A Lightweight Software Solution for Log Analysis

이시헌[1], 김지윤[1], 김서현[1], 황지온[1]*

[1]협성대학교 소프트웨어공학과, 화성, 대한민국

**Corresponding Author: zhwang@uhs.ac.kr*

Abstract

1. Background

고도화되는 사이버 위협과 AI 기술 발달이 맞물리며, AI 를 활용한 능동 공격 감지 시스템 구축이 늘어나고 있다. 하지만 이러한 시스템의 도입은 너무 큰 컴퓨팅 자원과 비용을 요구한다. 한편, 많은 GUI 기반 로그 분석 소프트웨어는 실시간 분석을 보장하지 못하거나, 웹 로그에 대한 백업 기능을 제공하지 못한다. 또한 설치 과정이 복잡하고 인터페이스가 사용자 친화적이지 않은 경우가 많다.

2. Objectives

본 연구는, '쉽게 설치하여 사용 가능한 경량화 된 범용 로그 해석 도구' 개발을 목적으로 한다. 이는, 적은 컴퓨팅 자원을 소비하며, 적은 비용으로 운용할 수 있고, 실시간 분석을 보장하며, 웹 로그에 대한 안전한 백업 기능을 제공하며, 설치 과정이 간단하고, 인터페이스가 사용자 친화적인 웹 기반의 로그 분석 도구를 말한다.

3. Methods

Docker container 기반의 시스템을 구성한다. 본 소프트웨어는 사용자를 위한 인터페이스를 Next.js 와 React 로 구현하여 제공하며, 호스트 시스템에 리버스 프록시로 연결하여 사용하도록 설계되었다. 해당 서비스는 내부적으로 격리된 PHP-Apahce container 에 준비된 API 와 통신한다. API 는 본 시스템의 핵심 기능(로그의 분석을 통한 웹 공격 감지, 로그의 백업, 로그를 기반으로 한 AI 보안 보고서 작성 등.)을 제공한다.

4. Results

경량의 로컬 LLM 과 정규식에 기반한 로그 분석을 통해, 웹 공격을 능동적으로 감지하고 시각화 하여 제시하는 소프트웨어 개발이 완료되었다.

5. Conclusions

소규모 사업체 혹은 개인이 저비용으로 적용하여 사용 가능한 경량 로그 분석 툴의 배포를 통하여, 개인과 사회 차원에서 발생 가능한 보안사고를 최소화할 수 있을 것이다.

공격 징후를 탐지하는 정규식 세트를 개선할 예정이다. 추후 BERT 등의 언어모델을 통한 로그 분석 연구를 수용하여, 감지 정확도를 개선할 예정이다.

Keywords: lightweight log analysis; real-time log monitoring; regex-based attack detection; local LLM integration

References

[1] 박재연, 이송연, 이하은, 이종우. "리눅스 아파치 웹 서버 실시간 로그 분석을 통한 공격 탐지 프로그램 개발" 정보과학회 컴퓨팅의 실제 논문지. vol. 24, no. 4, pp. 190-197, 2018, doi: 10.5626/KTCP.2018.24.4.190

[2] 김점구. "웹 보안 모니터링을 위한로그 분석 시스템 설계 및 구현" 한국차세대컴퓨팅학회 논문지 12, no.3 (2016) : 105-111.