정 보 보 호 학 회 지
제23권 제6호, 2013. 12

통합로그관리시스템의 기술 동향과 발전 방향

유 기 순*, 임 설 화**, 김 학 범***

요 약

최근 급증하고 있는 고도화된 사이버 공격은 많은 피해를 낳고 있다. 이러한 문제를 미연에 방지하기 위해 각종 보안 솔루션의 도입으로 보안 시스템 환경이 복잡하게 변하게 되었다. 보안 관리자는 복잡한 환경으로 인해 보안 시스템 관리의 어려움으로 우수한 보안 솔루션이 있음에도 위협에 제대로 대처하지 못하고 있다. 본 논문에서는 보안 시스템을 체계적으로 관리할 수 있고, IT 시스템에서 생성되는 이벤트와 로그를 통합해 늘어나고 있는 보안 위협에 적절한 대응이 가능하도록 도와주는 보안 시스템 관리 솔루션인 SIEM(Security Information and Event Management)에 대해 알아보고자 한다. 고도화되고 있는 사이버 공격과 복잡해진 클라우드 컴퓨팅, 데이터가 대량화됨에 따라 생겨난 빅데이터, 갈수록 강화되고 있는 컴플라이언스 요구사항을 만족할 수 있는 방안을 모색해봄으로써 SIEM이 앞으로 나아가야 할 방향에 대해 알아보고자 한다.

Ⅰ. 서 론

기업의 IT 환경은 업무 개선이나 새로운 업무를 위해 네트워크, 스토리지, 서버 장비들을 새롭게 추가도입하면서 확장된다. 또한 기존 장비들은 업무를 처리하는데 있어서 성능이 떨어질 경우 다른 업무에 사용되거나 폐기된다. 이러한 과정을 거치면서 복잡해진 IT 인프라의 구성으로 인해 제대로 관리되지 않는 장비가 생겨나게 되고, 업무간 연계가 원활하게 이루어지지 않아 운영되지 않는 장비도 생겨난다.

보안 시스템의 경우 이와 같은 현상이 더욱 두드러지게 나타나는데, 다양해진 사이버 위협만큼 도입되는 보안 솔루션의 종류 역시 증가하게 되어 복잡한 보안 시스템 환경을 구축하게 된다. 이렇게 만들어진 환경은 보안 관리자에게 너무 많은 경고를 전달하여 실제 위협을 판단하기 힘든 상황을 초래한다.

이러한 문제를 해결하기 위해 보안 시스템 관리가 필요하다. 로그는 시스템 및 네트워크에서 발생하는 사용자의 악의적인 활동이나 외부의 공격으로 의심되는 이벤트와 관련된 다양한 정보를 가지고 있어 효율적인 보안 시스템 관리 체계를 구축하는데 도움이 된다[1]. 이렇게 구축된 보안 시스템 관리 체계는 비용효율적인 보안 시스템을 구현하고, 보안 수준이 향상 될 수 있는 핵심 요소이다. 갈수록 강화되고 있는 컴플라이언스 이슈 역시 보안 시스템 관리의 중요성을 높인다. 정보보안 관련 의무규정이 증가하면서 기업은 내부 보안 상황을 보다 분명하게 살펴야할 필요성이 생겼으며, 중앙 집중적으로 보안 상황을 보여주고, 리포팅해 줄 수 있는 보안 시스템 관리가 필요하게 되었다.

〔표 1〕 SIEM 세계시장 전망[3]

	2009	2010	2011	2012	2013	2014	2015	2016	2011-2016 CAGR (%)
Security management									
Security intelligence and event management	826.5	1,052.3	1,302.0	1,483.0	1,686.3	1,891.1	2,065.0	2,226.0	11.3
Proactive endpoint risk management	378.5	425.1	471.0	500.3	532.9	572.7	616.5	652.6	6.7
Forensics and incident investigation	136.6	188.7	221.0	296.1	356.3	422.8	488.9	553.6	20.2
Policy and compliance	587.6	694.2	800.5	897.7	994.9	1,082.1	1,162.8	1,172.4	7.9
Security device systems management	273.7	254.5	201.4	214.0	227.9	244.9	263.6	279.1	6.7
Subtotal	2,202.9	2,614.7	2,995.9	3,391.1	3,798.4	4,213.6	4,596.8	4,883.6	10.3

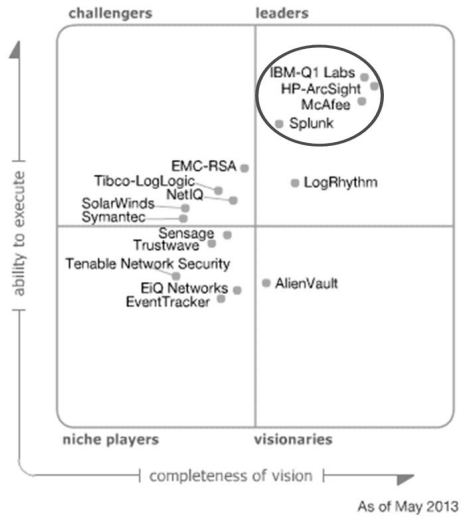
* 동국대학교 국제정보 대학원 (yugisun13@gmail.com)
* 동국대학교 국제정보 대학원 (sulhwa.im@gmail.com)
*** 동국대학교 국제정보 대학원 / (주)이너버스 (khb305@innerbus.com)

SIEM은 방화벽이나 IDS/IPS, 안티바이러스 등의 보안장비와 서버, 네트워크 장비 등으로부터 로그 및 이벤트를 수집 통합하여[2] 이들 간의 연관 분석을 통해 보안 상황을 인지하고, 신속한 사건 대응을 할 수 있도록 도와주며 로그관리 기능을 제공한다. 앞서 서술 하였듯이, IT 및 보안 시스템 환경이 복잡해지면서 로그 및 이벤트 관리 솔루션은 조직 내의 보안 인프라에서 필수 요소로 부상하고 있다[4]. SIEM은 로그의 효율적인 통합관리, 위험탐지, 사고대응, 포렌식과 보안과 관련된 컴플라이언스에 중요한 역할을 담당할 것으로 여겨진다.

