Cybersecurity를 위한 SOC & SIEM 기술의 동향

(Trends of SOC & SIEM Technology for Cybersecurity)

차병래***, 최명수**, 강은주***, 박 선*, 김종원*

(ByungRae Cha, MyeongSoo Choi, EunJu Kang, Sun Park, and JongWon Kim)

요 약

최근 많은 보안 사고의 발생에 따라 SOC(Security Operation Center)과 SIEM(Security Information & Event Management)에 대한 관심이 집중되고 있으며, 이에 따른 다양한 연구들과 정보 보안 업계의 다양한 상업화 제품들이 출시되고 있다. 이러한 상황을 반영하듯이 미국의 NIST에서는 Cybersecurity Framework에 관한 문서의 발간 및 개정을 진행하고 있다. 본 연구에서는 NIST의 Cyberseurity Framework를 고찰하고 SOC 및 SIEM 보안 기술 및 솔루션의 동향에 대해 살펴보고자 한다. 더불어 실시간 빅데이터 보안으로 오픈소스 Apache Metron을 소개한다.

■ 중심어 : 사이버시큐리티 프레임워크; SOC(Security Operation Center); SIEM(Security Information & Event Management); NIST(National Institute of Standards and Technology)

Abstract

According to the occurrence of many security incidents, the SOC(Security Operation Center) and SIEM(Security Information & Event Management) are concentrated recently. The various studies and commercial products of the information security industry are being released. As reflected in this situation, NIST in the US is publishing and revising the document about the Cybersecurity Framework. In this study, we investigated the NIST's Cyberseurity Framework, trends in SOC and SIEM security technologies and solutions, and also introduce the open source Apache Metron of a real-time Bigdata security tool.

■ keywords : Cybersecurity Framework; SOC(Security Operation Center); SIEM(Security Information & Event Management); NIST(National Institute of Standards and Technology)

Ⅰ. 서 론

국가 및 경제 측면의 보안은 중요한 인프라의 신뢰성에 따라 달라지며, 사이버 보안 위협은 국가 인프라의 복잡성과 연결성을 악용하여 국가의 보안, 경제 및 공공 안전 및 보건을 위험에 빠뜨릴 수 있다. 재정적 및 평판 위험과 마찬가지로 사이버 보안 위험도는 회사 및 조직의 수익에 막대한 영향을 미치며, 비용을 늘리고 매출에 영향을 줄 수 있다. 또한 조직의 혁신 능력과 고객 확보 능력에 악영향을 끼칠 수 있다. 더불어, 최근 악성코드를 이용한 봇넷 디도스 공격은 트래픽 규모가 막대했을 뿐만 아니라 수십만 대의 사물인터넷 기기를 악용했다는 점에서 보안 업계에 큰 충격을 주었다[1, 2]. 기존 보안 체계의 대안으로 기업 내외부의 다양한 정보를 수집해 보안 위협을 관리하는 SOC와 SIEM 등이 주목을 받고 있다. 이러한 상황을 반영하듯이 NIST는 Cybersecurity Framework 문서를 공개하면서 지속적으로 개정을 진행하고 있다[3].

본 연구에서는 NIST의 Cybersecurity Framework의 개괄적인 내용을 확인하며, SOC의 개념과 이에 관련된 Cisco의 SCO와 IBM의 security Operation Operating Model, 그리고 실시간 빅데이터 보안의 오픈소스 Apache Metron을 간략하게 정리하며, 더불어 SIEM의 기술 동향을 살펴본다.

