로그 기반 행위 이상 탐지 체계 아키텍처 설계

홍리나[1], 곽진[2]
[1]아주대학교 사이버보안학과 학부생
[2]아주대학교 사이버보안학과 교수

lina01@ajou.ac.kr, security@ajou.ac.kr

Architecture Design for Log-Based Behavioral Anomaly Detection System

Lina Hong[1], Jin Kwak[2]
[1]Dept. of Cyber Security, Ajou University
[2]Dept. of Cyber Security, Ajou University

요 약

본 연구는 리눅스 환경에서 오픈소스 기반의 행위 기반 로그 수집을 중심으로 보안 탐지 체계의 설계 방법론을 제시한다. Wazuh 와 ELK 스택을 연계하여 다계층 탐지 구조를 구성하고, Sigma 기반의 표준화된 룰 설계 및 적용 방안을 구체화한다.

1. 서론

권한 상승(privilege escalation) 단계는 공격자가 일반 사용자 권한을 탈취한 이후, 최고 관리자 권한(root)를 획득함으로서 시스템을 완전히 장악하는 치명적인 전술이다. MITRE 의 ATT&CK Framework 에서도 권한 상승은 주요 공격 전술(TA0004)로 분류되어있으며, 다양한 구현 기법들이 정리되어있다[1]. 이러한 권한 상승 시도를 초기에 탐지하기 위해서는 엔드포인트 보안 모니터링이 필수적이며, 시스템 로그를 활용한 행위 기반 탐지 기법은 비교적 적은 오버헤드로 효과적인 보안 통찰을 제공할 수 있다.

호스트 기반 침입탐지 시스템(HIDS)인 OSSEC 과 그 발전형인 Wazuh 는 리눅스 환경을 포함한 다양한 플랫폼의 이벤트 로그를 수집하고, 규칙 기반 탐지를 통해 이상행위를 식별하는 기능을 제공한다[2]. Wazuh 는 중앙 관리자(Server)와 각 호스트에 설치되는 에이전트로 구성되어 시스템 로그를 수집, 분석하고 정의된 룰에 따라 실시간 경고를 생성한다.

그러나 룰 기반 탐지는 탐지 규칙 설계 및 지속적인 유지 관리가 필수적이며, 최신 공격 기법을 반영하지 못할 경우 미탐지의 한계가 존재한다. 이러한 문제를 해결하기 위해, 탐지 룰의 표준화된 포맷인 Sigma 를 통해 SIEM 환경에 적용 가능한 탐지 규칙을 YAML 형식으로 기술하고 변환할 수 있는 프레임워크를 제공한다. 본 연구에서는 로그 기반 보안 탐지 체계를 구축하고, 탐지 룰 설계를 통해 다양한 공격 시나리오에 대응할 수 있는 방법론을 제시한다.

2. 로그 기반 탐지 체계 설계

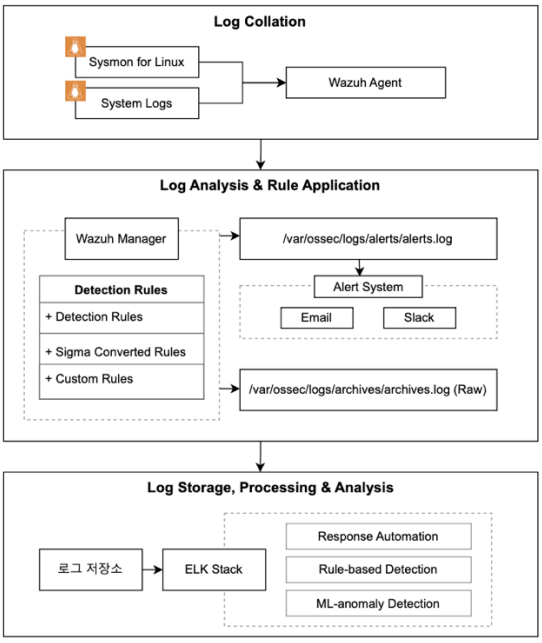
본 연구에서 구축하는 로그 기반 보안 탐지 체계는 Amazon Linux2 기반의 리눅스 엔드포인트 에이전트와 로그 수집/분석 서버로 구성된다. 리눅스 호스트에서는 Sysmon for Linux 와 Wazuh Agent 가 설치된다. Sysmon 은 마이크로소프트에서 제공하는 eBPF 기반 시스템 모니터링 도구로서, 프로세스 생성, 네트워크 연결, 파일 변경 등의 상세 이벤트를 커널 수준에서 포착하여 로그로 남긴다. 리눅스에서 기본적으로 생성되는 syslog 에서 탐지되기 어려운 세부 행위까지 기록함으로서, 공격자의 은밀한 행위도 로그로서 파악할 수 있도록 돕니다. Wazuh Agent 는 Sysmon 이 생성한 이벤트 로그 뿐만 아니라, auth.log 등의 운영체제 일반 로그도 수집하며, 이를 중앙의 Wazuh 관리 서버로 전송한다.

Wazuh 관리 서버는 수신한 로그를 사전에 정의된 탐지 룰과 대조하여 실시간으로 분석한다. 탐지 룰은 특정 프로세스 이름, 파일 경로, 시스템 호출 코드 등 로그 데이터의 패턴을 매칭하여 알려진 악성 행위를 식별한다. 예를 들어, 권한 상승 시나리오에서 일반 사용자가 sudo 명령을 반복적으로 실패하다가 성공하거나, setuid 비트가 설정된 비정상적인 바이너리 실행

등이 로그로 탐지될 경우 경고를 발생시키도록 규칙을 설정할 수 있다.