[표 1]에서 보이는 것과 같이 전 세계 SIEM 분야는 2016년 까지 연평균 성장률 10.3%로 49억 불까지 지속적으로 성장할 것으로 보인다. SIEM 제품군 단독 시장은 연평균 성장률 11.3%로 23억 불까지 성장 할 것으로 예측되고 있다[5].

보안 시스템 관리 솔루션으로는 보안 장비가 생성하는 로그를 분석하는 전사적보안관리(ESM), 각종 위협정보를 분석하는 위협관리시스템(TMS), 보유자산과 연계성을 고려해 취약점을 관리하는 위험관리시스템(RMS), 그리고 모든 IT 시스템이 생성하는 로그를 분석해 보안위협을 탐지하는 보안정보이벤트관리(SIEM) 등이 있다.

본 논문에서는 통합로그관리시스템인 SIEM의 기술 개요, 국내외 업체별 SIEM 제품을 확인하고 제품들 중 가트너에서 발행한 Magic Quadrant for Security Information and Event Management에서 리더로 뽑힌 HP의 ArcSight, IBM의 Qradar, McAfee와 Splunk를 좀 더 상세히 살펴 본 후 제품별 특징을 비교, SIEM 취약점에 대해 논의한 후 향후 개선되어야 할 사항을 살펴보고자 한다.



[그림 1] Magic Quadrant for Security Information and Event Management[6]

Ⅱ. 통합로그관리시스템 기술 개요

2.1 통합로그관리시스템 기능[1]

통합로그관리시스템의 경우 저장, 분석, 로그 삭제 등의 기능을 수행하며 다음과 같은 기능을 포함한다.

일반적인 로그 관리 기능으로는 로그파싱, 이벤트 필터링, 이벤트 통합이 있다. 로그파싱은 다른 로깅 프로세스에서 사용할 수 있도록 로그에서 특정 데이터를 추출 하는 것을 말한다. 이벤트 필터링은 장기보관 할 로그와 그렇지 않은 로그를 구분하는 것이고 이벤트 통합은 유사한 항목에서 발생한 여러 개의 이벤트를 하나로 통합하는 것을 말한다.

로그 저장 시 로그 로테이션 설정을 특정 기간이나 일정 크기로 정하여 로그를 저장하고, 이렇게 쌓인 로그들을 압축하게 되면 메모리 공간을 절약 할 수 있다. 로그 아카이브의 경우 컴플라이언스 요구 조건을 만족시킬 수 있도록 일정기간 동안 로그를 저장하는 것이다. 새로운 로그를 생성하는 과정에서 불필요한 항목들은 제거하여 로그 크기를 축소 할 수 있고, 저장된 로그들은 필요에 따라 파싱하여 다른 형식으로 변환 가능하다. 로그 정규화 과정은 각각의 로그 데이터 필드를 일관된 형식으로 변환하는 것을 말한다. 로그 무결성을 보장하기 위해 각 파일에 대한 메시지 다이제스트를 계산하고 저장하게 된다.

로그 분석 기능을 통해 여러 개의 로그에서 두 개 이상의 로그 항목간의 관계를 찾는 이벤트 상관관계분석이 가능하다. 이는 통계적 방법이나 시각화 도구 등 다양한 방법으로 수행 될 수 있다. 분석을 통해 얻어진 결과는 로그 뷰어를 통해 사용자들이 읽기 편한 형태로 정보가 제공 되고, 특정 기간 동안의 활동을 요약하거나 특정 이벤트의 일련 활동에 대해 자세히 정보를 기록한 리포팅 형식으로 제공 된다.

로그 제거 기능은 더 이상 필요하지 않은 로그, 즉 일정기간이 지난 로그들을 삭제하는 것이며 이를 통해 좀

더 효율적인 로그 관리가 가능하다.

다음 절부터는 대표적인 통합로그관리시스템인 SIEM에 대해 자세히 살펴보고자 한다.

2.2 SIEM 기술 개요

SIEM(Security Information & Event Management)은 서로 다른 시스템인 SIM(Security Information Management)과 SEM(Security Event Management)이 결합된 시스템이다. SIM은 다양한 보안 정보들을 수집해 기업의 최고 보안 담당자나 경영자가 자사의 보안 정책이 컴플라이언스 수준에 적합한지 확인해 줄 수 있는 솔루션으로 로그의 장기 저장과 분석 및 리포트를 제공한다. SEM이란 국내에서는 흔히 ESM(Enterprise Security Management)라 불리는 통합 보안 관제 솔루션을 말한다. 실시간 모니터링, 이벤트의 상관관계분석, 알림, 콘솔 뷰를 제공함으로써 다양한 보안 이벤트에서 핵심적인 보안 위협을 식별하여 알려주고 효과적인 IT 보안 위험 관리를 가능하게 해 주는 솔루션이다. 즉, SIEM은 IT 시스템에서 생성된 로그들을 수집 및 저장하고, 상관관계분석을 통해 보안위협에 대응하고 각각의 제품들을 통합관리 및 컴플라이언스를 제공하는 솔루션이다.

