AI Driven Cybersecurity APP

Harshal Avinash Taware

Date : 26-01-2024

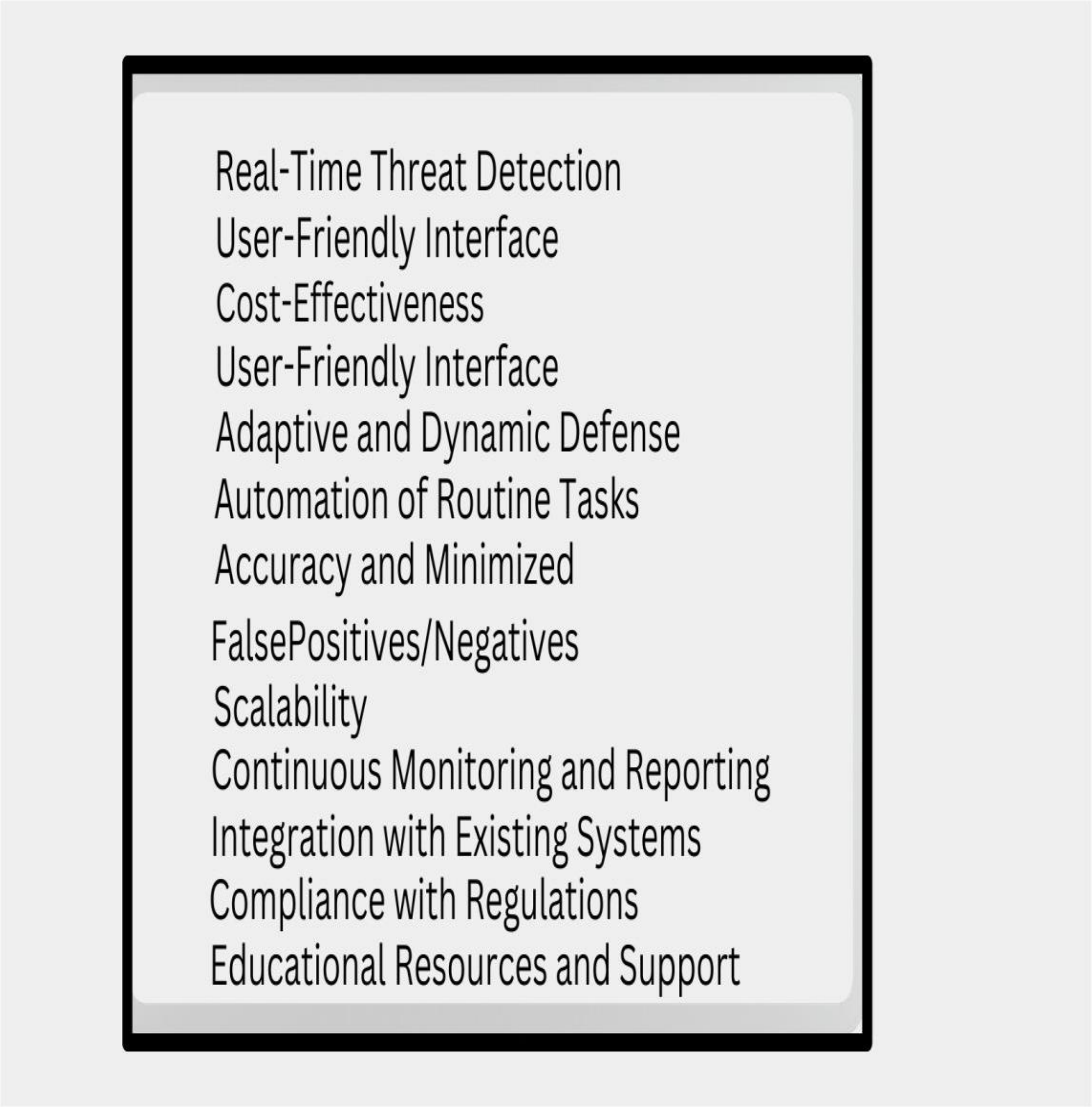
Abstract
In an era marked by escalating cyber threats, organizations face unprecedented challenges in safeguarding their digital assets. This abstract introduces an innovative solution—an AI-driven cybersecurity application designed to revolutionize the landscape of digital defense. Leveraging advanced machine learning algorithms, the application continuously analyzes network activity, adapts to emerging threat vectors, and provides real-time detection and mitigation. Its user-friendly interface ensures accessibility for cybersecurity professionals and non-experts alike, offering detailed insights and actionable recommendations. The scalability and adaptability of the app cater to businesses of varying sizes and complexities. This abstract encapsulates the essence of a cutting-edge cybersecurity solution poised to redefine how organizations fortify themselves against evolving cyber risks.