탐지 룰셋을 정의하는데 있어 Sigma 는 다양한 플랫폼에서 활용할 수 있도록 일반화되어있어, Wazuh 와 ELK 환경에 맞추어 변환하여 사용할 수 있다. 이를 통해 공격 기법에 대한 탐지 로직을 중복 작성할 필요없이 빠르게 룰을 작성하고 배포할 수 있으며, 룰 수정 및 유지보수 과정에서도 효율성을 확보할 수 있다.

또한 Wazuh 는 ELK Stack 과의 통합을 통해, 수집된 로그를 효율적으로 저장/조회할 수 있다. 본 연구에서는 Wazuh 의 기본 알람 기능 외에도 Kibana 대시보드를 활용하여 탐지된 이벤트를 시각화하고, 탐지 룰의 동작을 확인한다. 요약하면, **Sysmon** 은 풍부한 로그 데이터 제공을, **Wazuh** 는 실시간 분석과 경고를, **Sigma** 는 탐지 규칙 설계의 가이드를 담당함으로써 서로 보완적인 역할을 수행한다. 이러한 체계 설계를 통해 리눅스 엔드포인트에서 발생하는 권한 상승 공격의 징후를 놓치지 않고 탐지하는 것을 목표로 한다.



<그림 1> 로그 기반 탐지 체계 아키텍처

3. 로그 기반 탐지 룰 설계

각 시스템의 이벤트 로그를 수집하는 Wazuh Agent 는 Linux 환경에서 동작하는 Sysmon For Linux 와 auth.log, 커널 로그와 같은 시스템 로그를 모니터링하여 발생하는 보안 이벤트를 수집한다. 수집된 로그는 Wazuh Manager 로 전송되며, Wazuh Manager 의 내장된 OSSEC 기반의 경량 룰 엔진을 통해 실시간으로 로그를 분석한다. 이때, Sigma 룰을 Wazuh 의 XML 포맷으로 변환한 룰과 사용자 정의 룰을 함께 적용하여 의심스러운 행위를 식별한다. 이 1 차 분석 단계에서 탐지된 보안 이벤트는 경보(alert)로 생성되어 alerts.log 에 기록된다. 이 과정에서 Wazuh Manager 가 Agent 로 들어오는 로그 스트림을 실시간으로 처리하면서 알려진 위협 패턴이나 중대한 보안 이상징후를 즉시 탐지할 수 있도록 한다. 특히 악성 프로세스 실행, 커널 익스플로잇 징후 등 치명적인 영향이 예상되는 이벤트에 대해 경보를 발생시켜 즉각적인 대응을 시작할 수 있도록 한다.

한편, 모든 원시 로그는 archives.log 에 기록된다. 장기 보존, 심화 분석 및 로그 모니터링 성능 확보를 위해 별도의 로그 저장소에 전송된다. 일원화된 로그 데이터는 ELK 스택을 통한 상관관계 분석과 이상탐지에 활용된다. ELK 의 Detection Engine 을 통한 상관관계 분석, 지표 매칭, 사용자 정의 룰을 적용한다. 또한 EQL 을 활용한 이벤트 간 관계 탐지를 통해 다단계 공격 시나리오를 효과적으로 포착하고, 개별 시스템 수준에서 놓칠 수 있는 공격 흐름을 밝혀낼 수 있다. 또한 Elastic Threat Intelligence 와의 연동으로 악성 IP 및 해시 기반 위협 매칭도 지원한다. 이외에도 ML 기반 이상 탐지를 도입하여 비정상적인 행동 패턴을 자동으로 학습하고 이상치를 탐지할 수 있다. 로그인 시각, 프로세스 생성 패턴, 네트워크 활동 등의 베이스라인을 모델링하여, 규칙으로 정의되지 않은 새로운 유형의 위협도 포착할 수 있다. ML 탐지 결과는 점수화되어 대시보드로 시각화하고, 심각도가 높을 경우 추가 경보로 연동된다.

4. 결론

본 연구에서 설계한 로그 기반 보안 탐지 체계는 Defense in Depth 전략을 핵심 설계 원칙으로 삼아, 탐지의 누락 가능성을 최소화하고 대응의 신속성과 신뢰성을 동시에 확보하는 것을 목표로 한다. Wazuh Manager 을 통한 1 차 실시간 룰 기반 탐지와 ELK 스택에서 전송된 로그에 대한 2 차 상관관계 분석 및 머신러닝 기반 이상 탐지를 병행함으로써, 복합적인 공격 흐름이나 알려지지 않은 이상행위까지도 대응할 수 있도록 한다.

본 설계는 위협 탐지의 전 과정에서 계층적 대응과 심층 방어의 원리를 적용하여 고도화된 공격 시나리오 및 신종 위협에 대한 대응력을 확보하고, 탐지 공백의 가능성을 저감시켰다. 이러한 접근 방식을 통해 다변화된 현대 보안 위협 환경에서 효과적인 방어 체계를 구축하기 위한 실질적인 방법론으로 기능할 수 있음을 시사한다.

참고문헌

[1] MITRE ATT&CK Framework. "Privilege Escalation - Tactic TA0004," [Online]. Available: https://attack.mitre.org/tactics/TA0004/

[2] Wazuh Documentation. "Wazuh: The Open Source Security Platform," [Online]. Available: https://documentation.wazuh.com/