SIEM의 주요 기능은 다음과 같다.

① 데이터 통합(Data Aggregation): 중요한 이벤트의 누락을 방지하기 위해 네트워크, 보안, 서버, 데이터베이스, 응용 프로그램 등의 다양한 장비에서 발생한 데이터를 수집하고 정규화하여 데이터를 통합한다.

② 상관관계분석(Correlation): 상관관계분석은 보안 이벤트와 관련된 기능으로 여러 장비에서 발생한 이벤트를 연결하여 보안에 위협이 되는 정보를 확인한다.

③ 알림(Alerting): 상관관계분석을 통한 이벤트와 제품의 알림 이벤트 발생 시 대시보드나 이메일 등으로 관리자에게 위협정보를 자동으로 전달한다.

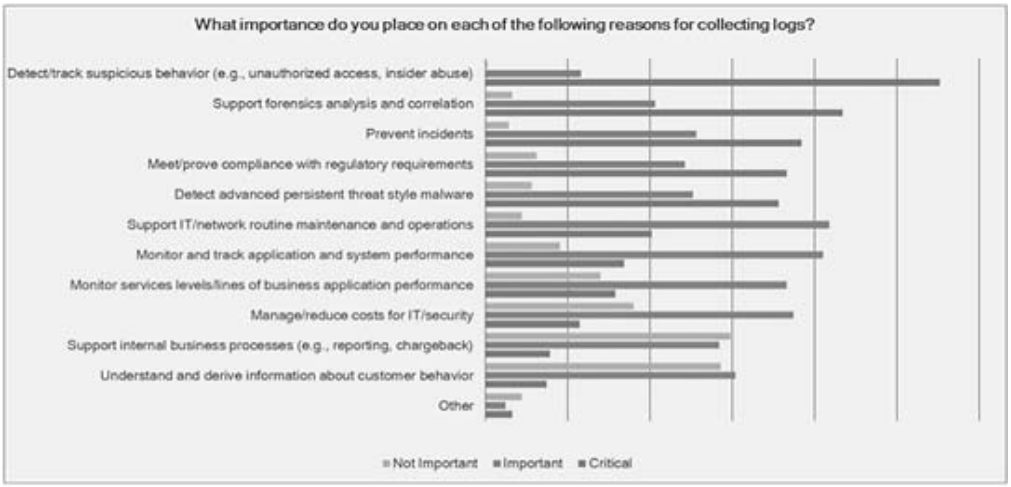
④ 대시보드(Dashboard): 현재 상황을 가시적으로 확인하기 쉽게 보여주거나 이벤트를 확인할 수 있는 차트를 만들어 정상적인 패턴의 행위가 아닌 것을 식별할 수 있도록 도와준다[7].

⑤ 컴플라이언스(Compliance): 규정 준수 데이터의 수집을 자동화하여 기존의 보안 관리 및 감사 프로세스에 맞게 보고서를 생성한다[8].

⑥ 저장(Retention): 정보 수명 관리를 위한 기능으로 컴플라이언스에서 요구하는 기간 동안 이전 로그들을 장기 저장하여 네트워크상에 이상 징후 발생 시 포렌식에 사용 될 수 있다.

2.3 SIEM 운영 방식

[그림 2]는 SANS가 IT 전문가 600명 이상을 상대로 2012년에 시행한 설문조사로, 그들이 로그 수집을 중요하게 생각하는 이유를 나타낸 것이다. 응답자들이 로그



[그림 2] 로그 수집이 중요한 이유[4]

수집을 중요하게 생각하는 가장 큰 이유로 의심스러운 행동의 감지와 추적을 위해서 라고 답했다. 그 다음으로는 포렌식이나 사고예방, 컴플라이언스 준수를 위해 로그 수집이 중요하다고 응답했다[4].

기존에 로그는 주로 시스템과 네트워크 내에서 발생하는 이벤트들의 기록으로 장애발생에 대한 대응을 위해 주로 사용되었다. 그러나 현재 로그는 필요한 정보를 검색하고, 보고서를 생성해 IT 인프라의 상태와 사용현황을 알려주어 시스템 네트워크 성능을 최적화하는데 사용될 뿐만 아니라 보안사고 발생 시 사용자의 악의적인 활동을 조사하고, 감사 자료 등에 활용되는 기업의 주요 정보 중 하나이다[1]. 특히 운영시스템과 애플리케이션 로그들은 보안 관련된 다양한 정보를 가지고 있기 때문에 체계적인 관리가 요구된다[10].

SIEM은 모든 IT 시스템에서 생성되는 로그들을 통합 분석하는 것이 핵심으로 네트워크장비, 보안장비, 서버, 애플리케이션 등에서 발생하는 모든 로그들을 수집한 후 각각의 제품 간에 교환되는 메시지 포맷을 표준화한 후 저장한다.

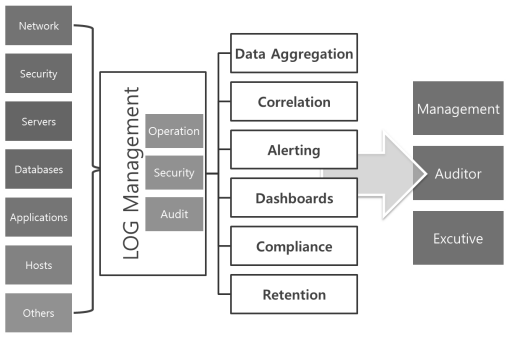
이렇게 표준화된 로그들은 상관관계분석을 통해 위협탐지 및 사전예측에 사용 되어 시스템의 전반적인 보안 수준을 높여준다. 이벤트 수집과 분석을 통해 복잡한 컴플라이언스 요구사항을 만족하고, 네트워크나 서버 등 IT 운영환경을 지속적으로 최적화 할 수 있도록 지원한다.

