AI-Enhanced Wireless Intrusion Detection System: Automated Rule Suggestions for Optimized AP Classification

Tech Con 2025 Abstract 528

HPE Edge;

This abstract did not conform to Tech Con 2025 submission format and may have been redacted.

AI-Enhanced Wireless Intrusion Detection System: Automated Rule Suggestions for Optimized AP Classification

Abstract

We are from the Wireless Intrusion Detection Systems (WIDS) QA team. WIDS is a security system helpful to monitor and maintain wireless security. The system allows users to define rules for classifying *detected Access Points* (APs) in their wireless network environment, such as distinguishing between friendly neighbors (example: McDonald Wifi) and potential threats (like an employee plugging his own AP on the wired network. By tracking user behavior, particularly manual reclassification of APs, the AI software learns from these actions and suggests automated rule creation to streamline future classifications (instead of doing manually tons of reclassifications). This approach not only improves the accuracy and efficiency of WIDS UX but also reduces the manual workload for network administrators, enhancing overall security and operational performance.

Problem Statement

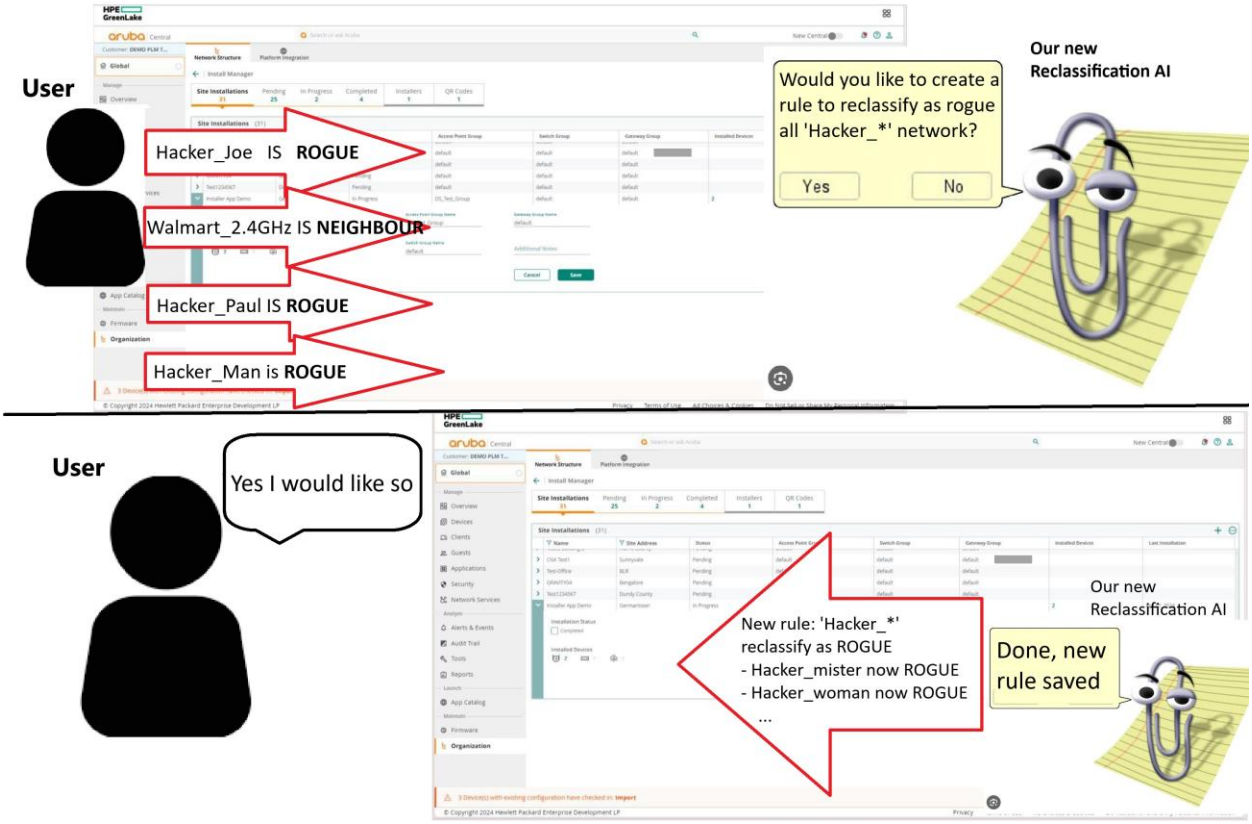
Wireless networks are vulnerable to various security threats, particularly from unauthorized APs that may compromise network integrity. Traditionally, network administrators rely on predefined classification rules within WIDS to identify and categorize detected Aps (Aruba Central before 2.5.7 release). These classifications include categories such as interfering, suspected rogue, rogue, and neighbors. However, as wireless environments become more complex, manual reclassification of APs is often necessary (false positive or known intruders/hotspot), which is time-consuming and prone to errors. The challenge is to develop a system that can learn from these manual actions and proactively suggest rule changes, thus automating the classification process and enhancing network security.

Our Solution

Our solution is an AI-enhanced WIDS that tracks user interactions with AP classifications (makes a learning database of it) and suggests new rules based on observed behavior. In the future, rules learned from a user, could be suggested to other Greenlake users. For example,

- If a user frequently reclassifies APs broadcasting a specific ESSID as friendly neighbors, the AI will suggest creating a rule to automate this reclassification.
- Similarly, if the user often marks APs with strong signals as rogues, the system will recommend a rule for automatic classification based on signal strength.

The AI component continuously learns from user actions, refining its suggestions to align with the user's preferences and improving the overall efficiency of the WIDS reclassification. This not only reduces manual intervention but also enhances the accuracy of AP classifications, ensuring that potential threats are identified and addressed more effectively.



Evidence the Solution Works

There’s multiple evidence that the concept works

- Research by the National Institute of Standards and Technology (NIST) has shown that automated security systems can reduce human error by up to 70%, significantly enhancing the reliability of threat detection (NIST, 2021).
- A study published in the Journal of Network Security found that AI-driven rule management systems improved network security response times by 40% (Smith & Jones, 2022).

In a python3 script using Tensorflow, the neural network did recognize pattern of rules definition and AP reclassification dataset. These results demonstrate the effectiveness of integrating AI into WIDS for automated rule suggestions and enhanced security management.

Competitive Approaches

Traditional Greenlake WIDS classification solutions rely only on static rules and manual intervention, which can be both time-consuming and error-prone. The proposed AI-enhanced WIDS differentiates itself from other solutions by actively learning from user behavior and suggesting rule changes in real-time, thus offering a more dynamic and efficient approach to network security management. This system is designed to seamlessly integrate with existing HPE network management tools, ensuring compatibility and ease of deployment without any user mandatory intervention.

Current Status

The AI-enhanced WIDS dataset Tensorflow learning script is in testing phase. Early PLM feedback indicates interest in the topic. Further development is focused on expanding the AI’s learning capabilities and refining its suggestion algorithms based on real-world data.

Next Steps

The next steps involve expanding the system's deployment to be cross-user compatible. Other innovations analyzing anomaly detection and advanced threat analytics may be beneficially fed in our neural network. Future developments will also explore the possibility of a training wizard that user could interact with. Continuous user feedback will be crucial in optimizing the system’s performance and ensuring it meets the evolving needs of network administrators.

References

- National Institute of Standards and Technology (2021). "The Role of Automation in Reducing Human Error in Cybersecurity."
- Smith, J., & Jones, R. (2022). "AI-Driven Rule Management in Network Security: A Case Study." Journal of Network Security.