사이버보안을 위한 SIEM 의 발전 동향

김종욱*, 방지원*, 최미정*
*강원대학교 컴퓨터과학과
e-mail : {goldbear564,jiwonbang, mjchoi}@kangwon.ac.kr

Development Trend of SIEM for Cyber Security

Jong-Wouk Kim*, Jiwon Bang*, Mi-Jung Choi
*Dept. of Computer Science, Kang-Won National University

요 약

과학기술, 정보통신과 같은 기술들이 발전함에 따라 혁신적인 기술들 또한 대거 등장하였다. 이러한 기술들을 기반으로 새로운 서비스들이 등장하여 사람들의 삶의 질 또한 꾸준히 향상되고 있다. 그러나 기술발전 이면에는 해킹, 바이러스, 취약점 공격과 같은 역기능들의 기술 또한 지속해서 발전하고 있다. 공격자들은 이러한 기술들을 이용하여 정보자산의 침해, 사이버 테러, 금전적인 피해와 같은 사회 문제를 꾸준히 일으키고 있으며, 기업적으로는 개인정보 유출 및 산업 기밀 유출과 같은 정보보안 사고 또한 꾸준히 발생하고 있다. 이와 같은 이유로 SIEM(Security Information & Event Management)은 24 시간 365 일 네트워크와 시스템에 대한 지속적인 모니터링을 통해 외부로부터의 침입이나 각종 바이러스 등에 대해 적절한 대책을 통해 고객의 자산을 보호한다. 따라서 본 논문에서는 과거에서부터 현재까지의 내부 네트워크 기술의 발전을 살펴본 후 정보보안 사고 및 이상징후 탐지를 위한 통합 보안시스템 로그 관리 솔루션인 SIEM 의 시대적 변화와 솔루션 동향에 대해 살펴보고자 한다.

1. 서론[1]

IT 기술이 발전함에 따라 모바일, 은행, 등 많은 분야에서 사용되어 사람들의 편의성이 증가하였다. 하지만 현재 국가 간 사이버 전쟁, 금전, 정보 유출 등을 목적으로 한 사이버 공간에서의 침해 및 피해 또한 꾸준히 증가하고 있다. 지속적인 사이버 공격에 대응하기 위하여 빅데이터 분석 기술을 활용한 SIEM(Security Information & Event Management) 솔루션[1]이 활용되고 있으며 이러한 상황을 반영하듯이 NIST 는 Cybersecurity Framework 문서를 공개하고 지속적으로 개정을 진행하고 있다[2,3].

과거에는 장애 처리 모니터링을 위해 로그를 단순하게 저장 및 관리를 하였다. SEM(Security Event Management)과 ESM(Enterprise Security Event Management)이 개발됨에 따라 단순 로그 저장에서 저장된 로그를 활용하기 시작하였다. ESM 은 보안솔루션 및 네트워크 장비들의 로그를 받아 상호 연관 관계를 파악하는 솔루션이다. 그러나 수개월 정도의 데이터만 저장할 수 있고, 관리되는 데이터에 대한 다양한 조건 검색이 불가능하다[4]. 로그 분석에 대한 기술이 발전함으로써 다양한 이기종 간 로그의 상관분석을 위한 대용량 처리 시스템 SIEM 이 등장하였다. SIEM 의 기능으로는 알려지지 않은 보안 위협 분석 및 실시간 모니터링을 통한 이상징후 탐지가 가능하고, 중요 정보 및 자산 유출 모니터링 또한 가능하다는 특징을 갖고있다.

그래서 본 논문의 2 장에서는 세대별 보안을 살펴본 후, 3 장에서는 SIEM 에 대한 설명과 진화에 대해 설명하였으며, 4 장에서는 SIEM 의 솔루션 동향을 살펴본 후 5 장에서는 SIEM 이 가능한 역량과 앞으로의 전망에 대해 간단히 소개한다.

2. 세대별 보안 동향

1 세대의 네트워크 보안 기술은 방화벽, IDS(Intrusion Detection System), 트랜잭션 보안, QoS(Quality of Service) 등이 있다. 이 시기에는 서버와 인터넷 사이에서 트래픽을 필터링하여 로컬 보안정책 및 인증된 트래픽만 통과를 허용하는 방화벽(Firewall), 시스템과 네트워크에서 데이터를 수집해 시스템의 침입이나 오용 사실을 탐지하는 IDS 가 있었다. 1 세대는 초급 단계의 보안에 대한 필수적인 요소 중 하나이다. 그러나 내부자를 위한 우회 서비스로 접근이 가능하며 허용된 룰의 경우에는 방어가 불가능하다는 단점이 있다.