2.4 국내·외 SIEM 제품 특징

국내·외를 망라하여 SIEM 제품은 기업의 보안 및 위험 정보를 수집하여 분석하고 이를 통한 관리 및 평가를 통해 사고 감지 지원을 제공하는 통합 솔루션이다. 그리고 기업 환경의 모든 종류의 로그에 대해 통합검색, 보고서 작성, 분석 및 경보 기능을 제공한다.

또한 기업의 규모에 관계없이 IT운영, 응용프로그램 개발, 정보보안 문제에 따른 법적 증거 자료로 활용이 가능한 원본로그 저장소로 이용할 수 있다.

봇넷이나 웜과 같은 외부의 위협 요소와 내부자에 의한 권한 오남용과 같은 위험요소를 관리하기 위해 기업 전반에 걸쳐 발생하는 모든 로그인, 로그오프, 파일접근, DB 쿼리문 등의 이벤트들에 대한 지능적인 상관관계분석을 통해 거짓 위험 정보와 위법행위 및 보안위험



〔그림 3〕 SIEM 운영 방식

등을 분류한다.

2.4.1 국내 제품

국내 SIEM 관련 시장은 ESM과 보안 관제 프로젝트를 통해 해당 솔루션을 도입하거나, 자체적으로 구축을 하거나, 전문 보안 컨설팅 기업이 제공하는 서비스 형태(ASP)로 사용하고 있다. 이렇듯 로그 관리에서 출발하여 SIEM 솔루션으로 발전하고 있기 때문에 무결성, 압축, 대용량 처리 및 속도, 검색에 기술적 강점을 가지고 있다[11].

국내 SIEM 제품은 어플라이언스나 소프트웨어의 형태로 제공되고 있다. 이들 제품의 특징은 대용량 로그 DB 이중화가 가능하며, 분산파일 시스템을 이용해 대용량 로그 데이터의 처리와 분석, 고속 검색이 가능하다.

또한 원격 접속을 통합 작업 내역 로그도 저장하며, 분산된 다수의 시스템에서 발생하는 모든 감사로그가 위·변조 되지 않도록 수집하고 저장하여 무결성을 보장한다. 그리고 하드디스크, DVD 등에 저장된 과거 데이터를 복원하고, 고속 압축 아카이빙 기술도 지원한다.

2.4.2 국외 제품[12]

국외 SIEM 제품도 국내 SIEM과 마찬가지로 어플라이언스나 소프트웨어의 형태로 제공되고 있다. 국외 제품의 특징은 클라우드 환경의 모든 IT 시스템과 인프라에서 생성되는 테라바이트급의 대용량 데이터와 사전 스키마, 에이전트, 데이터베이스, 필터링장치 없이 모든 애플리케이션, 서버 및 네트워크 장비로부터 데이터 포맷에 상관없이 모든 데이터를 수집한다.

수집된 이벤트를 검색, 업무반영 및 공유, 모니터링 및 알림, 상관관계분석, 보고서 작성을 위해 하나의 구조체 형식으로 일반화가 가능하다.

실시간으로 수집한 데이터를 자동 이벤트 경계 식별 및 자동 타임스탬프 자동화 과정을 거쳐 세분화하여 인덱싱하고, 이렇게 모인 방대한 양의 데이터들은 하나의 포인트에서 즉각적인 실시간 검색과 다중 소스에 걸친 데이터 연관성 추적이 가능하다.

로그는 서명되고 검증되므로 컴플라이언스의 필수 요소인 인증과 무결성을 보장한다. 로그를 적절한 기간 동안 저장하여 다양한 표준과 규정(SOX, HIPAA, PCI, NIST, FISMA)에 따른 감사에 필요한 콘텐츠를 제공한다.

Ⅲ. 통합로그관리시스템 발전방향

가트너의 관련 분야 예측에서도 보듯이 현존하는 IDS/IPS와 같은 플랫폼 기반 분석 기술로는 APT를 대응하기에 역부족이기 때문에 다양한 소스의 대용량 데이터를 분석할 수 있는 전용 보안 분석 기술이 필요한 상황이며, SIEM의 발전 방향 역시 이와 동일하다[11].

감사 및 보안 업무 측면에서의 로그관리 요구사항은 데이터 위·변조 방지를 통한 데이터의 무결성 유지와 실시간 로그분석을 통한 보안사고 탐지 및 예방, 전자금융과 개인정보 등 데이터 보관에 대한 법적·제도적 규제 대응이다. 운영측면에서의 로그관리 요구사항으로는 이기종 시스템 및 다양한 애플리케이션에서 발생하는 로그의 효율적 관리와 대용량 로그 데이터의 신속·정확한 조회 및 검색 기능, 장애 발생 시 신속한 로그 검색을 통한 원인 규명 소요시간 최소화가 필요하다. 즉 감사, 사후 추적 등에 필요한 정보의 통합 관리 및 운영과 위·변조 방지를 기반으로 한 원본 로그정보 관리, 발생되는 로그 정보를 실시간으로 분석하고 활용할 수 있는 방안이 필요하다. 따라서 감사 대응 및 컴플라이언스를 위한 전사적 통합 모니터링 체계가 필요하다.

