Proof of Concept

The MalWhere AI-powered cybersecurity system was designed to detect network intrusions, malware, and phishing attacks in real-time. While initial testing showed high accuracy on benchmark datasets, real-world testing revealed high false positive rates and challenges in generalization.

System Performance Evaluation

Malware Detection Performance

We evaluated our malware detection model on real-world executable files beyond the training dataset.

Testing Accuracy: 95%

Observations:

- The model incorrectly classifies many benign files as malware, leading to false positives.
- Outdated training data affects the ability to detect new malware variants.

Proposed Solution:

- Retrain the model with updated malware datasets.
- Incorporate behavioral analysis instead of relying solely on static PE features.

Network Intrusion Detection Performance

Our NIDS model was tested on live network traffic captured using Scapy.

Testing Accuracy: 100%

Observations:

- Normal network traffic is frequently misclassified as malicious, increasing false alarms.
- Encrypted traffic, VPNs, and new attack patterns were not detected effectively.

Proposed Solution:

- Improve feature selection by incorporating flow-based and behavioral features.
- Train the model on more diverse network traffic datasets, including real-world packet captures.

Model Adjustments & Improvements

Issue Identified	Proposed Solution	Expected Impact
Feature Mismatch	Extract more behavioral & dynamic features	Improved detection accuracy
Outdated Training Data	Use real-world datasets & malware repositories	Better generalization
Poor Real-World Performance	Train on live network & real malware samples	More reliable predictions

Our models perform well on training datasets but struggle with real-world samples. High false positives indicate the need for better feature selection and threshold tuning. Retraining on updated, diverse datasets improves generalization and real-time accuracy.

This Proof of Concept demonstrates that while AI can enhance cybersecurity, continuous improvements are needed for real-world deployment