1.0 Problem Statement

Design and develop an AI-driven cybersecurity application that effectively identifies, analyzes, and mitigates emerging and sophisticated cyber threats in real-time, providing robust protection for organizations against evolving cyber attacks, data breaches, and unauthorized access.

2.0 Customer Needs Assessment

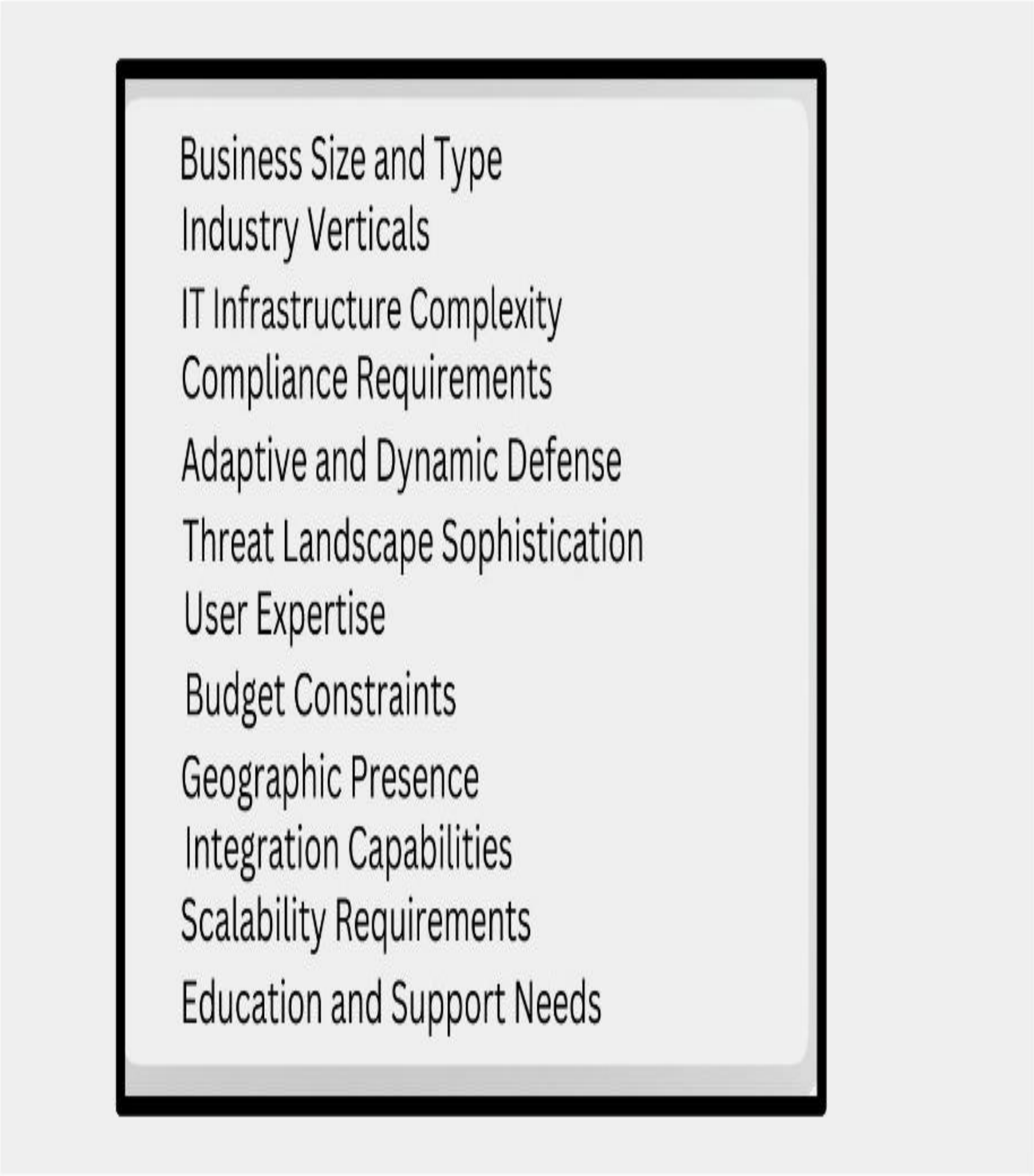
The AI-driven cybersecurity app is tailored to address the multifaceted needs of organizations in the digital security landscape. Clients emphasize the crucial requirement for real-time threat detection, seeking an application that can promptly identify and respond to potential security incidents. Furthermore, there is a strong demand for adaptive defense mechanisms, with organizations expecting the app to continuously learn and evolve using advanced machine learning to stay ahead of emerging cyber threats. The significance of a user-friendly interface is paramount, catering to cybersecurity professionals and non-experts alike, ensuring effective management and monitoring of cybersecurity measures. Beyond detection, there is a growing need for proactive defense measures, prompting organizations to seek solutions capable of autonomously mitigating threats in real-time. Accuracy, integration with existing systems, and scalability round out the key customer needs, positioning the AI-driven cybersecurity app as a dynamic and comprehensive solution in the face of evolving cybersecurity challenges.