3.1 SIEM 취약점

기업들의 서비스 환경이 업무 생산성 강화를 위한 모바일 환경과 IT 비용을 줄이기 위해 클라우드 환경을 도입하면서 IT 환경은 더욱 복잡해졌다. 또한 기업 내부 및 외부에서 IT 서비스를 통해 쏟아지는 빅데이터 이벤트들의 실시간 분석을 통해 위협에 빠르게 대응하고 향후 기업의 운영 환경과 행동 계획을 도출하기 위해 SIEM의 필요성은 증가하고 있다.

현재 기업에 위협이 되는 공격 추세는 단순한 해킹 시도가 아닌 사회 공학적 기법과 고도화된 제로데이 공격이 결합된 APT가 주를 이루고 있으며 개인정보보호법 등 규제 준수의 압력도 계속해서 증가하고 있는 추세이다.

따라서 SIEM은 더욱 강화되고 늘어나는 각종 컴플라이언스와 지속적으로 진화하는 위협으로부터 IT 자산 보호, 기존 및 새로운 기술 솔루션에 대한 보안 관리 제공 등의 과제에 직면해 있다[13].

3.1.1 컴플라이언스에 대한 부담 증가

컴플라이언스 미 준수로 인해 발생하는 불이익은 모든 산업 분야에 영향을 미치고, 그로 인해 재정적 불이익이 있을 수 있다.

지난 몇 년 동안 잇따른 금융사 및 보험사, 포털 사이트 해킹 등의 보안사고로 인해 [표 4]에서 보이는 것과 같이 관련 규정이 계속해서 증가하면서 컴플라이언스의 부담이 크게 증가하였다.

3.1.2. 진화하는 네트워크 위협 증가

각종 보안 위협은 점점 더 지능화되고, 정교해지고, 치밀해짐에 따라 기존의 보안 제품으로 탐지하는 데 어려움을 겪고 있다.

고도화된 APT는 각 산업 군에 치명적인 위협 요소가 되고 있으며 특히 표적으로 삼은 특정 기업이나 조직 네트워크에 침투해 탐지를 피하면서 활동 거점을 마련한 후 기밀정보를 수집해 지속적으로 빼돌리는 보다 은밀한 형태의 공격이 증가하고 있다[14]. 이 같은 기밀 정보의 유출은 표적 기업에 치명적인 금전적 손해를 입힐 수 있다.

3.1.3. 운영비용의 계속적인 증가

IT 서비스를 제공하는 기업의 지속적인 과제는 네트워크가 끊임없이 변화한다는 것이다[26]. 원활한 서비스를 위해 조직이 새로운 기술을 도입했을 때 IT 보안 프

로그램에 영향을 미치게 되어 막대한 유지보수 비용을 초래한다. 따라서 조직은 IT 보안 프로그램 도입 시부터 비즈니스 보안 요구 사항을 충족시키면서 비용 절감을 위해 확장성이 유연한 솔루션을 요구하게 된다.

3.2 통합로그관리시스템 향후 과제

[그림 4]에서 보이는 것과 같이 IT 전문가들은 APT 유형의 멀웨어를 탐지하는 것과 사고를 예방하기 위해 수집된 로그를 활용하는 것에 어려움을 나타내고 있다.

기업은 네트워크가 공격당하기 전에 정보보안 위험을 평가하여 상황을 사전에 파악함으로써 운영 효율성을 향상 시키고 잠재적 위협으로 인한 네트워크 보안 위험을 줄일 수 있어야 한다.

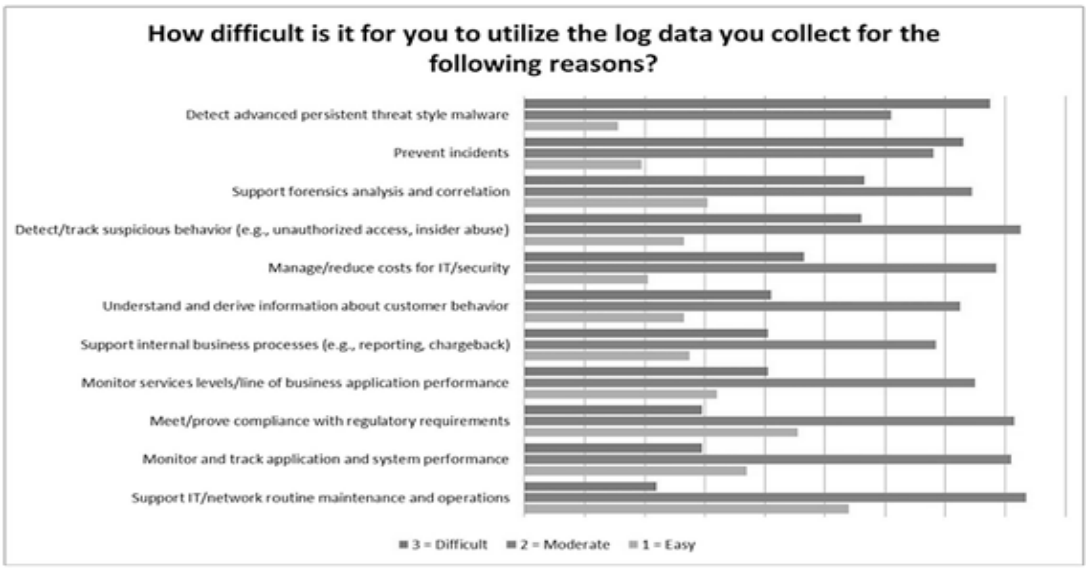
5~10년 동안 SIEM의 연구 개발은 근본적인 문제인 SIEM 아키텍처가 아닌 확장성과 비용절감에 대한 분야에만 집중 되어 있었다. 이로 인해 SIEM 아키텍처가 현재 문제가 되고 있는 시스템의 로드나 보안의 요구사항을 반영하지 못하고 있다. 따라서 SIEM 솔루션 벤더들은 확장성과 더불어 근본적인 아키텍처의 변화를 고려해야한다[16].

