CASE STUDY

Implementing an Intrusion Prevention System (IPS) to Protect a High-Traffic E-commerce Platform.

Presented By

Name	Registration No.
1. Mahamed Mohibur Reheman	2241018123
2. Aditya Sahu	2241019169
3. Sanjeeb Kumar Pusti	2241016499
4. Asutosh Samal	2241019249

Table of Content

Objective

1

Develop a Hybrid IPS integrating ML with traditional IPS

Combines machine learning and rule-based methods for stronger, adaptive intrusion prevention.

2

Address limitations of static rule-based systems

Overcome rigid, static IPS rules by enabling adaptability and detecting unknown evolving threats.

3

Ensure real-time threat detection, prevention, and adaptability

Provide real-time monitoring, quick prevention, and adaptive learning against diverse cyberattacks.

What is IPS ?

1

IPS = Intrusion Prevention System

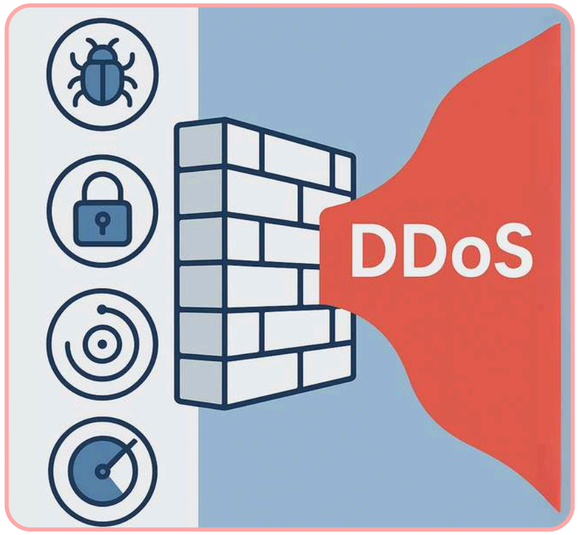
A proactive network security solution that continuously monitors, detects, and blocks malicious traffic to protect systems.

2

Immediate Intrusion Response

Operates inline in active mode, ensuring immediate prevention of attacks, unlike IDS which only passively monitors threats.

3



Practical Examples of IPS

Effectively blocks DDoS attacks, malware infiltration, suspicious port scans, and brute force login attempts in real-time.

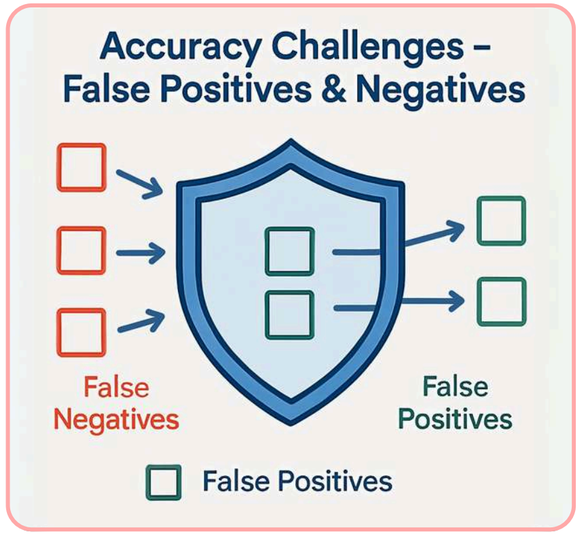
Problems in Traditional IPS

1

Signature Limitation

Traditional IPS fails to detect zero-day or evolving attacks as it depends heavily on signature-based detection methods.

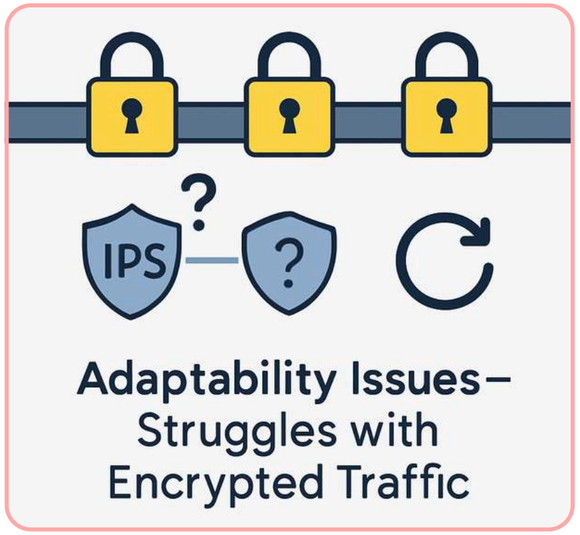
2



Accuracy Challenges

High rates of false positives and negatives reduce effectiveness, causing either missed threats or unnecessary alerts in networks.