Real-Time Threat Detection
User-Friendly Interface
Cost-Effectiveness
User-Friendly Interface
Adaptive and Dynamic Defense
Automation of Routine Tasks
Accuracy and Minimized
FalsePositives/Negatives
Scalability
Continuous Monitoring and Reporting
Integration with Existing Systems
Compliance with Regulations
Educational Resources and Support

Table 1. Initial Customer Needs List Obtained from Interviews and Observations

2.1 Weighting of Customer Needs



Business Size and Type
Industry Verticals
IT Infrastructure Complexity
Compliance Requirements
Adaptive and Dynamic Defense
Threat Landscape Sophistication
User Expertise
Budget Constraints
Geographic Presence
Integration Capabilities
Scalability Requirements
Education and Support Needs

Table 2. Hierarchal Customer Needs List (With Weighting factors)

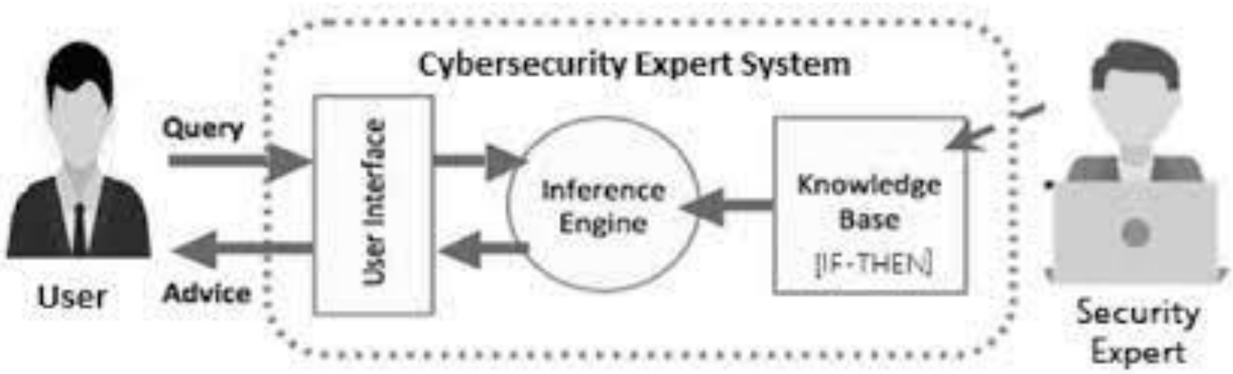


Figure 1. Cybersecurity Expert System

3.0 Revised Needs Statement and Target Specifications

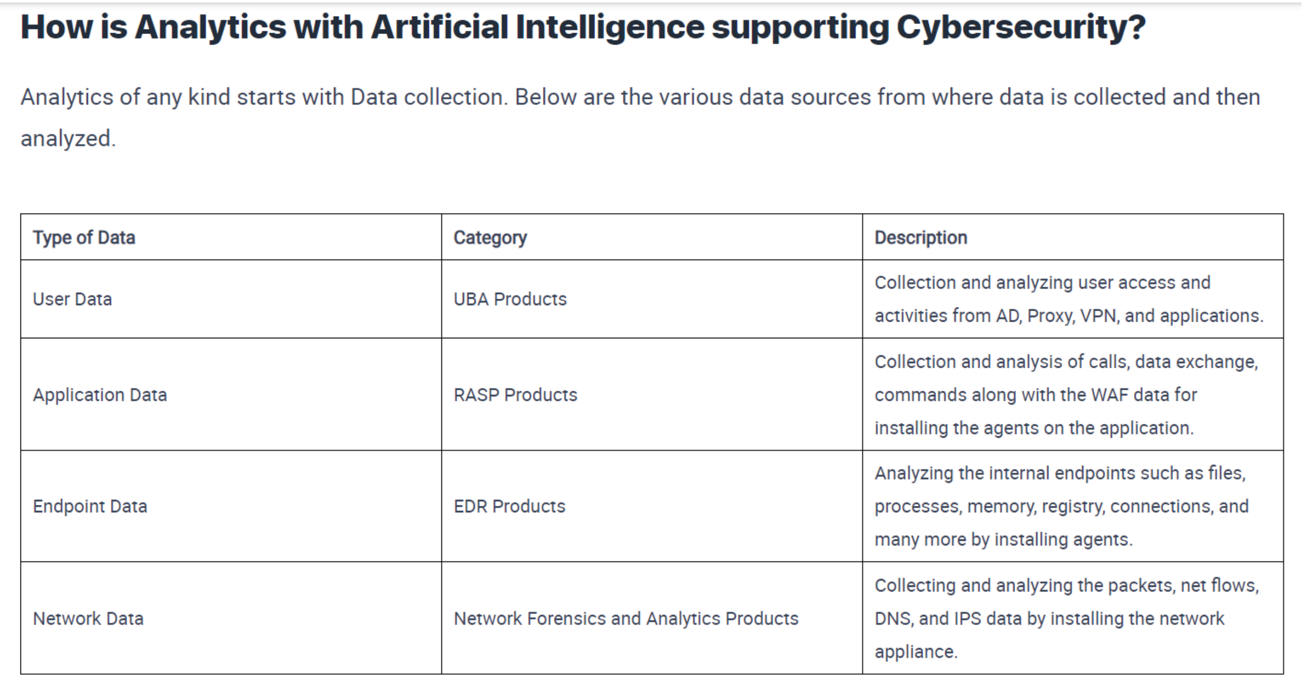
Customer Needs Statement :

In a rapidly evolving digital landscape, organizations require an AI-driven cybersecurity application that goes beyond traditional solutions. The pressing need is for real-time threat detection coupled with adaptive defense mechanisms, ensuring swift identification and mitigation of emerging cyber threats. Users demand a user-friendly interface that caters to both cybersecurity professionals and non-experts, facilitating seamless management. Additionally, there is a growing emphasis on proactive defense measures, with organizations seeking an application capable of autonomously mitigating threats in real-time while maintaining high accuracy. Integration with existing systems and scalability remain paramount, addressing the diverse cybersecurity needs of organizations of varying sizes.

Target Specifications :

The target specifications for the AI-driven cybersecurity app are refined to address the nuanced requirements of organizations seeking an advanced digital defense solution. The application is designed to provide real-time threat detection, leveraging adaptive defense mechanisms through continuous machine learning. The user interface prioritizes intuitive design for accessibility across user expertise levels. Proactive defense measures are a focal point, ensuring the app not only identifies but autonomously mitigates threats. Integration capabilities with existing systems are emphasized, allowing seamless compatibility and minimizing disruptions. Scalability is inherent, accommodating the diverse cybersecurity needs of organizations ranging from small businesses to large enterprises. These specifications position the AI-driven cybersecurity app as a dynamic, comprehensive, and user-centric solution in the ever-changing cybersecurity landscape.

4.0 External Search



How is Analytics with Artificial Intelligence supporting Cybersecurity?

Analytics of any kind starts with Data collection. Below are the various data sources from where data is collected and then analyzed.