3.2.1 보안 인텔리전스 강화

보안 인텔리전스는 다양한 보안 기술의 상호작용을 가능하게 하는 개념과 방법론으로서 다양한 소스로 부

〔표 2〕 국내 로그 관리 관련 규제[15]

분야	규제명칭	주요내용
공통분야	개인정보보호법	개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호, 개인정보의 안전성 확보 조치, 접근 권한 관리, 접속기록의 보관 및 위·변조방지 등
정보통신 분야	정보통신망법	정보통신망을 건전하고 안전하게 이용할 수 있는 환경 조성, 침해사고의 원인 분석 및 침해사고 관련정보의 제공 방법, 개인정보의 보호조치, 접근통제 등
	정보통신기반보호법	전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행, 주요 정보통신기반시설 침해행위 금지, 침해사고의 통지, 복구조치 등
	위치정보보호법	위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호, 위치 정보의 보호조치, 위치정보의 관리적·기술적 보호조치 등
산업분야	산업기술 유출방지법	산업기술의 부정한 유출을 방지하고 산업기술을 보호, 국가핵심기술의 보호조치
금융분야	전자금융거래법	전자금융거래의 법률관계를 명확히 하여 전자금융거래의 안전성과 신뢰성을 확보, 전자금융거래기록의 생성 및 보존, 거래기록의 보존기간 및 방법, 전산자료 보호대책, 모니터링, 로그기록 관리 등
	보험업법	보험업을 경영하는 자의 건전한 경영을 도모하고 보험계약자, 피보험자, 그 밖의 이해관계인의 권익을 보호, 통신판매전문보험회사의 운영에 관한 사항 등
	신용정보보호법	신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 도모, 신용정보전산시스템의 안전보호, 신용정보 관리책임의 명확화 및 업무처리기록의 보존 등
전자상거래 분야	전자상거래법	전자문서의 안전성과 신뢰성을 확보, 거래기록의 보존, 사업자가 보존하는 거래기록의 대상 등
	전자서명법	전자서명에 관한 기본적인 사항을 정함, 인증업무에 관한 기록의 관리, 개인정보의 보호 등
	전자문서 및 전자거래 기본법	전자문서 및 전자거래의 법률관계를 명확히 하고 전자문서 및 전자거래의 안전성과 신뢰성을 확보, 전자문서의 보관 등
정부분야	전자정부법	행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정, 전자적 대민서비스 보안대책, 정보통신망 등의 보안대책 수립·시행, 인증기록의 보관, 신원 확인 및 접근권한 관리 체계의 구축 등
국방분야	국방정보화법	국방정보화 및 국방정보자원관리에 관한 사항을 규정, 국방정보침해에 대한 대응, 국방정보보호 협력체계의 구축 등
의료분야	의료법	모든 국민이 수준 높은 의료 혜택을 받을 수 있도록 국민의료에 필요한 사항을 규정, 전자의무기록, 전자의무기록의 관리·보존에 필요한 장비 등



［그림 4］ 로그 활용의 어려움[4]

터 정보를 통합하고 상호 연관성을 갖는 컨텍스트 기반의 분석 기술을 의미한다. 이는 APT와 같은 알려지지 않은 치명적인 위협·공격에 대응하기 위해, 주요 IT 기반 시설의 네트워크, 시스템, 응용 서비스 등으로부터 발생하는 데이터 및 보안 이벤트 간의 연관성을 분석하여 보안 지능을 향상시키는 차세대 보안 정보 분석 패러다임으로 해석되고 있다[11].

주요 IT 기반 시설의 네트워크, 시스템, 응용 프로그램 등에서 발생하는 데이터와 보안 이벤트의 연관성을 분석하여 알려지지 않은 새로운 공격을 가능한 한 빨리 탐지하고 해당 공격에 대한 차단과 범인을 식별할 수 있도록 보안 관리자에게 플래그를 전달하여 사고 대응 프로세스를 활성화할 수 있도록 해야 한다.

