WinLogGuardian

Garrett Christensen
Computer Science Department, Utah Valley University

Introduction

WinLogGuardian is a security log analysis tool designed to simplify the interpretation of Windows Security Logs. Windows Security Logs can be dense and difficult to understand, especially for those without a background in cybersecurity. This project uses a built in system along with Artificial Intelligence to interpret these logs and provide an explanation in plaintext. It also provides actionable insights for the user to take to respond to threats quickly.

Features

- Analyzes Windows Security Logs and assigns a severity level using a customizable JSON mapping.
- Integrates with OpenAI's API model to provide clear summaries and actionable security recommendations.
- Condenses repeated logs to reduce clutter and highlight important events
- Simple graphical user interface for easy navigation
- Real time alert system to notify the user of incoming critical logs.

AI Report Example

"This log entry signifies a failed logon attempt. An attempt was made to access the "Admin" account from the IP address "192.168.1.10", but was unsuccessful presumably because of an incorrect username or password.
Security Actions:
1. Alert the user : The account owner of "Admin" should be immediately notified about the failed login attempt. Whether it was a result of their mistake or not, they should be aware of it.
2. Identify the source : If the user did not initiate this, try to locate where the IP address 192.168.1.10 is coming from (for example: locational data, linked user, linked device etc).
3. Increase monitoring on the affected account : Keep a watchful eye on the activity related to the account "Admin" to prevent any nefarious activities from happening. …"

Results & Impact

WinLogGuardian streamlines the process of interpreting complex Windows Security Logs. By leveraging AI, this program provides clear, readable summaries that helps users quickly understand potential threats and take action. The condensed log view minimizes redundancy, making it easier to focus on critical events. Real time alerting system ensures that users are notified of critical severity events. Overall, this project enhances security awareness and responsiveness, especially for users without a deep cybersecurity background.

Future Updates

- Scheduled Log Analysis
- Cloud Integration
- More advanced Visualization
- Custom alerting system
- Multiplatform integration

References

- P.K. Sahoo, R.K. Chottray, and S. Pattnaiak, "Research issues on windows event log," *International Journal of Computer Applications*, vol. 41, no. 19, 2012, Foundation of Computer Science.
- R. Vaarandi and M. Pihelgas, "Using security logs for collecting and reporting technical security metrics," in *2014 IEEE Military Communications Conference*, 2014, pp. 294–299.
- G. Thomas, "Windows 8 Security Event Log," [Online]. Available: https://www.computerperformance.co.uk/win8/windows-8-security-event-log/. [Accessed: Apr. 12, 2025].
- K. Kent and M. Souppaya, "Guide to computer security log management," *NIST Special Publication*, vol. 92, pp. 1–72, 2006.
- N. Stanciu, "Importance of event log management to ensure information system security," *Metalurgia International*, vol. 18, no. 2, pp. 144, 2013.
- E. Akbaş, "Enhancing Incident Response with Live Logs: The Significance and Challenges of Maintaining Sufficient Log Retention for Mitigating Cyber Attacks," in *International Conference on Cyber Security ICCYS-23*, vol. 10, 2023.
- N.G. Camacho, "The role of AI in cybersecurity: Addressing threats in the digital age," *Journal of Artificial Intelligence General Science (JAIGS)*, vol. 3, no. 1, pp. 143–154, 2024.
- F. Jimmy, "Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses," *Valley International Journal Digital Library*, vol. 1, pp. 564–574, 2021.