2 세대 내부 네트워크 보안 기술은 IPS(Intrusion Prevention System), 스팸 차단 시스템 등으로 1 세대 솔루션의 기능 및 성능을 개선된 기술이 등장하였다. 대표적인 기술로는 IPS 가 있다. IPS 는 네트워크 방화벽 구성과 동일하게 모든 트래픽이 해당 보안장비를 거쳐야만 목적지로 전송될 수 있는 In-Line 방식의 트

[1] 본 연구는 한국전력공사의 2018 년 착수 에너지 거점대학 클러스터 사업에 의해 지원되었음 (과제번호:R18XA05)

래픽 방어 시스템이다. 하지만 IPS 는 패턴 매칭 방식을 사용하기 때문에 새로운 취약점을 이용한 Zero-Day 공격 발생 시 탐지를 하지 못하거나 오탐을 하는 경우도 발생하였다.

3 세대 내부 네트워크 보안 기술은 웹 방화벽(WAF, Web Application Firewall), 통합보안 시스템(UTM, Unified Threat Management), 통합보안관제(ESM), 위협관리시스템(TMS, Threat Management System), DB 접근/권한 차단 솔루션, DDoS 차단 솔루션 등 많은 기술들이 개발되었다. 통합보안관제는 설치된 보안 장비를 단일 보안 관리 시스템으로 통합하였으며 이를 통해 단일 보안관리체계가 가능해져 통일된 보안 정책을 수립할 수 있게 되었다. 통합보안시스템은 IPS, IDS, VPN, Anti-Virus 등의 기능들이 하나로 결합한 시스템으로 바이러스, 웜(Warm), 트로이 목마(Trojan) 등의 악성코드와 네트워크 공격을 종합적으로 처리해주는 시스템이다[5].

4 세대 내부 네트워크 보안 기술은 어플리케이션 침입차단시스템, 보안 감사용 솔루션, 악성코드 유포지 차단, APT 솔루션, 좀비 탐지 및 차단 시스템 등이 생겼다. 이 시기에는 시그니처 기반만으로는 충분치 않다는 인식이 생기는 시기다. 그 때문에 알려지지 않은 공격 및 Zero-Day 공격을 방어하기 위한 안티-봇 및 샌드박싱 기술 또한 생겨났다. 그러나 이로 인해 보안 인프라가 하나로 통합되지 못하여 더욱 복잡해지는 문제점 또한 발생하였다.

3. SIEM 의 발전

현재의 사이버 위협은 파악조차 힘들고 정교한 공격이 진행됨으로써 기존의 보안 시스템으로는 탐지하기가 어렵다. 이런 공격을 탐지하기 위해 보안 업계는 빅데이터 기술을 접목하는 노력을 기울이고 있다[6]. SIEM 은 빅데이터 기술과 융합하여 모든 IT 시스템에서 생성되는 로그와 이벤트를 통합 관리해 외부 위협을 사전에 예측하고, 내부 정보 유출을 방지하는 솔루션이다. 빅데이터 이전의 통합 로그 관리는 주로 로그 관리 시스템 또는 ESM 을 활용하였다. 그러나 빅데이터 시대가 열리면서 이벤트 위주의 단시간 위협 분석 기반이었던 ESM 이 빅데이터 수준의 장시간 심층 분석 기반인 SIEM 이 2005 년 Gartner 에 의해 정의가 되었다[1].

SIEM 은 네트워크 및 시스템 이벤트와 실시간 분석을 결합하여 사고 대응을 하는 SEM(Security Event Management)과 장기간 로그 파일의 저장, 기록 분석 및 보고 활동을 제공하는 SIM(Security Information Management)이 결합된 솔루션이다[5,7,8]. 이러한 기능은 빅데이터 기술과의 융합으로 대량의 로그를 관리하여 외부 및 내부의 위협을 탐지할 수 있도록 도와준다. SIEM 은 네트워크의 경계부터 최종 사용자까지 전체 범위에 있는 네트워크 장비 및 보안 장비들의 로그를 수집, 저장 및 분석을 할 수 있는 효율적인 통합 로그 관리 기능, 사고 대응 및 포렌식, 알려진 위협 및 알려지지 않은 위협 탐지와 실시간 모니터링 기능, 내부자 위협에 대한 대응이 가능하다[9]. 그뿐만 아니라, 종합적인 보안 보고 및 규제 준수 관리가 용이하며 장기적 분석 및 실시간 보고 기능을 통해 조직 및 기업의 자산을 지켜내는데 큰 역할을 하는 솔루션이다.