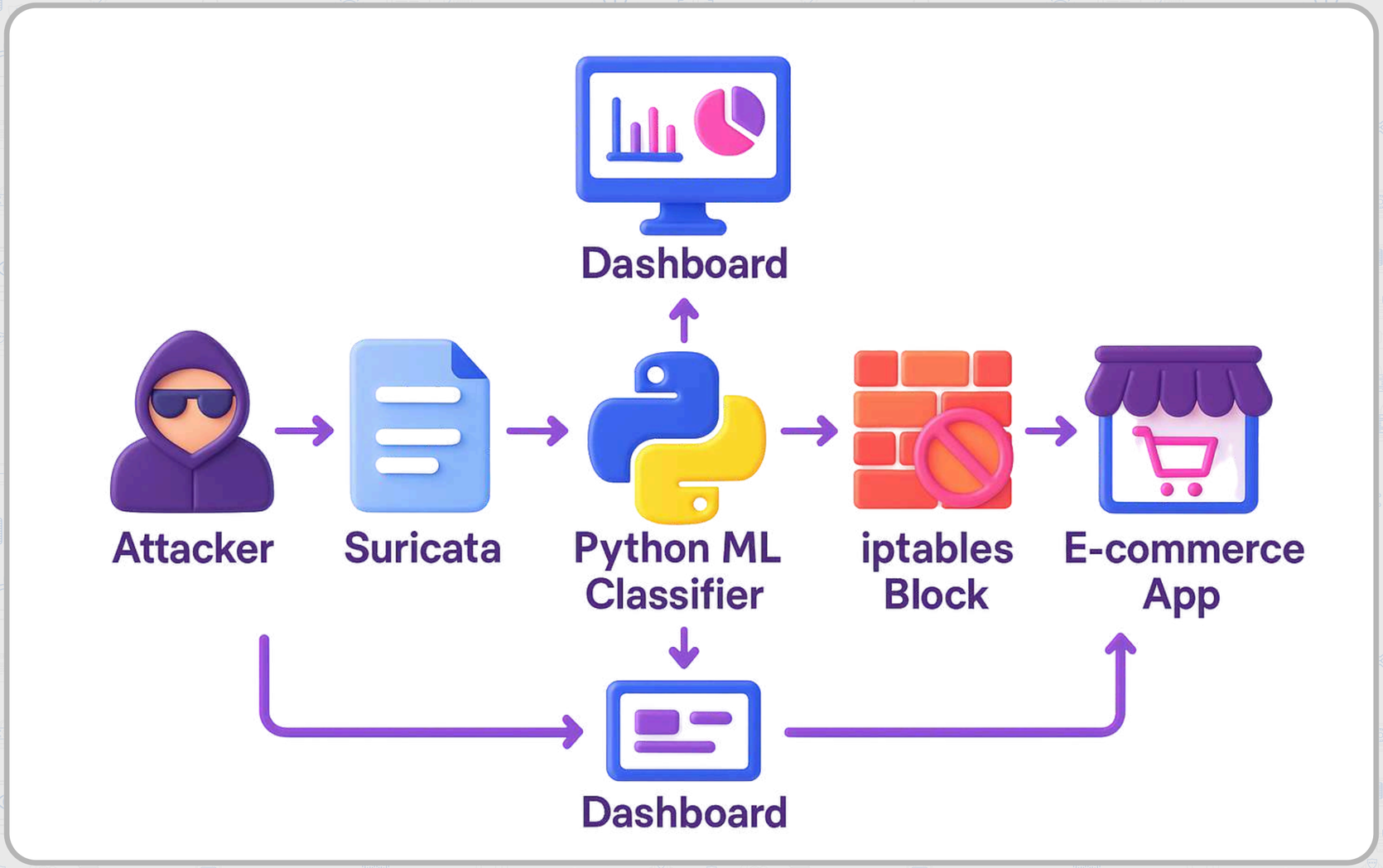
3



Adaptability Issues

Requires frequent manual updates and struggles with encrypted traffic, making it less efficient in large-scale modern environments.