Ⅱ. NIST의 Cybersecurity Framework

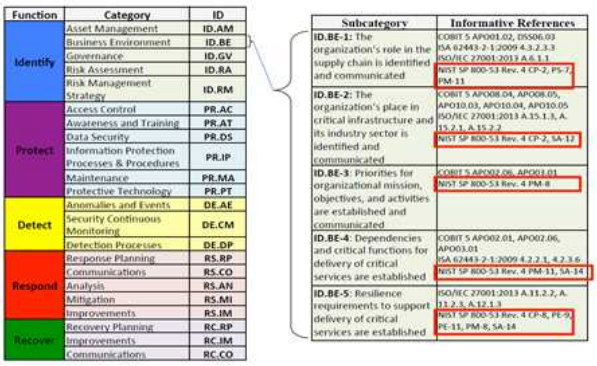
NIST(National Institute of Standards and Technology)

* 정회원, 광주과학기술원 전기전자컴퓨터공학부
** 정회원, 제노테크(주)
*** 정회원, 호남대학교 정보통신공학과
이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2016-0-00149, "2 Factor 기반의 인증이 강화된 NFC폰 O2O 결제 시스템 개발").

접수일자 : 2017년 06월 16일
수정일자 : 2017년 08월 17일
게재확정일 : 2017년 09월 19일
교신저자 : 김종원 e-mail : jmkim@jnu.ac.kr

의 Cybersecurity Framework(CSF, NIST 800-53)는 2014년 2월에 조직의 내·외부 간의 위험 및 사이버보안 관리 통신을 위하여 설계되었다. CSF의 메커니즘은 사이버보안의 현재 상황과 사이버보안을 위한 타겟의 상태를 기술하게 되며, 연속 또는 반복되는 프로세스의 전후 관계의 개선을 위하여 기회를 식별 및 우선사항을 결정한다. 더불어, 타겟의 상태 추이를 평가하며, 사이버보안의 위험에 관하여 내·외부 간에 통신하게 된다. Cybersecurity Framework(CSF)의 구성은 크게 Framework Core, Framework Implementation Tiers, 그리고 Framework Profile로 [그림 1]과 같이 구성된다[3].

그림 1. NIST의 Cybersecurity Framework의 컴포넌트



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

그림 2. Framework Core의 구성 요소

Framework Core는 일련의 사이버 보안 활동, 바람직한 결과, 그리고 주요 인프라스트럭처 분야에서 공통적으로 적용되는 참조 자료이며, Framework Core의 핵심은 사이버 보안 활동 및 결과를 집행 단계에서 구현/운영 단계에 이르는 조직 전체의 의사소통을 허용하는 방식으로 업계 표준, 지침 및 관행을 제시한다. [그림 2]와 같이 Framework Core는 Functions, Categories, Subcategories, 그리고 Informative References의 요소들로 구성되며, Framework Core의 Functions는 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recovery) 의 5 개 기능들을 동시 및 연속적으로 구성 및 함께 고려하며, 이 기능들은 조직의 사이버 보안 위험 관리의 라이프 사이클에 대한 고차원적이고 전략적인 시각을 제공하게 된다.

Framework Implementation Tiers는 조직이 사이버 보안 위험을 파악하는 방법과 그 위험을 관리하기 위한 프로세스를 제공한다. Tiers 는 조직의 사이버 보안 위험 관리 기법이 프레임 워크에 정의 된 특성(예: 위험 및 위협 인식, 반복 가능 및 적응성)을 나타내는 정도를 설명한다. Tier는 Partial(Tier 1)에서 Adaptive(Tier 4)까지 범위에서 조직의 관행을 특성화(Risk Management Process, Integrated Risk Management Program, External Participation, 그리고 Cyber Supply Chain Risk Management)하며, 이러한 Tiers는 비공식적이고 반응적인 대응에서 민첩하고 위험에 노출된 접근 방식으로의 진행을 반영한다. Tier 선정 프로세스 중에 조직은 현재의 위험 관리 관행, 위협 환경, 법률 및 규정 요구 사항, 비즈니스/임무 목표 및 조직적 제약 사항을 고려해야 한다.

