2. IDEATION PHASE

2.1 Thought Behind the Project

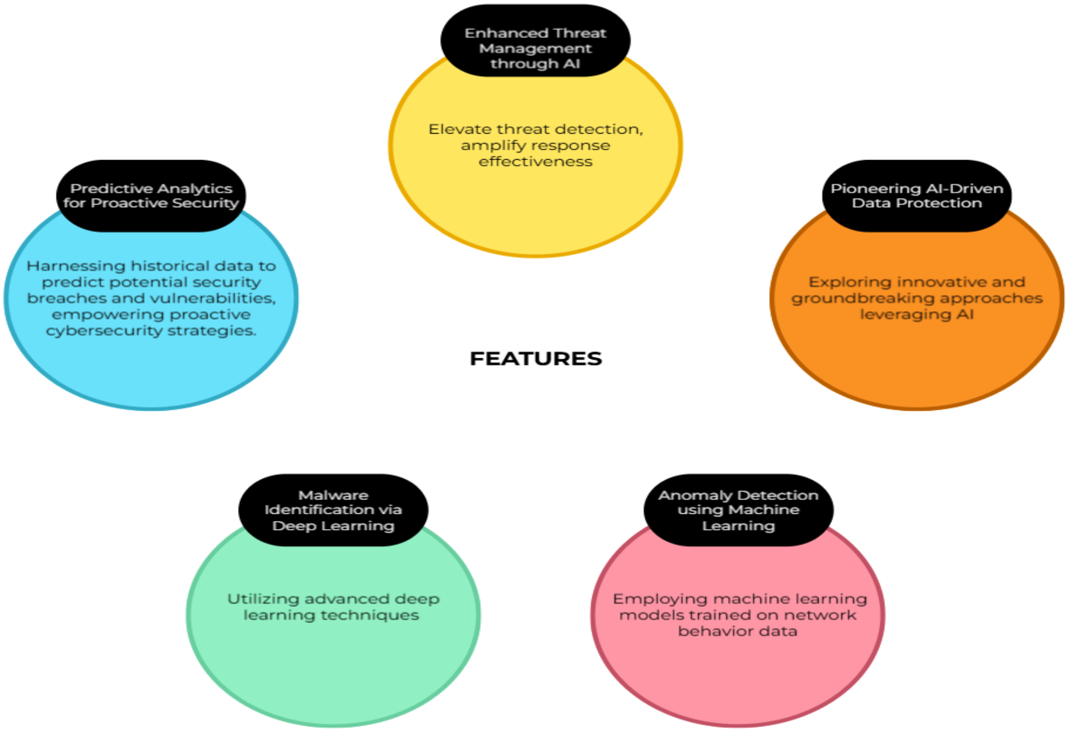
Saniya - With the rise in cybersecurity attacks like ransomwares, phishing, zero-day attacks, I find it important and necessary to have a real time monitoring system to get all the updates regarding the vulnerabilities.

Yashashri - The exciting part is building a security system that isn't static; it actually evolves and learns in response to new threats and data.

Pranoti - Ensuring real-time security monitoring is crucial in today's digital world. Detecting and addressing threats proactively can significantly enhance website security.

Mansi - Cybersecurity is an ongoing battle. A system that integrates both automated and manual security testing ensures comprehensive protection, covering both known and unknown threats.

2.2 Features



Enhanced Threat Management through AI
Elevate threat detection, amplify response effectiveness
Predictive Analytics for Proactive Security
Harnessing historical data to predict potential security breaches and vulnerabilities, empowering proactive cybersecurity strategies.
Pioneering AI-Driven Data Protection
Exploring innovative and groundbreaking approaches leveraging AI
FEATURES
Malware Identification via Deep Learning
Utilizing advanced deep learning techniques
Anomaly Detection using Machine Learning
Employing machine learning models trained on network behavior data

2.3 Empathy Map

Saniya -

1) Users - I feel our users are the IT Professionals, cybersecurity analysts who use websites and work online regularly.
2) Concerns - IT Professionals and cybersecurity analysts are under pressure to detect threats quickly and accurately. They go through increasing numbers of cyber threats on a day to day basis and often require tools that are efficient and well integrated. After going through some data, it was observed that there aren't many complex solutions developed.
3) Requirements - They demand rapid and accurate threat detection, efficient reporting mechanisms and seamless integration of multiple security systems.
4) Pain points - Delays in threat detection, overwhelming false positives and disjointed security systems that complicate analysis.
5) Gains - Faster threat response times, improved security posture, and reduced manual workload through automation.

Yashashri -

1) Target Audience: This initiative is designed for professionals in roles such as Security Operations Center (SOC) Analysts, Incident Responders, Threat Intelligence Teams, Chief Information Security Officers (CISOs), and IT Security Managers.
2) Overall Project Objective: The primary goal is to maximize the use of real-time security intelligence to bolster defensive strategies and preemptively reduce potential threats.

Pranoti -

1) Problem – Cyber threats evolve quickly, making websites vulnerable.
2) Need – A system for real-time monitoring and rapid threat detection.
3) Challenge – Security tools often produce false positives, wasting time.
4) Impact – Stronger, faster, and automated cybersecurity defenses.

Mansi -

1) Cyber threats are no longer occasional incidents; they are a constant reality**.** I see the need for a proactive security approach that doesn't just detect threats but anticipates them before they cause damage.
2) Time is the most critical factor in cybersecurity**.** The difference between detecting an attack in seconds versus minutes can determine whether a system stays secure or gets compromised. A fast and automated response mechanism is essential.