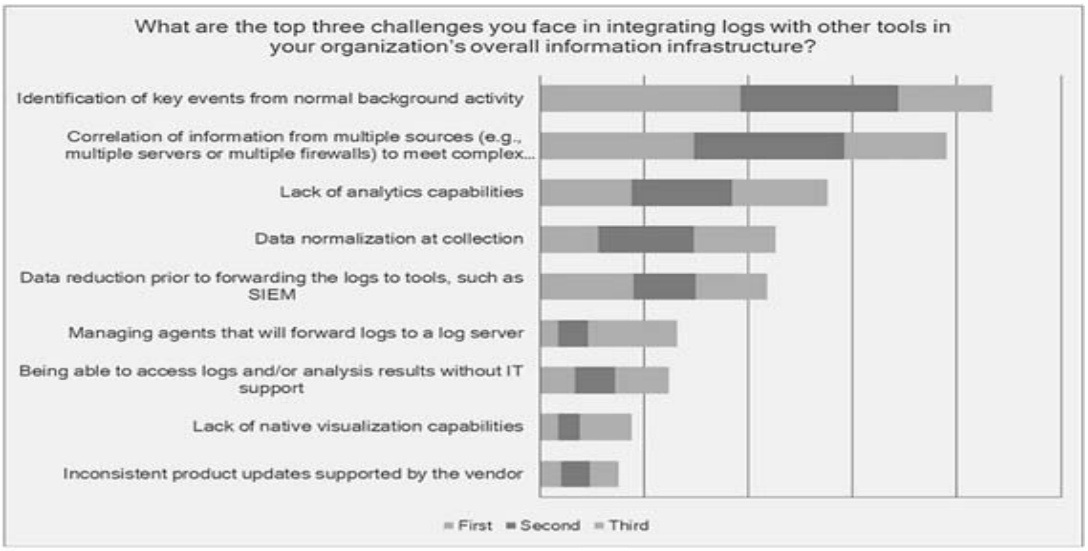
기업의 모든 로그 원본 데이터를 수집하고 저장하는 것이 필수적이지만, 보안 관리자가 문제를 해결하기 위해 모든 정보를 확인하고 꼼꼼하게 살펴 추려낼 수 없기 때문에 통합된 실시간 이벤트 상관관계분석, 위협 발견, 컴플라이언스 보고 및 감사를 통해 수집된 모든 정보를 지능적으로 축소시킬 수 있어야 한다. 또한 이렇게 축소한 이벤트 내에서 문제를 초래할 수 있는 공격을 추출하고 우선적으로 처리하도록 해야 한다. 이와 같이 이벤트의 우선순위 선정은 효율적인 대처를 가능하게 하고, 시뮬레이션 및 시각화 도구, 리스크 관리 기능을 제공함으로써 네트워크에서 발생할 수 있는 존재하는 보안 위협을 정확히 찾아내는 것을 도와줄 수 있다[13].

3.2.2 빅데이터 분석 활용

보안 빅데이터 분석 시스템 구현 관점에서 보안 빅데이터 관리 정책 및 표준화가 필요하며[17], 보안 빅데이터의 활용을 위해서는 내외부 데이터 통합 수집·분석 역량과 인프라, 조직이 필요하다.

고도화된 보안 위협으로 인해 발생하는 이상 징후에 대한 대응이 얼마나 신속하게 이루어지느냐가 중요한 경쟁력으로 평가 되는 보안 업계 특성상, 전통적인 방식으로는 급증하는 데이터를 감당할 수 없었던 문제점의 해소와 이전에는 파악조차 어려웠던 정교한 공격까지 쉽게 탐지할 수 있는 해결책으로서의 가능성을 빅데이터 기술에서 엿볼 수 있다.

빅데이터를 활용한 보안 분석은 분석기술의 고도화 측면에서 기존에 해결하지 못한 보안 분석이 가능할 것으로 예측된다. 그 예로 빅데이터 활용을 통한 기업 내에서 알려지지 않은 위협 패턴을 발견하고, 내부망에 대한 위협 감시와 내부행위 감시기술을 위한 연구에 활용되고 있다. 이는 비즈니스 가치를 높일 수 있을 것으로 예측되며, 보안 분석과 관련된 분석 대상, 정보의 규모, 속도, 다양성 및 복잡도가 급속도로 성장하고 있는 상태이다[5].



[그림 5] 로그 관리 및 통합의 어려운 양상[4]

SIEM은 실시간 모니터링, 위협에 대한 인텔리전스, 행위 프로파일링, 데이터 및 사용자 모니터링, 응용 프로그램 모니터링, 분석 등과 같은 대량의 복합 데이터 처리를 할 수 있어야 한다.

3.2.3 컴플라이언스 관리

현재 SIEM은 컴플라이언스를 지원하고 검증하는 데 중요한 역할을 담당한다. 더 나은 컴플라이언스 충족을 위해 책임 추적성, 투명성, 측정 가능성 등을 제공해야 한다.

- 책임 추적성 : 누가 무엇을 언제 하였는지 제공
- 투명성 : 보안 관리, 비즈니스 애플리케이션, 보호되고 있는 자산에 대한 가시성 제공
- 측정 가능성 : 기업 내 위험에 대한 지표 및 보고
- Out-of-the-box 리포팅 엔진을 사용하여 컴플라이언스 준수를 돕기 위해 보고서 제공
- 규정 준수 워크플로우 및 보안 제어의 전달은 조직의 재정 감소로 인한 규제 비준수의 위험을 제어[13]

3.2.4 운영 효율성 향상

기업의 여러 부서와 직원은 다양한 역할과 요구사항을 가진다. 따라서 전체 이기종 네트워크에서 로그 관리를 위한 중앙 집중식 보안 관리 솔루션이 없는 경우 컴플라이언스 준수 노력을 입증하지 못하거나, 컴플라이언스 감사를 통과하지 못할 위험이 있다.

SIEM은 컴플라이언스가 요구 되는 보안 및 네트워크 장치를 자동화 기능으로 검색 할 수 있어야 하며 이렇게 검색된 장비들의 이벤트 자료를 한곳으로 통합하여 관리 할 수 있는 기능이 요구 된다. 또한 조직의 변화에 맞추어 적용할 수 있는 확장성의 유연함이 요구된다. 효율성의 향상되면 이러한 노력과 비용들이 경제적인 관점에서 줄어들게 된다.

Ⅳ. 결 론

기업은 특정 IT 시스템의 위험을 완화하기 위해 포인트 솔루션에 많은 투자를 해왔다. 그에 따라 투자한 보안 솔루션에서 제공하는 정보를 통합하여 기업에 유용한 정보를 만들어 줄 수 있는 또 다른 통합 솔루션이 필요해졌다.