Type of Data	Category	Description
User Data	UBA Products	Collection and analyzing user access and activities from AD, Proxy, VPN, and applications.
Application Data	RASP Products	Collection and analysis of calls, data exchange, commands along with the WAF data for installing the agents on the application.
Endpoint Data	EDR Products	Analyzing the internal endpoints such as files, processes, memory, registry, connections, and many more by installing agents.
Network Data	Network Forensics and Analytics Products	Collecting and analyzing the packets, net flows, DNS, and IPS data by installing the network appliance.

4.1 Benchmarking

These are some of the tools that are using the various algorithm of AI to get the best security to organizations.

- Symantec's Targeted Attack Analytics
- Sophos' Intercept X tool
- IBM QRadar Advisor
- Vectra's Cognito
- Darktrace Antigena

1. **Symantec's Targeted Attack Analytics** - This tool is used to uncover private and targeted attacks. It applies Artificial intelligence and machine learning to the processes, knowledge, and capabilities of Symantec's security experts and researchers. Symantec used the Targeted Attack analytics tool to counter the Dragonfly 2.0 attack. This attack targeted multiple energy companies in The USA and tried to gain access to operational networks.
2. **Sophos' Intercept X tool** - Sophos is a British software and hardware security company. Intercept X uses a deep learning neural network that functions like a human brain. Before a file is performed, Intercept X will retrieve millions of features from a file, perform an in-depth review and decide whether a file is benevolent or harmful within 20 milliseconds
3. **IBM QRadar Advisor** - IBM's QRadar Advisor is utilizing IBM Watson technologies to counter cyber-attacks. This utilizes AI to auto-examine signs of any vulnerability or

exploitation. QRadar Advisor utilizes cognitive reasoning to provide valuable feedback and speeds up the response process.

4. **Vectra's Cognito** - Vectra's Cognito detects attackers in real-time using AI. Threat detection and identification of attackers are automated in this tool. Cognito collects logs, cloud events, network usage data, and behavioral detection algorithms to reveal hidden attackers in workloads and IOT devices.
5. **Darktrace Antigena** - Darktrace is an effective method of self-defense. Antigena extends the critical functionality of Darktrace to recognize and duplicate the role of digital antibodies that recognize and neutralize threats and viruses. Antigena utilizes the Enterprise Immune System of Darktrace to recognize and react to malicious behavior in real-time based on the nature of the danger.

4.2 Business Opportunity

Al in Cybersecurity Market Dynamics Driver :

Rise in Cyberattacks Alarming Statistics and Urgent Need for Robust Cybersecurity Measures. Globally, the frequency of cyberattacks is on the rise, impacting individuals, enterprises, and governments, leading to substantial financial losses. Cybercriminals target endpoints, networks, and data, with motives ranging from political rivalry and financial gain to damaging reputation and furthering radical religious group interests. Prominent ransomware such as WannaCry, Petya, NotPetya, and BadRabbit have significantly affected large-scale enterprises and government organizations. The CISCO cybersecurity threat trends report for 2021 reveals alarming statistics, including a high percentage of organizations facing phishing attempts, malicious browser ads, crypto mining, and ransomware-related activities. The escalating sophistication of cyber threats, particularly ransomware, is compelling organizations globally to prioritize cybersecurity solutions and services for safeguarding critical IT infrastructure and sensitive data. According to Microsoft, the US was the primary target of 46% of cyberattacks in 2020, emphasizing the urgent need for robust cybersecurity measures worldwide.

5.0 Business Model

The business model for monetizing the AI-driven cybersecurity app involves a subscription-based pricing strategy. Customers can choose from different subscription tiers based on their business size, specific cybersecurity needs, and desired features. The subscription model ensures a recurring revenue stream, allowing continuous updates, improvements, and customer support. Additionally, the business can explore offering premium services, such as advanced threat intelligence feeds or personalized cybersecurity consultations, as upsell options. This business model aligns with scalability, ensuring affordability for small businesses while accommodating the diverse requirements of larger enterprises.