Proposed Solution (Hybrid: IPS + ML)



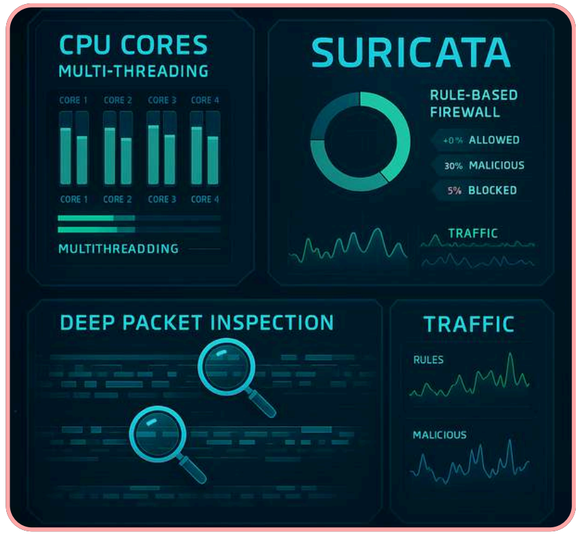
Technologies Used: Suricata

1

Open-Source IPS/IDS

Suricata is a high-performance, open-source IPS/IDS engine supporting accurate real-time threat detection.

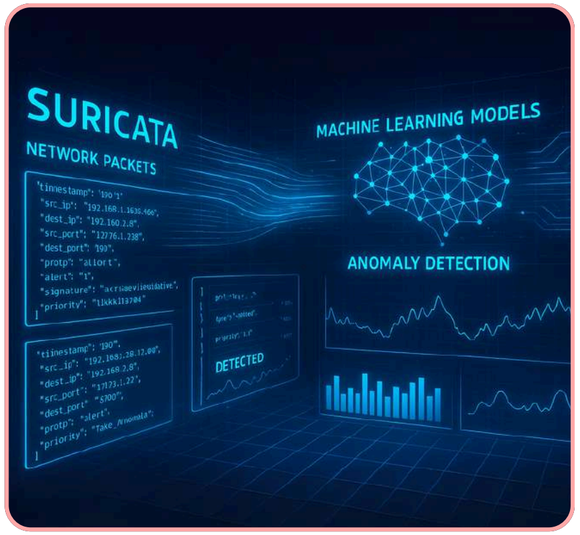
2



Advanced Features

Supports multi-threading, deep packet inspection, and flexible rule-based detection for stronger network security.

3

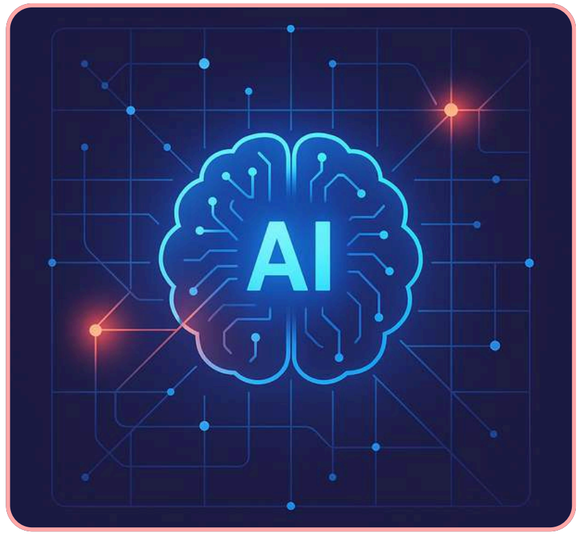


Data & Logging

Suricata captures packets in JSON format, generating alerts and logs that feed machine learning models for anomaly analysis.

