LogSage: Secure Log Monitoring

Arza Henrie
Computer Science Department, Utah Valley University
Faculty Advisor: Dr. Sayeed Sajal

Introduction

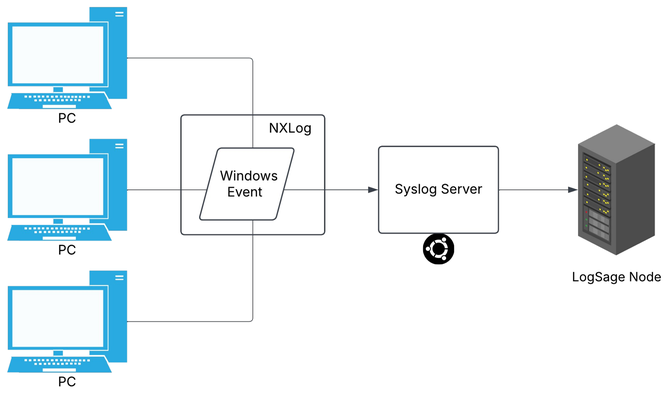
LogSage is a machine learning-based system for secure Windows Event log monitoring and user behavior analysis. Unlike cloud-reliant tools, LogSage performs **localized training and threat detection**, keeping sensitive data **on-premise** to protect privacy and reduce risk. Our approach demonstrates the growing importance of deploying AI **within internal systems** to strengthen cybersecurity without compromising data integrity.

Technologies Used

Logs → Windows, Ubuntu, NXLog, rsyslog
Data Processing → Bash, Go, pandas, numpy
Machine Learning → Python, sklearn, joblib
Web Application → Flask, HTML, CSS, JavaScript, Plotly
Languages → Go, Python, Bash, JavaScript, HTML, CSS

System Design

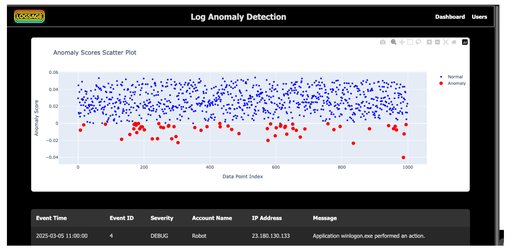
- **User PCs:** Endpoints generating Windows Event Logs from system activity, security events, and applications.
- **NXLog:** Lightweight agent on user PCs that forwards logs to the central logging system.
- **Syslog Server:** Central log repository for long-term analysis and security auditing.
- **LogSage Node:** Machine learning component that analyzes logs to detect anomalies and potential security threats.



Non-Private AI-Driven SIEM Solutions

- **IBM QRadar SIEM:** AI-powered alert enrichment, threat prioritization, and third-party integration for large-scale security management [1].
- **SentinelOne Singularity™:** AI-driven threat detection and response with deep visibility via the Elastic Search AI Platform [2].
- **CrowdStrike Falcon:** Unified threat intelligence and analytics with seamless data integration and AI-based detection [3].

App Design Iterations



The first design included only a simple dashboard of logs being received and anomalies tied to logs flagged by the machine learning model. The latest iteration includes a dashboard for all logs and user analytics on a separate page.

Continuing Research

- **Multi-Platform Log Ingestion:** Extend LogSage's capabilities to support logs from Linux, macOS, and cloud-based systems, enabling broader threat visibility across hybrid environments.
- **Advanced Ensemble Learning:** Improve anomaly detection by combining multiple machine learning models, increasing precision and reducing false positives.
- **Real-Time Alerting:** Implement low-latency alerting systems to deliver immediate notifications, enhancing incident response times and operational resilience.

References

IBM. *IBM QRadar SIEM*. 2024, Apr. Accessed 18 Mar. 2024. Available: https://www.ibm.com/products/qradar-siem.

Elastic. *AI-Driven SIEM Solution & Security Analytics: Elastic Security*. 2025. Accessed 19 Mar. 2025. Available: https://www.elastic.co/security/siem.

CrowdStrike. *Next-Gen SIEM: CrowdStrike*. 2025. Accessed 5 Mar. 2025. Available: https://www.crowdstrike.com/platform/next-gen-siem/