1) SIEM 1.0

SIEM 1.0 솔루션은 오직 보안에만 초점을 두고 설계되었다. 현재의 SIEM 솔루션과는 달리 고급 이벤트만 집중하였기 때문에, SIEM 1.0 에서는 운영 및 규정 준수와 감사 사례와 같은 보안 이외의 용도로 사용되지 않았다. SIEM 1.0 은 많은 데이터 축소가 있었기 때문에 중요한 데이터들이 손실되었다. 이화 같은 이유로 포렌식에 사용될 데이터들 또한 손실되었으며 자산 및 네트워크 흐름 데이터와 같은 다른 중요한 상황 별 데이터 요소는 수집하지 않았다. 이런 제한된 데이터들을 기반으로 분석된 상관관계 분석의 결과는 정확하지 않기 때문에 실제 위협에 대응 및 탐지에는 적합하지 않았다. SIEM 1.0 은 이러한 문제와 높은 비용이 요구되었기 때문에 활용이 되지 못하였다. 그렇기에 고도화된 위협의 탐지 및 대응, 분석을 위해 다음 세대 SIEM 의 필요성을 느끼게 되었다.

2) SIEM 2.0

SIEM 2.0 은 단순한 보안 데이터 및 데이터 축소보다 더 광범위한 목적에 초점을 두고 맞추었다. 기존의 SIEM 1.0 보다 더 많은 데이터를 사용하였다. 네트워크 트래픽 및 호스트의 데이터, Application 계층과 같이 더 많은 곳에서 데이터를 수집하고 활용하는 방향으로 발전하였다. 이러한 정보들을 토대로 포렌식과 자동화된 규정 준수가 가능해졌으며, 가장 핵심적인 기능인 상관관계 분석 기능 또한 더욱 강력해졌다. 또한, 네트워크에서 활동하는 정보들을 수집하여 네트워크 계층의 위험 및 위협에 대한 정보 또한 확인이 가능하게 되었다. 사용되는 데이터의 범위가 응용계층까지 넓어짐에 따라 호스트의 취약점과 위험 수준까지 파악이 가능해졌으며, 데이터의 흐름을 파악하여 어디서 데이터가 유출되었는지 파악할 수 있고, 내부 위협 또한 탐지가 가능해졌다.

3) SIEM 3.0

SIEM 3.0[10]은 방화벽 및 취약성 관리(Vulnerability Management)과 같은 다른 사이버 보안 관리 플랫폼 간의 양방향 통신이 가능하게 되어 각 플랫폼의 효율성이 향상되었다. 또한 SIEM 을 활용하여 네트워크 성능 모니터링과 사용자 행위 분석을 통해 디지털 포렌식 과정에서 사용되는 증거의 유형을 지표화 한 IOC(Indicators of Compromise)를 찾을 수 있다. 이는 침해 지표로 디지털 침해 사고를 분석하는데 사용된다.

SIEM 엔진은 솔루션 자체가 아닌 SIEM 이 가능한 기능들을 따로 판매가 되는 추세이다. 성능 면에서는 초당 이벤트 수, 로그/데이터/Application 소스의 수, 준수 보고서, Dash Board 및 사용자 행위 분석의 강도와 같은 여러 사항에 따라 고객에게 제공이 된다. 또한 자동화된 프로세스 중 최종 사용자, 사용된 소프트웨어, IP 주소, 트래픽과 프로토콜 등을 사용한 상황

별 인식 또한 가능해졌다.

4. SIEM 솔루션의 동향

앞서 SIEM 은 보안 위험 및 위협의 탐지 그리고 규정에 대한 관리가 가능하다고 설명하였다. 그리고 사이버 보안 패러다임은 예방에서 탐지 중심으로 전환이 되었다[1]. 때문에 SIEM 의 위협 탐지 기능은 기업에 있어서 훨씬 더 가치가 높아졌다. 그러나 SIEM 의 미래는 앞으로도 이러한 내·외부에서의 위협을 탐지하여 대응에 초점을 맞출지, 아니면 규정 준수 및 규정 감사를 지키는 것에 초점을 맞추느냐에 따라 변화가 진행될 것으로 보인다. 과거 EU 의 GDPR 의 시행으로 인한 기업의 어려움이 있었으며, 캘리포니아 소비자 개인 정보 보호법(California Consumer Privacy Act 2018)이 통과되며 미국의 GDPR 에 의해 또 한 번 기업의 혼란을 고려한다면 기업들은 다시 한번 SIEM 의 규정 준수 및 감사 기능에 의존하게 될 전망으로 보인다.