Technologies Used: Machine Learning

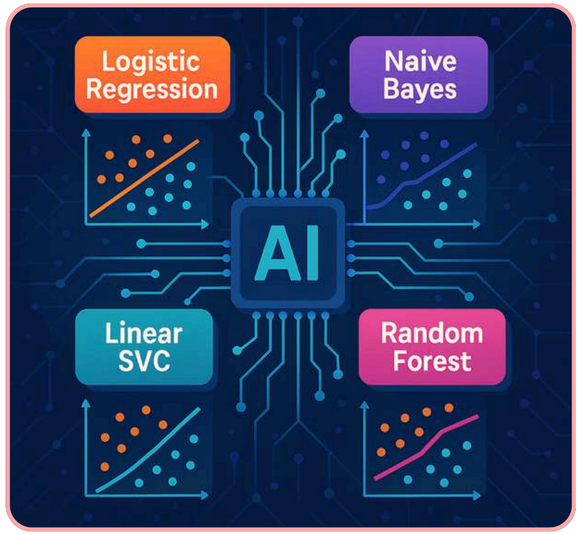
1



Detection Role

Machine Learning efficiently detects unknown attacks, anomalies, unusual behaviors, and hidden malicious traffic patterns.

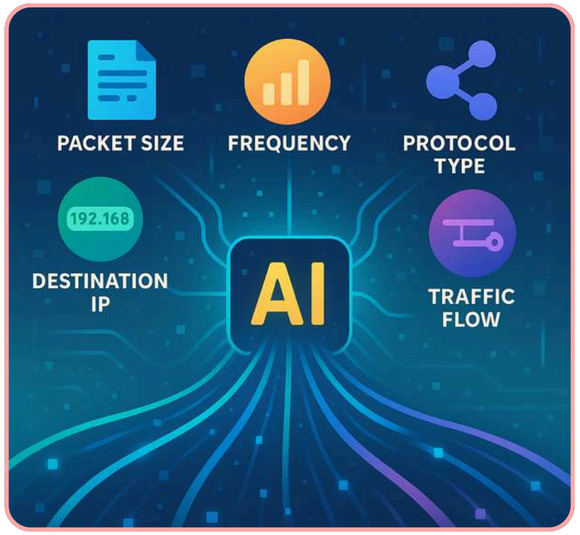
2



Algorithms Used

Implemented algorithms include Logistic Regression, Naive Bayes, Linear SVC, Random Forest, and other advanced techniques.

