사이버 위협 대응을 위한 효율적인 정보 수집 및 통신 아키텍처 구성 방안

김형래, 조병모, 김태규
LIG 넥스원

hyeongrae.kim@lignex1.com, byoungmo.cho@lignex1.com, taekyu.kim@lignex1.com

Efficient Information and Communication Architecture for Cyber Threat Response

Kim Hyeong Rae, Cho Byeong Mo, Kim Tae Kyu
LIGNex1

요 약

본 논문은 보안 정보 및 이벤트 관리(Security Information and Event Management, 이하 SIEM) 시스템의 표준 구조와 주요 기능에 대해서 살펴보고, 해당 구조에서 내제된 문제점과 이를 해결할 수 있는 시스템 구조 및 기법들에 대하여 서술한다.

Ⅰ. 서론

사이버 위협이 증가하면서 많은 보안 업체에서는 보안 정보와 이벤트 정보 관리를 통해 위협을 빠르게 탐지하여 대응할 수 있는 다양한 SIEM 제품과 이를 확장한 EDR(Endpoint Detection and Response) 제품들을 출시하여 서비스하고 있고, 다수의 분석 보고서를 통해 각 제품마다 고유의 특징들과 장단점들을 쉽게 확인할 수 있다[1]. 각 제품마다 특징이 다르고, 제품의 기술적 보안으로 인해 각 제품별 상세한 아키텍처들은 공개가 안되어있는 상황이지만, 많은 제품들의 공통적 특징들을 분석해 보면 표준적인 아키텍처를 유추할 수 있다. 본 논문에서는 보안 정보 및 이벤트 관리 시스템의 공통적인 특징을 분석하여 효율적인 계층 구조를 정의하고, 해당 시스템이 가지고 있는 고유의 문제점에 대해 서술한다. 그리고, 그러한 문제점들을 해결하기 위한 기법들을 제시한다.

Ⅱ. SIEM 시스템의 효율적인 계층 구조

많은 사이버 보안 선두 업체들은 전통적인 보안 정보 및 이벤트 정보 수집 분석을 기반으로 사용자의 행위 분석이나 지식 시스템과의 접목을 통해 사이버 위협에 대한 대응 시스템을 구축하여 제품을 서비스 하고 있다. 대부분의 업체들은 제품의 기밀 유지를 위해 상세한 아키텍처 구조와 서비스 구성을 공개하고 있지는 않지만, 알려진 정보들을 비교 분석해 보면 공통적인 구성 방안을 도출할 수 있다. 국내 대표적인 보안 업체에서 공개한 보안 관제 시스템 구성과 비교해보면 효율적인 정보 수집 및 관리 시스템 구조에 대한 대략적인 아키텍처 구조를 유추해볼 수 있다[2]. 효율적인 SIEM 구조와 각 계층별 주요 서비스들에 대한 내용을 요약해보면 그림 1 과 같이 기술할 수 있다.

그림 1 SIEM 의 일반적인 계층 구조 및 기능

가장 하단의 수집 계층은 방화벽, 라우터 등의 각종 IPS 장비나 네트워크 장비로부터 생성되는 로그 정보를 수집하는 영역이다. 로그의 출처는 장비뿐 만이 아니라 OS 에서 생성하는 syslog 나 응용 프로그램의 로그 등이 모두 포함된다. 이러한 로그들은 데이터의 출처가 매우 다양하기 때문에 일괄된 형태의 데이터로 재구성해주는 과정이 필요하다. 일반적으로 데이터를 한 저장영역으로 모아주는 역할을 하는 기능이 수집 계층에 포함되어 있고, 수집된 데이터를 효율적으로 사용하기 위해 정형화 또는 색인 작업을 하는 기능들이 함께 위치하고 있다.

수집 계층에서 저장된 데이터는 위협 대응을 위한 의미 있는 정보 추출을 위한 작업의 입력으로 사용되고 이러한 작업이 일어나는 곳을 분석 계층이라고 한다. 분석 계층에서는 정형화된 로그 데이터로부터 특정한

패턴을 찾아내던가 예외적인 상황에 대한 설정을 기준으로 삼아 정상적이지 않는 이상 행위에 대한 탐지 및 분석을 수행한다. 이때 이루어지는 탐지 및 분석은 사용자가 로그를 직접 분석하여 수행하는 경우는 거의 없고 규격화된 룰을 정의하거나 수치화된 지표를 미리 설정해두어 해당 사례가 발생하였을 때 자동으로 경보를 발생하는 방식으로 분석이 이루어진다.

수집 계층과 분석 계층이 자동화 서비스와 관련된 영역이라면 관제 관점에서 분석가 혹은 관리자가 서비스를 직접 사용하는 영역이 필요하다. 이러한 영역을 응용 계층이라고 한다. 응용 계층은 조직의 관제 대상 시스템 영역을 모니터링하며 로그를 발생하는 장비 및 자산의 상태를 확인하고, 분석 계층에서 생성하는 위협의 징후나 경보를 실시간으로 확인할 수 있는 시각적 시스템인 상황도가 가장 대표적인 예라고 할 수 있다. 또한, 분석 계층에서 사용하는 로그 분석에 대한 룰이나 경보 발생에 대한 규칙을 설정하고, 특별한 경우에는 로그 정보를 직접 분석하여 위협 대응을 하기도 한다. 이러한 작업에 필요한 다양한 기능 및 도구들이 응용 계층에서 사용자 편의성 측면에서 많이 제공되고 활용된다.