(그림 1) 2017 Gartner Magic Quadrant for SIEM

(그림 1)은 2017 년 Gartner 보고서[11]에서 제공된 상위 18 개의 SIEM 솔루션을 개발한 업체들이 있으며 이에 대한 장단점들을 세부적으로 설명하고 있다. 위 그림의 'LEADERS'는 일반적으로 시장의 요구사항과 기능이 가장 많이 일치하는 제품을 제공하는 회사들이며, 새로운 요구 사항들에 대한 뛰어난 비전과 실행 증거를 제시하는 업체들이다. 'CHALLENGERS'는 최소 규모의 SIEM 고객들을 가지고 있으며 일반 시장 요구 사항의 하위 집합을 충족하는 제품을 제공하는 업체로 구성된다. 'VISONARIES'는 SIEM 시장의 요구사항과 강력한 기능을 제공하지만 'LEADERS'보다는 다소 떨어지는 기능을 탑재한 업체들의 집합 군이다. 'NICHE PLAYERS'는 특정 SIEM 의 사용 사례 또는 SIEM 기능 요구사항의 하위 집합과 잘 일치하는 SIEM 기능을 제공하는 업체들로 구성된다. 그리고 많은 새로운 벤더들이 UEBA(User and Entity Behavior Analysis)에 중점을 둔 제품에 SIEM 을 추가했다고 언급했으며, 이는 사용자, 장비, 소프트웨어 등의 이상 행동을 문맥 분석(Context Analysis) 수준에서 파악함으로써 보안 위협을 탐지하는 것이다. 이 UEBA 를 통한 사이버 보안을 제공하는 회사 또는 솔루션은 HPE, IBM, Splunk, LogRhythm 등이 있으며, 이러한 새로운 접근 방식 때문에 SIEM 시장이 다시 한번 바뀔 수 있다고 언급했다.

5. 결론

최근에는 보다 많은 기관과 기업들이 해커들의 표적이 되고 있으며, 많은 보안 사고가 발생함에 따라 SIEM 에 대한 많은 관심이 다시 집중되고 다양한 연구들과 솔루션들이 출시되고 있다. 따라서 본 논문에서는 지금까지 SIEM 의 동향과 앞으로 SIEM 의 가능성과 동향을 소개하였다. SIEM 은 네트워크 내의 다양한 이기종들의 로그 및 상태를 수집하여 상관관계 분석을 통해 내·외부로부터의 공격 또는 침입을 탐지할 수 있다. 또한, 필요한 정보들을 확인할 수 있는 보고서 또한 생성하여 기업의 네트워크의 상태와 사용 현황의 파악과 규정 준수와 감사를 할 수 있다. 그러므로 앞으로의 SIEM 은 기업 및 조직이 원하는 방향이 보안이라면 보안에 특화된 SIEM 을 사용하고 규정 준수 및 규정 감사라면 규정 준수 및 규정 감사에 특화된 SIEM 을 사용하게 될 것으로 예상된다. 또한 현재 SIEM 은 온프레미스(On-Premise)로 제공되지만, 앞으로 SaaS(Software as a Service) 또는 클라우드 방식이 도입되어 하이브리드 IT 인프라가 사용될 것으로 예상되는 바이다.

참고문헌

[1] Williams Amrit, "Improve IT Security With Vulnerability Management", Gartner

[2] NIST, "Framework for Improving Critical Infrastructure Cybersecurity", National Institute of Standards and Technology

[3] 차병래 최명수, 강은주, 박선, 김종원, "Cybersecurity 를 위한 SOC & SIEM 기술의 동향", 스마트미디어저널

[4] 한기형, 정형종, 이두식, 채명희, 윤철희, 노규성, "빅데이터 플랫폼을 이용한 보안로그 분석 시스템 구현 모델 연구", 한국디지털정책학회

[5] 김봉현, 조동욱, "네트워크 보안 기술 동향과 전망", 한국통신학회지

[6] 김동한, "빅데이터 환경에서 지능형 로그 관리 플랫폼으로 진화하는 보안 정보/이벤트 관리(SIEM) 동향", 정보통신잔업진흥원

[7] 심재화, 김성환, 정태명, "보안 정보/이벤트 관리(SIEM)를 이용한 국내외 솔루션 동향 연구", 한국통신학회

[8] Cesario Di Sarno, Alessia Garofalo, Ilaria Matteucci, Marco Vallini, "A novel security information and event management system for enhancing cyber security in a

hydroelectric dam", International Journal of Critical Infrastructure Protection
[9] 김종현, 임선희, 김익균, 조현숙, 노병규, "빅데이터를 활용한 사이버 보안 기술 동향", 한국전자통신연구원
[10] Christopher Kissel, "Security and Information Event Management(SIEM) The transition to SIEM 3.0", FireEye
[11] Kelly M. Kavanagh, Toby Bussa 외 1 명, "Magic Quadrant for Security Information and Event Management", Gartner