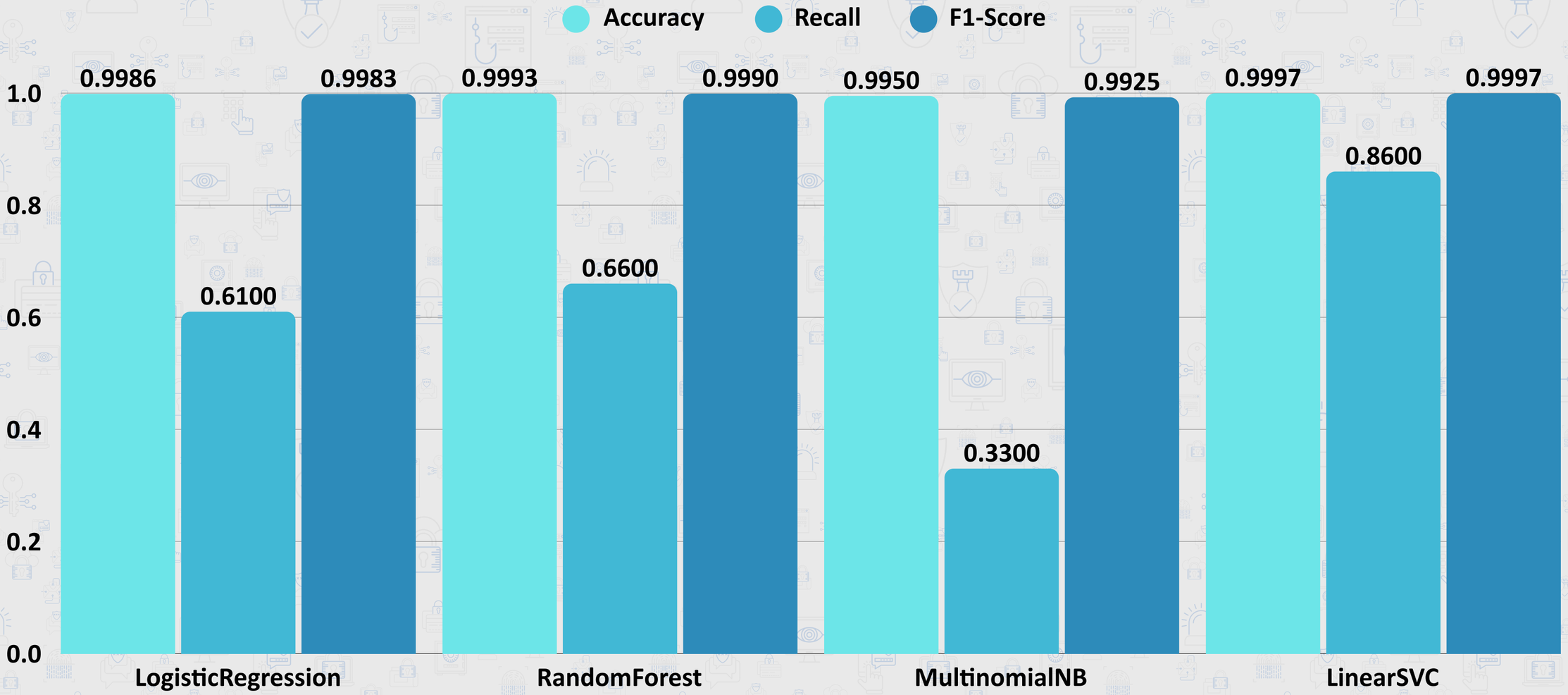
3



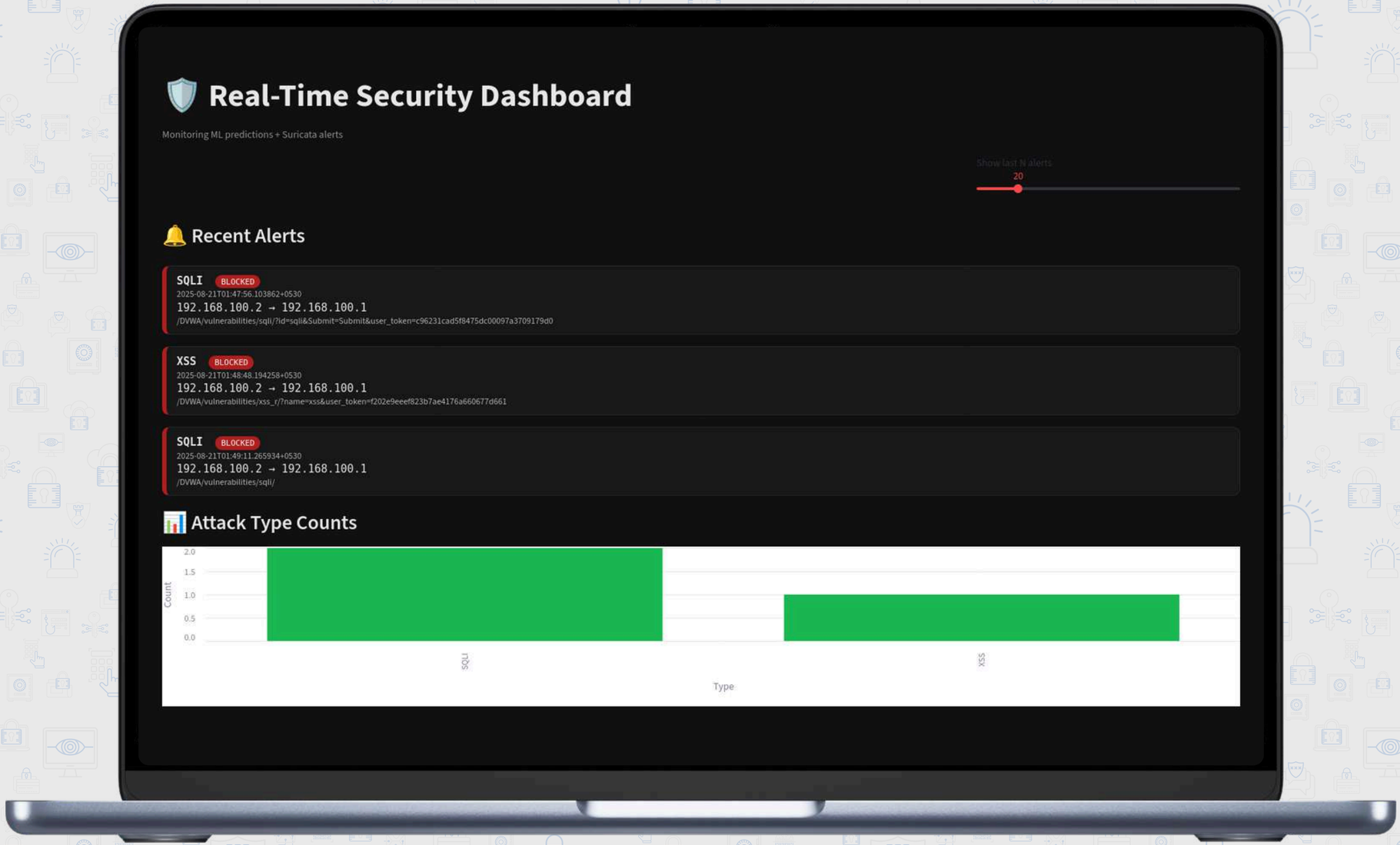
Input Features

Input features include packet size, frequency, protocol type, source/destination IPs, detailed traffic flow patterns.

Technologies Used: Machine Learning

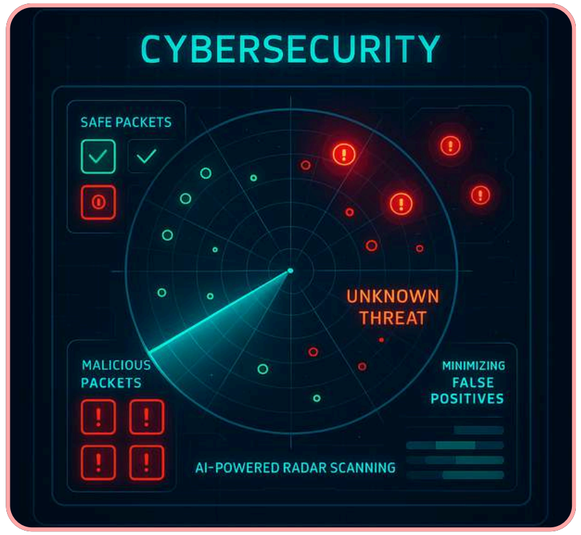


Dashboard


Real-Time Security Dashboard
Monitoring ML predictions + Suricata alerts
Show last N alerts
20
Recent Alerts
SQLI BLOCKED
2025-08-21T01:47:56.103862+0530
192.168.100.2 → 192.168.100.1
/DVWA/vulnerabilities/sqli/?id=sqli&Submit=Submit&user_token=c96231cad5f8475dc00097a3709179d0