Ⅲ. SIEM 시스템의 문제점 및 대응 방안

계층화된 보안 정보 및 이벤트 관리 시스템 구조는 명확한 역할 구분에 따른 서비스 배치를 유용하게 하여 관리 및 운용 측면에서 효율적인 아키텍처를 구성할 수 있다. 하지만, SIEM 환경에서는 다양한 정보 출처에서 만들어진 로그 정보가 분석 과정을 통해 관리자에게 결과로 전달되는 과정 동안 여러 단계의 정보 가공 및 정보 처리가 수반되기 때문에 위협 행위에 해당하는 이벤트 발생 시점과 위협의 인지 시점 사이의 시간차가 발생할 수 밖에 없다. 예를 들어, 악의 적인 정보 탈취를 위해 통신 경로를 생성하고 내부 자료를 외부로 빼돌리는 작업이 발생할 경우, 통신 연결에 대한 로그와 전송된 데이터에 대한 확인 과정은 사건이 발생한 후에 분석 과정을 통해 파악이 될 수 밖에 없다. 이러한 원인은 많은 수의 장비에서 발생하는 로그 정보를 실시간으로 모니터링하는 구조의 수집 계층 구현은 SIEM 환경이 운용 장비에 많은 성능적인 부담을 주기 때문에 대부분의 경우에는 주기적으로 일정 시간 동안 정보를 모은 후 일괄적으로 수집 데이터를 중앙 집중 형태의 정보 저장소로 전달하는 방식을 적용하고 있다.

이러한 구조적인 한계점으로 인해 SIEM 시스템은 완벽한 실시간성을 보장하지 못하고, 대신 사례 분석 과정을 통해 취약점 확인 및 예방 대응 관점에서 많이 활용된다. 이러한 문제점을 보완하기 위해서는 두 가지 측면에서 제약사항을 극복해야 한다. 우선은 이벤트 발생 시점에서부터 경보 생성까지의 소요 시간 최소화이다. 이벤트 발생에서부터 탐지까지의 평균 진단 시간을 최소화하기 위해 많은 제품들이 자동화 기법을 도입하고 탐색 엔진을 고도화 하고 있다. Elastic search 와 같은 빅데이터 기반의 데이터 처리 엔진이 널리 알려짐에 따라 로그 데이터를 장비 내에서 로컬 캐싱을 통해 저장 후 주기적 전송 방식을 택하기 보다는 로그 데이터 발생 즉시 데이터를 저장소로 전달하여 수집에 소요되는 시간을 최소화 할 수 있다.

소요 시간 최소화 관점에서는 고도화된 데이터 수집 및 검색 엔진을 활용하여 해결할 수 있지만, 데이터의 집중과 대규모 자료 저장에 대한 시스템 부담은 근본적으로 해결하기가 쉽지 않다. 그러한 문제점을 해결하기 위한 방법은 수집된 데이터를 정제하여 데이터 저장소로 전달되는 분량을 줄이는 방법이 가장 효과적이다. 데이터의 양을 줄이는 방법에는 여러 기술들이 적용될 수 있지만, 가장 대중적이고 쉽게 구현 가능한 방법은 중복되는 데이터 식별을 통한 선택적 전송 및 필터링이다. 일차적으로 데이터를 수집하는 영역에서 반복되는 이벤트 로그를 필터링하여 중복성을 제거하거나, 주기적인 상태 정보에 대해 모든 데이터를 전송하는 것이 아닌 단계별 상태 정보 비교를 통해 차이가 나는 부분에 대해서만 선택적 정규화를 적용하여 수집 데이터의 양을 최소화할 수 있다. 이러한 접근 방식은 유사한 장비 종류에 공통으로 적용하였을 때 비교적 높은 효율을 얻어낼 수 있다.

Ⅳ. 결론

본 논문에서는 SIEM 시스템이 효율적으로 구성될 수 있는 아키텍처와 각 계층에서의 핵심 기능에 대하여 살펴보았다. 그리고, SIEM 시스템이 가지고 있는 구조적 문제점과 이를 해결하기 위한 해결 방안에 대하여 기술하였다. 본 논문에서 언급된 문제 외에도 보다 정밀한 사이버 위협 대응에 필요한 많은 필수 기술요소들이 산적해 있지만, 가장 중요한 부분에 대한 이슈만 우선적으로 정리하였다. 현재에도 많은 연구가 진행되고 있지만, 단순한 로그나 이벤트 정보만을 기반으로 위협에 대응하기 보다는 사용자의 행위 분석을 반영하거나 지식정보 시스템과 연계한 보다 고도화된 서비스들이 지속적으로 시중에 출시되고 있기 때문에 관련 기술의 흐름을 지속적으로 살펴보고 SIEM 시스템을 개선해 나가는데 지속적으로 관심을 두어야 할 필요성이 있다.

참 고 문 헌

[1] 한국침해사고대응팀협의회, 한국 CPO 포럼, "Security Consumer Report," 2019.

[2] 한국 IBM, "IBM 보안 프레임워크로 본 보안 간편화 전략," 2014.

(http://www-903.ibm.com/swgmkt/sec/Sec2014_01.pdf)