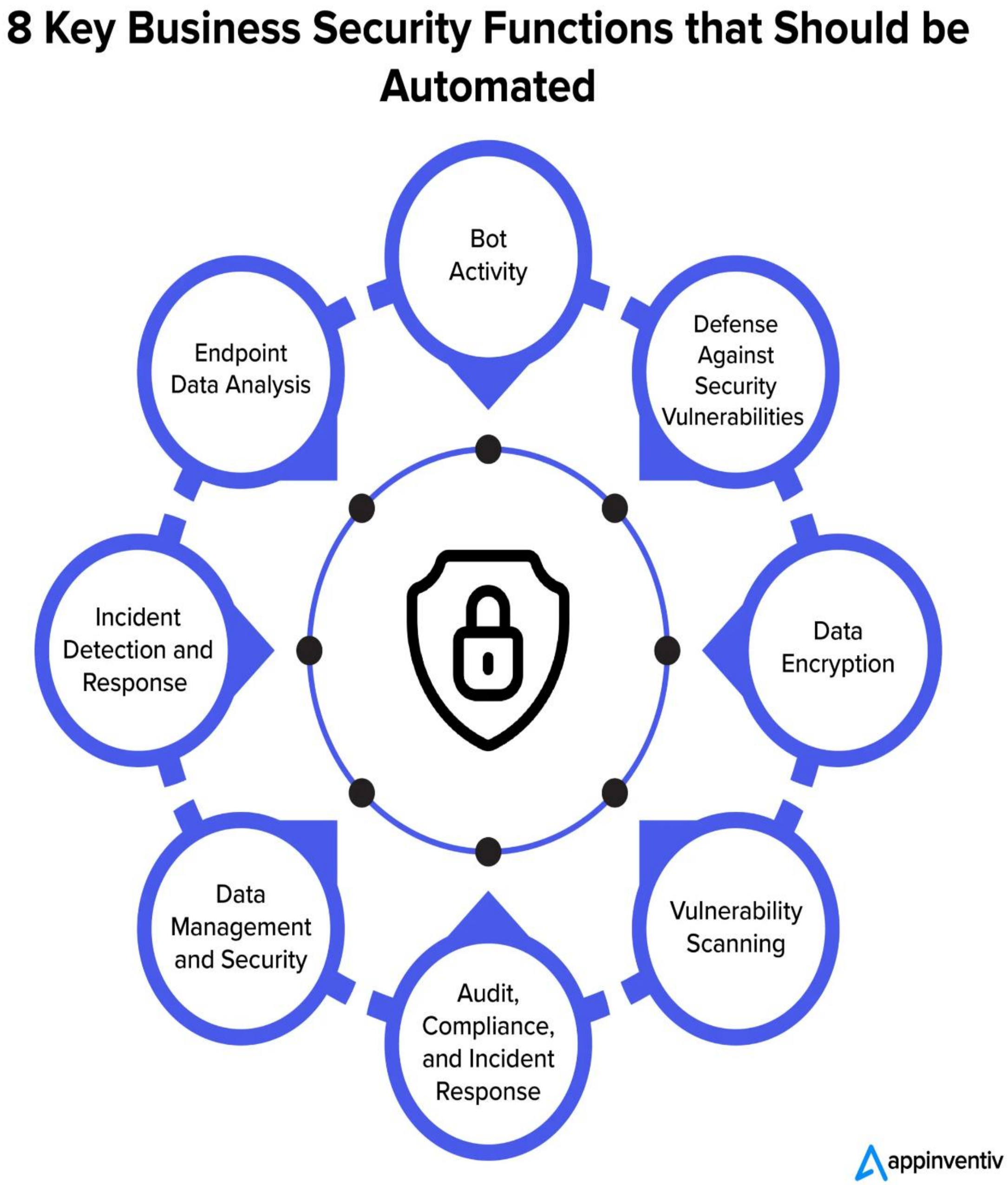

8 Key Business Security Functions that Should be Automated
Bot Activity
Defense Against Security Vulnerabilities
Data Encryption
Vulnerability Scanning
Audit, Compliance, and Incident Response
Data Management and Security
Incident Detection and Response
Endpoint Data Analysis
appinventiv

