ELK Stack 과 Wazuh 통합 플랫폼 연구

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

guswls050728@ajou.ac.kr, security@ajou.ac.kr

A Study on the Integration of ELK Stack and Wazuh Platform

Hyun-Jin Kim[1], Jin Kwak[2]
[1]Dept. of Cyber Security, Ajou University
[2]Dept. of Cyber Security, Ajou University

요 약

본 논문에서 고도화되고 은밀해지는 사이버 공격에 효과적으로 대응하고자 다양한 EDR 솔루션들을 검토하였다. 그 중 ELK Stack 과 Wazuh 를 통합하여 사이버 공격에 탐지하고 대응하는 플랫폼을 제시하였다. 이를 위하여 각각의 특징과 장단점을 분석해보았으며, 연구 결과, 강력한 보안 모니터링 체계 및 자동화 대응이 가능한 플랫폼을 구축할 수 있음을 확인하였다.

1. 서론

최근 고도화되고 은밀해진 사이버 공격들 때문에 효과적으로 탐지하거나 방어하기 어려워지고 있다. 전통적인 보안 솔루션을 대부분 정해진 룰이나 플레이 북을 기반으로 동작하기 때문에, 알려진 패턴에는 어느 정도 대응할 수 있으나 새로운 기법을 사용하는 위협에는 매우 취약한 한계를 갖고 있다. 이를 해결하기 위해 다양한 연구가 진행되고 있지만, 강력한 보안 모니터링 기능을 제공하는 오픈 소스 솔루션인 Wazuh 에 대한 연구는 상대적으로 부족하다.

이에 본 논문에서는 Wazuh 와 ELK Stack 을 연동하여, 엔드포인트의 보안 이벤트를 효과적으로 수집, 분석, 시각화 할 수 있는 통합 EDR 플랫폼을 제안하고자 한다. 이를 통해 보다 향상된 탐지, 대응 체계를 마련하고, 운영 효율성을 높이는 것을 목표로 한다.

2. 본론

2.1. EDR (Endpoint Detection and Response)

EDR 이란, Endpoint Detection and Response 의 약자로, 엔드포인트 단말기에서 발생할 수 있는 Malware 나 Ransomware 와 같은 사이버 위협을 탐지하고 대응하기 위하여 지속적인 감시하는 기능을 제공하는 엔드포인트 솔루션이다. 현재 다양한 오픈 소스 EDR 솔루션이 존재하며, 본 논문에서는 대표적인 솔루션과 Wazuh 의 기능적 차이점과 장단점을 비교하고자 한다.

항목	OSSEC	Velociraptor	Wazuh
기능	기본 IDS 기능 중심	메모리/디스크 포렌식 특화	IDS + FIM + 취약점 진단 통합
확장성	낮음	중간	높음 (다양한 통합 지원)
사용 편의성	단순	복잡	보통 (Dashboard 제공)
커뮤니티/지원	적음	활발 (구글 주도)	활발 (공식 지원 + 커뮤니티)
설치/운영 난이도	쉬움	어려움	중간

<표 1> OSSEC, Velociraptor, Wazuh 비교

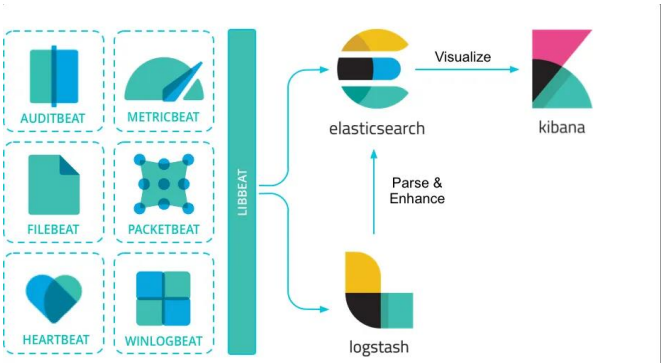
OSSEC 은 경량 IDS 로 설치와 운영이 간편하지만, 확장성이 낮고, 고급 분석 기능은 부족하다. Velociraptor 는 포렌식 분석에 강점을 가지나, 사용 및 운영 난이도가 높다. 반면 Wazuh 는 IDS, FIM, 취약점 탐지 등 다양한 기능을 통합 제공하면서도, Dashboard 를 통한 직관적인 운영이 가능하다. 이러한 비교를 통해, Wazuh 는 종합적인 보안 기능 제공과 운용 편의성 측면에서 타 오픈 소스 EDR 솔루션과 비교해도 뒤쳐지지 않는 EDR 솔루션임을 확인할 수 있다.

2.2. ELK Stack

ELK Stack 이란 Elasticsearch, Logstash, Kibana 을 통합하여 로그 수집, 문서 검색, 보안 정보 및 이벤트 관리(SIEM) 등 광범위하게 데이터를 수집 및 처리, 시각화를 해준다. Logstash 는 데이터를 수집 및 필터링(혹은 변환)을 통해서 원하는 형태로 가공한다. Elasticsearch 는 수집된 데이터를 인덱싱하고 분석하며, 검색하는 기능을 제공한다. Kibana 는 Elasticsearch 에서 인덱싱 되고 분석된 결과를 시각화를 통하여 보여준다. 본 연구에서는 Wazuh 로 수집 및 정제한 데이터

를 전달받아 분석 및 시각화 하는 역할이다.