XSS BLOCKED
2025-08-21T01:48:48.194258+0530
192.168.100.2 → 192.168.100.1
/DVWA/vulnerabilities/xss_r/?name=xss&user_token=f202e9eeef823b7ae4176a660677d661
SQLI BLOCKED
2025-08-21T01:49:11.265934+0530
192.168.100.2 → 192.168.100.1
/DVWA/vulnerabilities/sqli/
Attack Type Counts
2.0
1.5
1.0
0.5
0.0
Count
sqli
xss
Type

Advantages

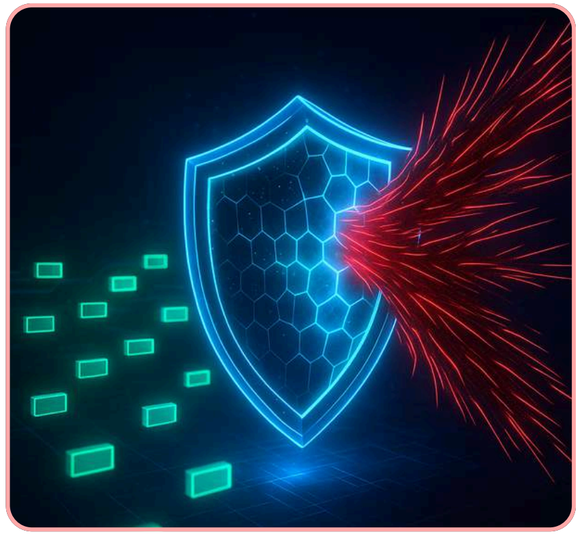
1



Comprehensive Threat Detection

Detects known and unknown threats efficiently, minimizing false positives/negatives, enhancing system security accuracy.

