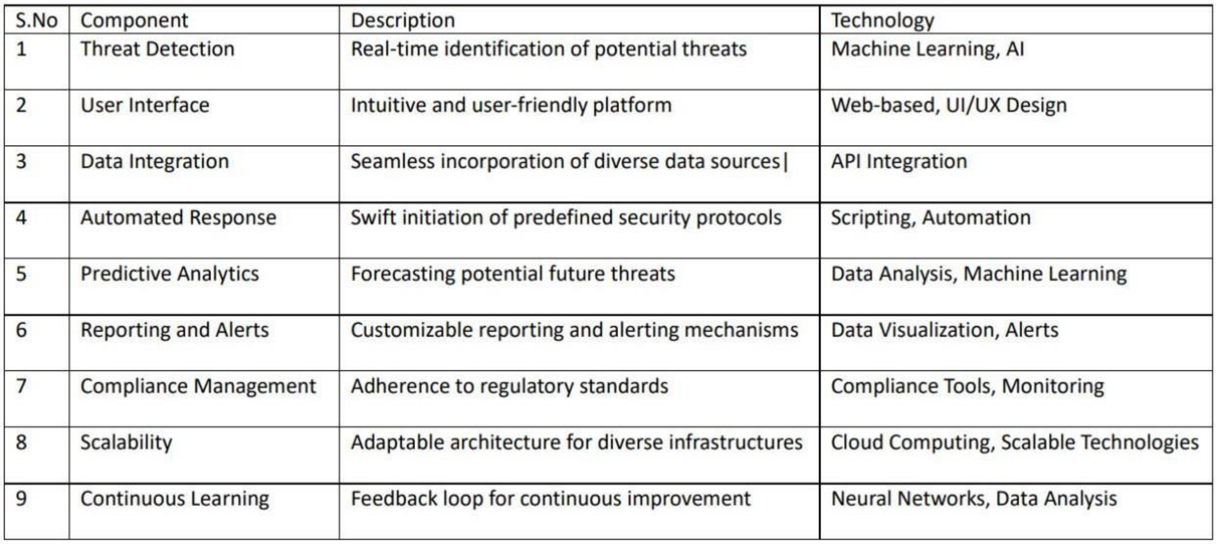
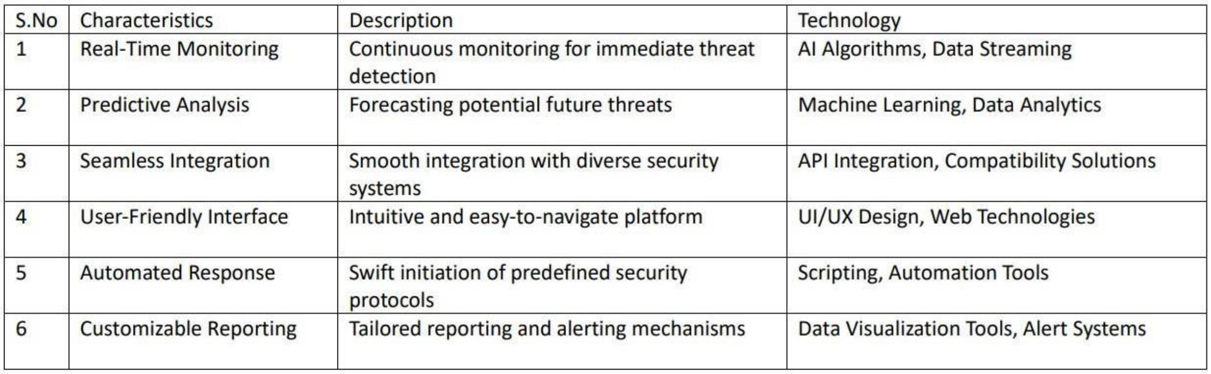


Table 1: Components & Technologies:



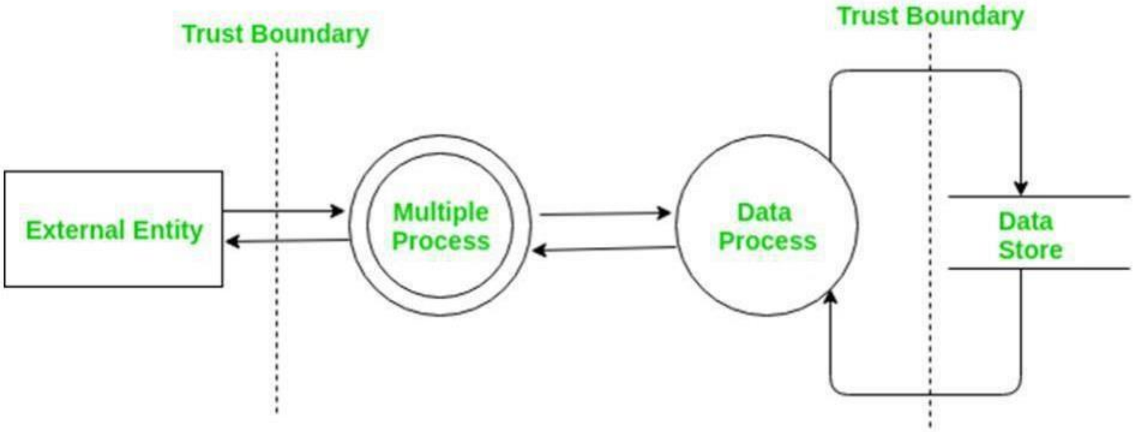
S.No	Component	Description	Technology
1	Threat Detection	Real-time identification of potential threats	Machine Learning, AI
2	User Interface	Intuitive and user-friendly platform	Web-based, UI/UX Design
3	Data Integration	Seamless incorporation of diverse data sources|	API Integration
4	Automated Response	Swift initiation of predefined security protocols	Scripting, Automation
5	Predictive Analytics	Forecasting potential future threats	Data Analysis, Machine Learning
6	Reporting and Alerts	Customizable reporting and alerting mechanisms	Data Visualization, Alerts
7	Compliance Management	Adherence to regulatory standards	Compliance Tools, Monitoring
8	Scalability	Adaptable architecture for diverse infrastructures	Cloud Computing, Scalable Technologies
9	Continuous Learning	Feedback loop for continuous improvement	Neural Networks, Data Analysis

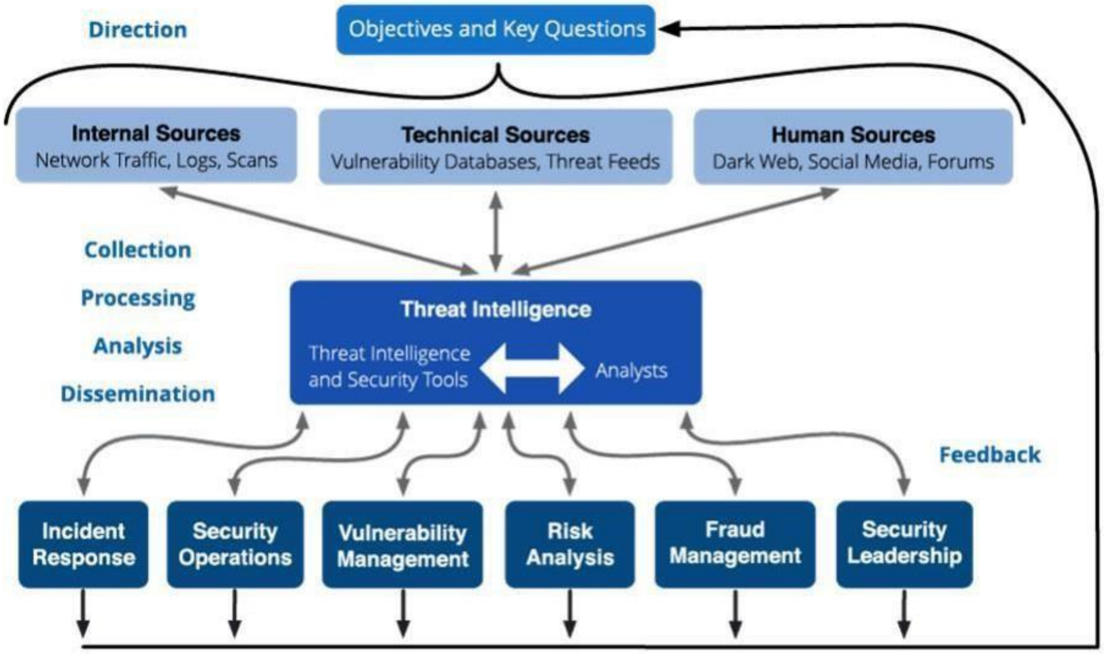
Table 2: Application Characteristics:



S.No	Characteristics	Description	Technology
1	Real-Time Monitoring	Continuous monitoring for immediate threat detection	AI Algorithms, Data Streaming
2	Predictive Analysis	Forecasting potential future threats	Machine Learning, Data Analytics
3	Seamless Integration	Smooth integration with diverse security systems	API Integration, Compatibility Solutions
4	User-Friendly Interface	Intuitive and easy-to-navigate platform	UI/UX Design, Web Technologies
5	Automated Response	Swift initiation of predefined security protocols	Scripting, Automation Tools
6	Customizable Reporting	Tailored reporting and alerting mechanisms	Data Visualization Tools, Alert Systems