(그림 2) ELK Stack 구상도



2.3. Wazuh

Wazuh 는 엔드포인트 및 서버의 보안 모니터링, 침입 탐지, 취약점 관리, 규정 준수 검증 등의 기능을 제공하는 통합 보안 플랫폼이다. 주요 기능으로는 로그 수집 및 분석, 침입 탐지, 파일 무결성 검사, 취약점 탐지, 규정 준수 모니터링, 그리고 자동화된 경고 시스템이 있다. 이러한 기능들을 통해 보다 효과적으로 사이버 위협에 대응할 수 있다.

구성요소로는 다음과 같다. Wazuh Agent 는 각 엔드포인트에 설치되어 로그 및 데이터를 수집 및 전달한다. Wazuh Manager 는 에이전트로부터 데이터를 받아서 분석하고, 경고를 생성한다. Wazuh Indexer 는 분석된 데이터를 저장하고 검색 및 인덱싱한다. Wazuh Dashboard 는 데이터를 시각화하고 사용자에게 보여주는 웹 인터페이스이다. 본 논문에서 각 엔드포인트에서 데이터를 수집하고 데이터를 분석 및 인덱싱하여 ELK 에 전달하는 역할을 한다.

(그림 2) Wazuh 의 주요 기능

Endpoint security	Threat intelligence	Security operations	Cloud security
Configuration assessment	Threat hunting	Incident response	Container security
Malware detection	Log data analysis	Regulatory compliance	Posture management
File integrity monitoring	Vulnerability detection	IT hygiene	Workload protection

2.4. ELK Stack, Wazuh 통합 플랫폼 제안

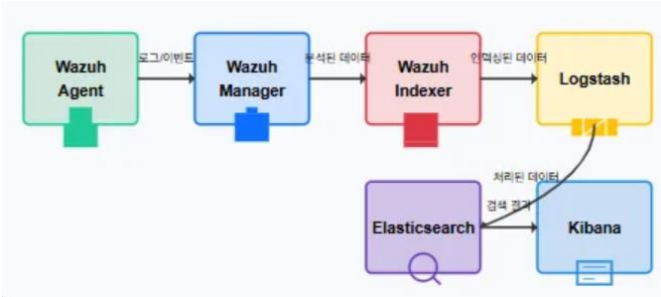
본 논문에서 엔드포인트 보안 모니터링과 로그 분석을 위한 통합 플랫폼으로 Wazuh 와 ELK Stack 을 결합한 아키텍처를 제안한다. 이 통합 모델은 Wazuh 의 강력한 보안 모니터링 기능과 ELK Stack 의 우수한 데이터 분석 및 시각화 기능을 결합하여 보다 효과적인 보안 관리 체계를 구축하는 것을 목표로 한다.

제안하는 플랫폼의 흐름은 다음과 같다.

1. Wazuh Agent: 각 엔드포인트에 설치되어 시스템 로그, 파일 무결성 정보, 보안 이벤트 등의 데이터를 수집하여 Wazuh Manger(Server)에게 전달한다.
2. Wazuh Manager: Agent 로부터 수집된 데이터를 중앙에서 수신하고 분석한다. 규칙 기반 분석을 통해 보안 위협을 탐지하고 경고를 생성한다. 위협 탐지를 하기 위한 좋은 모듈이 이미 다수 존재하기 때문에 이를 적극 활용하여 위협을 탐지한다. 또한 내가 원하는 패턴을 Wazuh Rule 로 작성하여 탐지가 가능하다.
3. Wazuh Indexer: 분석된 데이터를 인덱싱하고 저장하여 검색 가능한 형태로 유지한다.
4. Logstash: Wazuh Indexer 로부터 데이터를 수신하여 추가적인 필터링과 변환 작업을 수행 후 Elasticsearch 에게 전송한다.
5. Elasticsearch: 가공된 데이터를 검색 엔진에 저장하고 분석을 수행한다. Sigma Rule 을 통하여 원하는 패턴을 탐지할 수 있다.
6. Kibana: 최종 분석 결과를 다양한 대시보드와 시각화 도구를 통해 표현한다.

통합 시 고려해야 할 사항은 각 수집하는 데이터의 형태가 다를 수 있으니 데이터의 정규화 과정이 필요하다. 또한 대량의 보안 이벤트를 처리할 때 시스템 병목 현상을 방지하기 위한 자원 할당과 설정 최적화가 필요하다.

(그림 3) ELK + Wazuh 구상도



3. 결론

본 논문에서 Wazuh 와 ELK Stack 을 통합한 플랫폼을 구축할 수 있는 방안을 연구하였다. Wazuh 의 기본적인 기능과 모듈을 활용하고, ELK Stack 의 우수한 데이터 분석 및 시각화 기능을 결합함으로써, 단일 솔루션에 비해 더 향상된 탐지 및 대응 체계를 구축할 수 있음을 확인하였다. 본 통합 플랫폼을 통해 실시간 위협 모니터링, 효율적인 로그 분석, 시각적 관리가 가능해질 것으로 기대된다. 향후에는 머신러닝 기반 위협 탐지 기능을 추가하여 보다 지능적이고 자동화된 보안 체계로 확장할 수 있을 것이다.

참고문헌

[1] Elastic, "Elastic Stack Documentation," Elastic, 2024.
[2] Wazuh Inc., "Wazuh Documentation," Wazuh, 2024.
[3] CrowdStrike, "What is endpoint detection and response (EDR)?", 2023.
[4] Amazon Web Services, "ELK Stack 이란 무엇인가요?", AWS, 2023.
[5] Wazuh Inc., "Wazuh: The Open-Source Security Platform", 2023.
[6] "Introduction to the Elastic Stack", Elastic Stack Documentation, 2023.