이에 기존 SIEM은 네트워크 내의 다양한 이기종 로그를 수집 및 저장하고, 이렇게 수집된 로그들의 정규화 과정을 거쳐 필요한 정보를 검색하고 컴플라이언스를 위한 보고서를 생성해 기업 IT 인프라의 상태와 사용 현황을 알려주고, 또한 상관관계 분석을 통해 기업 네트워크 내의 위협을 감지했다. 또한 보안사고 발생 시에는 로그 데이터를 기초로 원인을 추적하고, 감사하는 역할

을 해왔다.

하지만 [그림 5]에서 보여주는 바와 같이 회사의 인프라 구조에서 다른 툴과 로그를 통합할 때, 이벤트 발생 시 정상적인 이벤트인지 식별하는 문제나 다양한 장비들에서 발생한 정보들의 연관성에 관한 문제 그리고 분석 기능의 부족등과 같은 문제를 낳고 있다. 또한 현재 기업의 IT환경은 업무 생산성 강화를 위한 모바일 환경과 IT 비용을 줄이기 위한 클라우드 환경의 도입으로 점점 더 복잡해짐에 따라 SIEM에 대한 더욱 고도화된 기능을 요구한다.

따라서 차세대 SIEM은 빅데이터 활용 및 보안 인텔리전스를 통합하여 접근함으로써 사전에 외부 위험을 예측하고, 내부자에 의한 정보 유출을 방지 할 수 있는 기능을 강화해야 한다. 보안사고 관련 규정이 증가함에 따라 더 나은 컴플라이언스를 제공할 수 있도록 노력해야 하며, 끊임없이 변화하는 네트워크 환경 속에서도 유연하게 대처 할 수 있도록 변화해야 한다.

약어정리

APT	Advanced Persistent Threat
COBIT	Control OBjectives for Information related Technology
ESM	Enterprise Security Management
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NIST	National Institute of Standards and Technology
PCI	Payment Card Industry
RMS	Risk Management System
SEM	Security Event Management
SIEM	Security Information & Event Management
SIM	Security Information Management
SOX	Sarbanes Oxley
TMS	Threat Management System

참고문헌

[1] NIST FIPS PUB 800-92, *Guide to Computer Security Log Management*, Sep. 2006.

[2] 김종현, 임선희, 김익균, 조현숙, 노병규, “빅데이터를 활용한 사이버 보안 기술 동향”, ETRI 전자통신동향분석 제 28권 제 3호, June. 2013.

[3] IDC, “Korea Security Software 2012-2016 Forecast Update 2011 Review,” May 2012.

[4] 윤정광, “효과적인 SIEM 도입을 위한 7계명”, 아이티데일리, Sep. 2008.

[5] 노병규, 김도우, 김경신, 김익균, “지능형 사이버보안 기술 동향 및 이슈”, PM Issue Report 2013-제1권 이슈3, Feb. 2013.

[6] Mark Nicolett, Kelly M, Kavanagh, “Magic Quadrant for Security Information and Event Management”, Gartner Group, July. 2013.

[7] Adrian Lane, “Understanding and selecting SIEM/LM:Use Cases, Part1”, Securosis, April. 2010.

[8] AccelOps, “Compliance Management and Compliance Automation-How and How Efficient Part1”, April. 2010.

[9] Jerry Shenk, “Learning from Logs: SANS Eighth Annual 2012 Log and Event Management Survey Results”, A SANS Whitepaper, May. 2012.

[10] 오현식, “IT 기초 데이터, 로그를 살펴라”, 데이터넷.

[11] 김동한, “빅데이터 환경에서 지능형 로그 관리 플랫폼으로 진화하는 보안 정보/이벤트 관리(SIEM) 동향”, 정보통신산업진흥원 주간기술동향, Aug. 2013.

[12] Mark Nicolett, Kelly M, Kavanagh, “Magic Quadrant for Security Information and Event Management”, Gartner Group, May. 2012.

[13] Q1Labs, “The Business Case for a Next-Generation SIEM”, Q1 Whitepaper.

[14] 정경원, 고수연, “현지화 전략을 통해 한국 보안 시장 성장 같이 가겠다.”, ITDaily, Feb. 2013.

[15] 로그 컴플라이언스 연구 센터, *로그 컴플라이언스 연구 보고서*, ㈜이너버스, June. 2013

[16] Adrian Lane, Mike Rothman, “Security Management 2.0: Time to Replace Your SIEM?”,

Securosis version 1.5, McAfee, Oct. 2011.
[17] 최대수, “빅데이터 환경에서 차세대 통합보안 기술”, Software Convergence Symposium 2013 발표자료, Jan. 2013.

〈저자소개〉

유 기 순 (Ki-Soon Yu)
학생회원

2007년 2월 : 안동대학교 컴퓨터공학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 네트워크 보안, 모바일 보안

임 설 화 (Sul-Hwa Im)
학생회원

2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 모바일 보안, 보안 컨설팅, 클라우드 컴퓨팅 보안, 네트워크 보안

김 학 범 (Hak-Beom KIM)
정회원

1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원(KISA) 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2011년 9월~2013년 3월 : (주)지엔에스인증원 ISMS본부장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2013년 4월~현재 : ㈜이너버스 연구소장
<관심분야> 통합로그 시스템, 빅데이터 보안, 클라우드 컴퓨팅 보안, 개인정보보호, PIMS