Figure 2.Business Model

7.0 Final Design

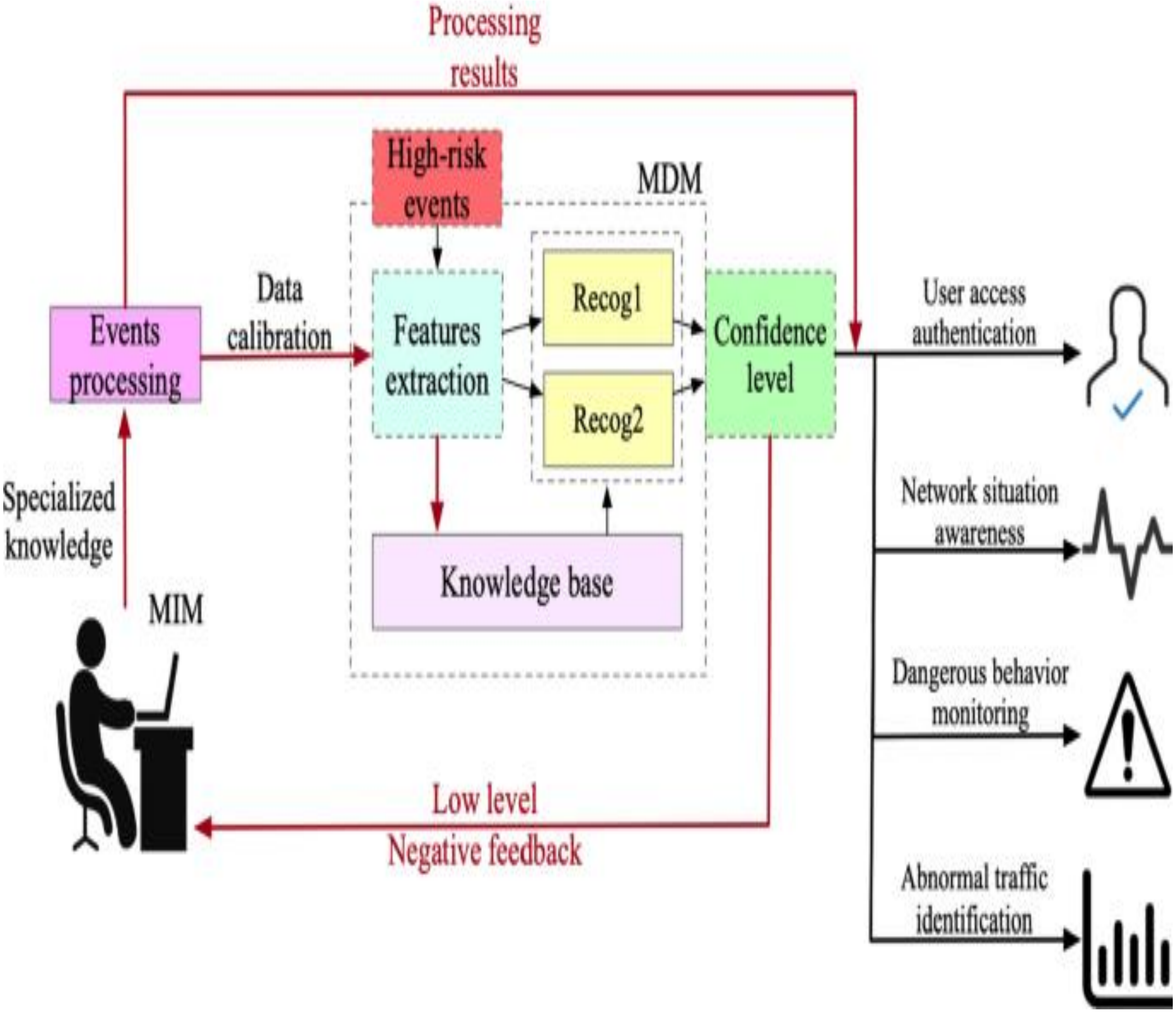


Figure 3.Final Model

7.1 How does it work?

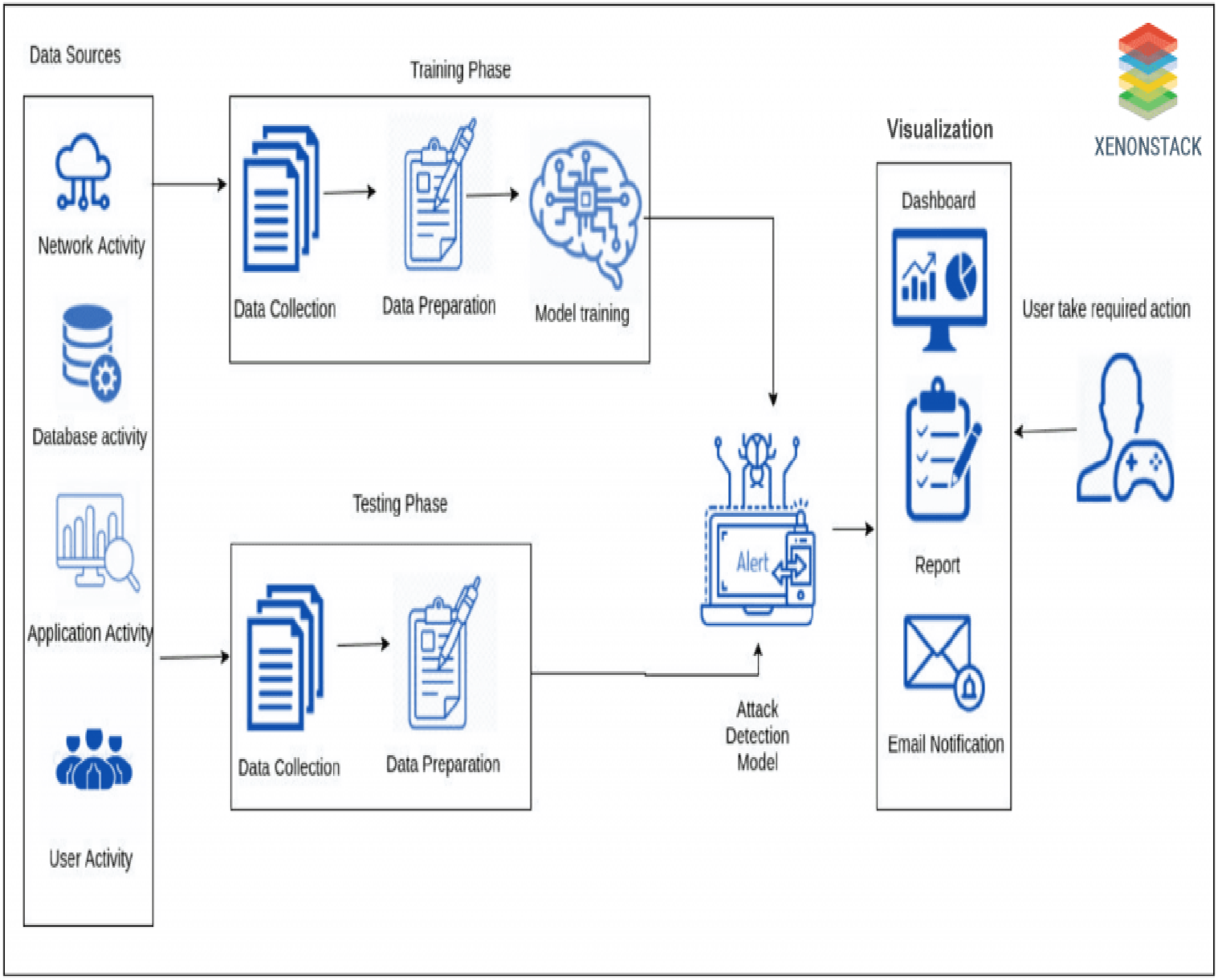


Figure 2.Working Model

8.0 Conclusions

The AI-driven cybersecurity app collects network activity data, analyzing patterns for potential threats. It provides users with real-time insights into detected threats, including their nature and severity. Users receive detailed reports on cybersecurity incidents, aiding in understanding and responding to security events. Additionally, the app offers actionable recommendations for proactive defense measures. All data collection and reporting are conducted with a focus on user privacy and compliance with relevant regulations.

References

https://appinventiv.com/blog/ai-in-cybersecurity
https://www.xenonstack.com/blog/artificial-intelligence-cyber-security
https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity
https://www.thesslstore.com/blog/5-real-world-ai-cybersecurity-applications-that-may-benefit-your-business
https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ai-cyber-security