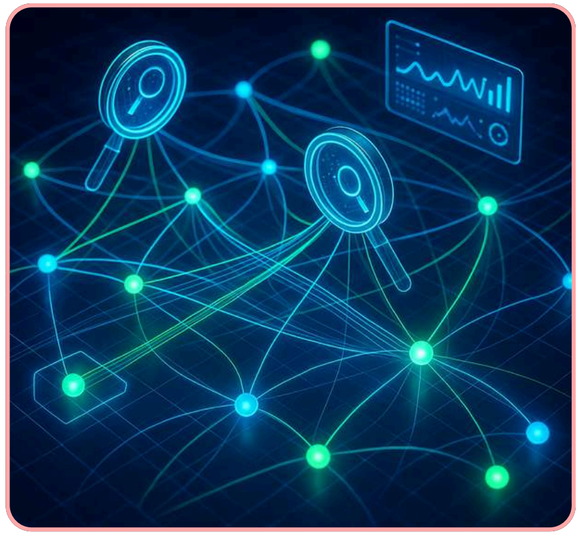
2



Adaptive Real-Time Prevention

Prevents evolving cyberattacks instantly with adaptive intelligence, ensuring proactive, dynamic, and reliable defense mechanisms.

3

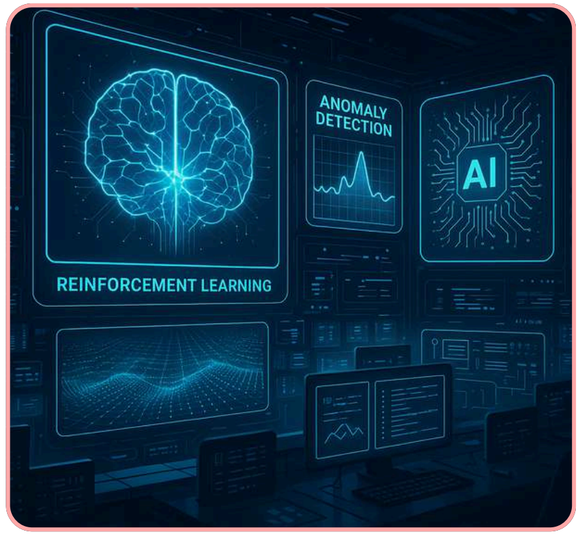


Enhanced Network Visibility

Provides detailed monitoring, deeper insights, and improved visibility for stronger, transparent, and secure network infrastructure.

Future Scope

1



AI-Driven Threat Intelligence

Integration with AI-powered platforms using Deep Learning and Reinforcement Learning for advanced anomaly detection.

2

Cloud-Native Deployment

Seamless deployment in scalable, containerized environments like Kubernetes and Docker for flexible, adaptive security.

3

Secure & Scalable Logging

Leverage blockchain for tamper-proof logging and Big Data frameworks like Kafka, Spark for large-scale analysis.

Conclusion

1

Stronger Adaptive Defense

Combining Hybrid IPS with Machine Learning provides smarter, adaptive, and resilient protection against evolving network threats.

2

Enhanced Security Framework

Effectively addresses traditional IPS limitations, delivering a robust and security framework for enterprise-level infrastructures.

3

Future-Ready Cybersecurity

Lays the foundation for intelligent, AI-driven cybersecurity ecosystems capable of detecting and preventing emerging threats.

References

1. National Institute of Standards and Technology - Guide to Intrusion Detection and Prevention Systems
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

2. Open Web Application Security Project - Top 10 Web Application Security Risks (SQLi, XSS, etc.)
https://owasp.org/www-project-top-ten/

3. Suricata IDS/IPS Official Documentation - Open-source network threat detection engine
https://suricata.io/documentation/

4. FreeCodeCamp - Real Time IDS with Python
https://www.freecodecamp.org/news/build-a-real-time-intrusion-detection-system-with-python/

5. Research Paper - "A Survey on Intrusion Detection and Prevention Systems" (IEEE)
https://ieeexplore.ieee.org/document/8721429

THANK YOU