Data flow


Trust Boundary
Trust Boundary
External Entity
Multiple Process
Data Process
Data Store


Direction
Objectives and Key Questions
Internal Sources
Network Traffic, Logs, Scans
Technical Sources
Vulnerability Databases, Threat Feeds
Human Sources
Dark Web, Social Media, Forums
Collection
Processing
Analysis
Dissemination
Threat Intelligence
Threat Intelligence and Security Tools
Analysts
Feedback
Incident Response
Security Operations
Vulnerability Management
Risk Analysis
Fraud Management
Security Leadership

User Stories

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance Criteria	Priority	Release
Customer (Mobile User)	**AI-based Threat Intelligence**	USN-1	As a user, I can register for the AI-based Threat Intelligence Platform by entering my email, password, and confirming my password.	I can access my AI-based threat intelligence dashboard	High	Sprint-1
Administrator	**AI Model Configuration**	USN-16	As an administrator, I can configure the AI models used for threat intelligence, specifying the sources and data parameters.	AI models are configured and operational	High	Sprint-2
Customer (Web User)	**Real-time Threat Alerts**	USN-17	As a web user, I can receive real-time threat alerts on my dashboard based on AI analysis of incoming data.	I can see real-time threat alerts relevant to my account.	High	Sprint-3
Customer Care Executive	**Incident Handling**	USN-18	As a customer care executive, I can view and respond to AI-generated incident reports and take appropriate action.	I can access incident reports and follow the prescribed action plan.	High	Sprint-3
Administrator	**Data Integration**	USN-19	As an administrator, I can integrate new data sources into the AI-based threat intelligence platform to enhance analysis.	New data sources are successfully integrated and contribute to threat analysis.	Medium	Sprint-4
Customer (Mobile User)	**Profile Customization**	USN-20	As a user, I can customize my threat alert preferences and notification channels within the AI-based platform.	I receive threat alerts through my preferred channels and for the selected types of threats.	Medium	Sprint-2

Overview

Building an AI-Based Threat Intelligence Platform: In an era marked by an ever-expanding digital landscape and increasingly sophisticated cyber threats, the need for robust and intelligent cybersecurity solutions has never been more pressing. The "AI-Based Threat Intelligence Platform" project is a pioneering endeavour that seeks to fortify organizations' defenses against a multitude of cyber adversaries. By harnessing the power of artificial intelligence, this platform aims to provide real-time threat detection, rapid incident response, and proactive defense mechanisms to safeguard critical assets and data.

Challenges: Cyber threats have become more diverse and elusive, with attackers employing advanced techniques to infiltrate systems, steal sensitive data, disrupt operations, and exploit vulnerabilities. Traditional security measures are often insufficient in the face of these evolving threats, necessitating a proactive, adaptive, and intelligence-driven approach.

Vision: This project envisions an AI-based Threat Intelligence Platform that not only identifies known threats but also uncovers emerging and zero-day threats before they can inflict harm. By collecting, normalizing, and analyzing vast quantities of data from various sources, the platform will provide an all-encompassing view of an organization's threat landscape. Using advanced machine learning algorithms, it will separate benign anomalies from malicious activities and enable rapid incident response, ultimately empowering organizations to stay one step ahead of cyber adversaries.

Significance: The AI-Based Threat Intelligence Platform stands to redefine the landscape of cybersecurity by offering a proactive defense strategy, enhanced visibility, and the ability to swiftly respond to threats, reducing the risk of data breaches, financial losses, and reputational damage for organizations of all sizes and sectors.

Overview

Building an AI-Based Threat Intelligence Platform: In an era marked by an ever-expanding digital landscape and increasingly sophisticated cyber threats, the need for robust and intelligent cybersecurity solutions has never been more pressing. The "AI-Based Threat Intelligence Platform" project is a pioneering endeavour that seeks to fortify organizations' defenses against a multitude of cyber adversaries. By harnessing the power of artificial intelligence, this platform aims to provide real-time threat detection, rapid incident response, and proactive defense mechanisms to safeguard critical assets and data.

Challenges: Cyber threats have become more diverse and elusive, with attackers employing advanced techniques to infiltrate systems, steal sensitive data, disrupt operations, and exploit vulnerabilities. Traditional security measures are often insufficient in the face of these evolving threats, necessitating a proactive, adaptive, and intelligence-driven approach.

