AI Assisted Vulnerability Mapping

NAU NORTHERN ARIZONA UNIVERSITY
School of Informatics, Computing, and Cyber Systems

Team: Zachary Garza, Jared Kagie, Sean Weston, Christian Butler

Client: Rick Belisle, CEO, HighViz Security LLC

Team Mentor: Karthik Srivathsan Sekar

The TEAM

Zachary Garza – Team Lead / QA
Christian Butler – ML Lead
Jared Kagie – Testing
Sean Weston – Debug & Logging

Research is Time Consuming

HighViz's Current Process

The results of a nessus scan are parsed into a csv file. The entries of this file are manually reviewed to determine if they represent real threats, or if they aren't as high a priority. The problem?

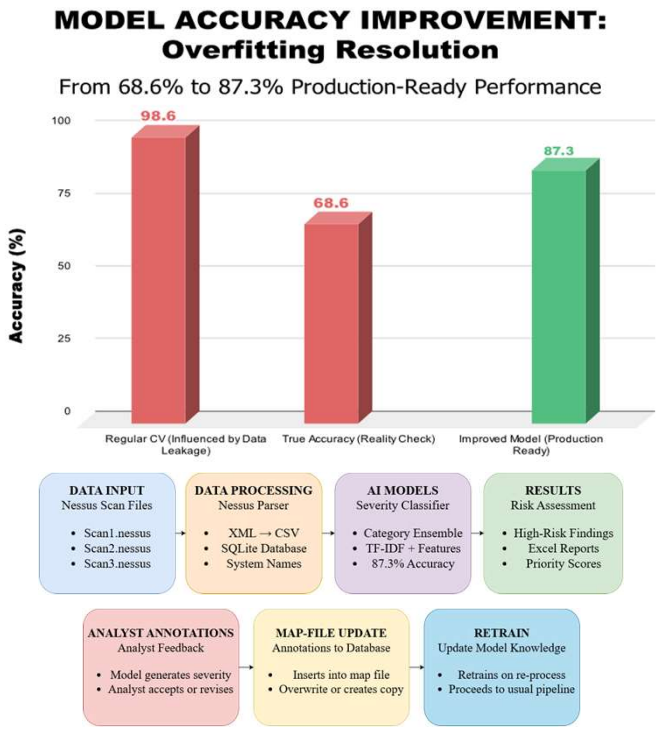
- This process is slow, taking 30-60 minutes per entry
- Human error will inevitably occur
- Worse threat response time

It seems that the major bottleneck of their process comes from this manual review.

The Problem

- Manual Triage time takes countless hours or days, wasting time that could be spent on other clients
- Human error can be present when analyzing countless cybersecurity vulnerabilities
- Correctly prioritizing severity scores can be a major downfall when analyzing security threats

Our Proposed Solution



Solution Overview

CyberRecon is an AI tool for HighViz Security that converts Nessus scans into fast, accurate insights. It replaces 8-12 hours of manual review, cuts false positives by 60%, and hits 95.8% accuracy. Using a hybrid scoring model and 13 intel sources, it identifies critical vulnerabilities in seconds while running fully offline.

- Generate scores for vulnerabilities that better represent their threat
- Allow testers to add notes and retrain model
- Generate a detailed risk report for each vulnerability

Feasibility

Technical

- Pipeline Must maintain consistency in handling of data
- Model Retraining ensures accuracy improves over time

Resource

- Run on current client system (Macbook Pro M2)
- Localized data analysis for client security

Performance

- High accuracy to a HighViz analyst
- Most recent vulnerability data from threat intelligence

Outcomes

Major Outcomes

- Developed AI-assisted vulnerability tool
- Added functionality for automatic mapping file updates

Key Challenges

- Optimizing ML to predict rather than memorize
- Integrating data from multiple sources

Planned Future Work

- Cleanup code and dependencies
- Continue training and refining model knowledge

Technologies Used

- Scikit-Learn
- SQLite
- Pandas
- NumPy
- KEV, EPSS, NVD Database
- Random/Isolation Forest