Vision: This project envisions an AI-based Threat Intelligence Platform that not only identifies known threats but also uncovers emerging and zero-day threats before they can inflict harm. By collecting, normalizing, and analyzing vast quantities of data from various sources, the platform will provide an all-encompassing view of an organization's threat landscape. Using advanced machine learning algorithms, it will separate benign anomalies from malicious activities and enable rapid incident response, ultimately empowering organizations to stay one step ahead of cyber adversaries.

Significance: The AI-Based Threat Intelligence Platform stands to redefine the landscape of cybersecurity by offering a proactive defense strategy, enhanced visibility, and the ability to swiftly respond to threats, reducing the risk of data breaches, financial losses, and reputational damage for organizations of all sizes and sector.

Conclusion :-

Stage 1: Web Application Testing
Web application testing involves evaluating web applications for potential vulnerabilities and security weaknesses. It includes various assessments such as penetration testing, vulnerability scanning, and security auditing. The aim is to identify and mitigate risks that could lead to unauthorized access, data breaches, or other security threats within web applications. This process ensures the application's security, resilience against attacks, and adherence to best security practices.

Stage 2: Understanding the Nessus Report
The Nessus report typically contains detailed information about identified vulnerabilities in a network or system. It provides a comprehensive overview of security issues, their severity levels, affected systems, and potential risks. It often includes the Common Vulnerability Scoring System (CVSS) scores, which help prioritize vulnerabilities for remediation. The report guides security professionals in understanding and addressing identified weaknesses to improve overall security postur

Stage 3: Understanding SOC / SIEM / QRadar Dashboard

SOC (Security Operations Center): It is a centralized unit responsible for monitoring, detecting, analyzing, and responding to security incidents on an organizational level.

SIEM (Security Information and Event Management): It's a software solution that aggregates and analyzes security data from various sources, providing real-time analysis of security alerts and offering threat intelligence.

QRadar Dashboard: IBM QRadar is a SIEM product that provides a security dashboard displaying comprehensive data on security events, vulnerabilities, and threats. The dashboard offers real-time monitoring, analytics, and reporting, aiding security teams in managing and responding to potential security incidents effectively.

These tools and concepts (SOC, SIEM, and QRadar) help in centralizing security information, monitoring network activities, identifying potential threats, and aiding in the response to security incidents for improved cybersecurity. They present critical information in a consolidated manner, allowing security professionals to make informed decisions and take proactive measures to safeguard the network and its assets.

Future Scope :-

Stage 1: Future Scope of Web Application Testing
The future scope of web application testing is continually evolving to address the ever-changing cybersecurity landscape. Key advancements include:

Increased Automation: Utilizing AI and machine learning to automate testing processes, reducing manual efforts and improving efficiency.

Focus on APIs and Microservices: With the rise of microservices architecture, testing these smaller, distributed services and their APIs will be crucial.
Emphasis on IoT Security: As the Internet of Things (IoT) expands, there will be a focus on testing the security of interconnected devices and applications.

Enhanced Threat Modeling: Developing more robust threat models to proactively identify and address potential vulnerabilities before they are exploited.

Integrating DevSecOps: Merging security practices into the DevOps process to ensure security is integrated throughout the software development lifecycle.

Stage 2: Future Scope of Testing Processes

The future scope of testing processes encompasses broader technological advancements and methodologies such as:

Shift to Continuous Testing: Implementing continuous testing practices to allow for more frequent testing iterations in line with agile development methodologies.

Increased Adoption of AI/ML: Leveraging artificial intelligence and machine learning for predictive analytics, test optimization, and test automation.
Security Testing Advancements: Integrating security testing seamlessly into the testing process to ensure robust security measures from the early stages of development.

Enhanced User Experience Testing: Focusing on user-centric testing methodologies for enhanced user experience and accessibility testing.

Stage 3: Future Scope of SOC / SIEM
The future scope of Security Operations Center (SOC) and Security Information and Event Management (SIEM) involves advancements in:

Threat Intelligence Integration: Improved integration of threat intelligence feeds to enhance the detection and response to sophisticated threats.

Behavioral Analytics: Utilizing advanced behavioral analytics to detect anomalous behavior and potential threats in real-time.

Automation and Orchestration: Implementing more automation for incident response processes and security orchestration to handle threats more efficiently.

Cloud Security Monitoring: Adapting SOC and SIEM to monitor and secure cloud environments more effectively.

Predictive Capabilities: Evolving towards predictive analysis, forecasting potential threats before they manifest, and ensuring a proactive security stance.

These future scopes are crucial for staying ahead in the cybersecurity domain, ensuring robust testing practices and strengthening security measures in an ever- evolving technological landscape.

Topics explored :-

- Artificial Intelligence
- Machine Learning
- Cyber Security
- Team Management

Tools explored :-

- Tenable Nessus
- Qrador

--------**THE END**--------------