Framework Profile 은 조직이 프레임 워크 범주 및 하위 범주에서 선택한 비즈니스 요구 사항을 기반으로 한 결과를 나타내며, 이 Profile은 특정 구현 시나리오에서 Framework Core에 대한 표준, 지침 및 실행 방식의 조정으로 특징지어질 수 있다. Profile은 "현재" 프로필("있는 그대로" 상태)과 "대상" 프로필("예정된" 상태)을 비교하여 사이버 보안 상태를 개선 할 수 있는 기회를 식별하는 데 사용할 수 있다. 조직은 Profile을 개발하기 위해 모든 범주 및 하위 범주를 검토하고 비즈니스 동인 및 위험 평가에 따라 가장 중요한 항목을 결정하게 되며, 조직의 위험을 해결하기 위해 필요한 경우 범주 및 하위 범주를 추가할 수 있다. 현재 프로파일은 목표 프로파일에 대한 진행의 우선순위 지정 및 측정을 지원하는 동시에 비용 효율성 및 혁신 등 다른 비즈니스 요구를 고려하는 데 사용될 수 있으며, Profile을 사용하여 조직 내에서 또는 조직 간에 자체 평가를 수행하고 의사소통할 수도 있다.

프레임워크 구현을 위한 조정(Coordination of Framework Implementation)은 [그림 3]과 같이 조직의 Implementation/Operations, Business/Process, 그리고 Executive 레벨에서 일반적인 정보 흐름과 의사결정의 흐름을 묘사하고 있다. 또한, 조직은 이 CSF 프레임워크를 사이버 보안 위험을 식별, 평가 및 관리하기 위한 체계적인 프로세스의 핵심 부분으로 사용할 수 있다. CSF 프레임워크는 기존 프로세스를 대체하도록 설계되지 않았으며, 조직은 현재의 프로세스를 사용하여 이를 CSF 프레임워크에 오버레이하여 현재의 사이버 보안 위험 접근법의 간극을 판별하고 개선된 로드맵(Roadmap)을 개발할 수 있다. 조직은 사이버 보안 위험 관리 도구로 CSF

프레임워크를 활용하여 중요한 서비스 제공에 가장 중요한 활동들을 결정하고 비용 측면의 영향을 극대화하기 위해 비용 우선 순위를 정할 수 있게 된다. 조직이 CSF 프레임워크를 사용하여 새로운 사이버 보안 프로그램을 만들거나 기존 프로그램을 개선하기 위해서는 다음 [그림 4]의 단계들이 필요에 따라 반복되어 사이버 보안을 지속적으로 개선해야 한다.

CSF 프레임워크의 측정(measurement)은 조직의 내부와 외부 양쪽의 강한 신뢰 관계를 위한 기반을 제공한다. 시간 경과에 따른 상태 및 추세를 내부적으로, 외부 감사를 통해, 적합성 평가를 통해 측정함으로써 조직은 의미 있는 위험 정보를 이해하고 전달할 수 있게 된다. CSF 프레임워크는 포괄적인 측정의 기저로 사용될 수 있으며, 프레임워크의 측정하는 주요 용어는 "Metric"와 "Measures"를 사용하게 된다. 사이버 보안을 측정하는 목적은 사이버 보안을 비즈니스 목표와 연관시켜 인과 관계를 이해하고 정량화하는 것이다.

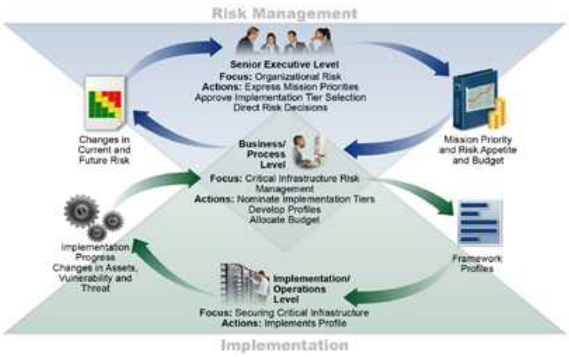


그림 3. 조직의 정보 및 의사결정 흐름의 개념도

그림 4. 프레임워크를 통한 사이버보안 프로그램의 개발 및 개선

III. Security Operation Center (SOC)

최근 많은 조직 및 기관에서는 사이버 범죄와 IT 남용의 대응책으로 자신들만의 SOC를 소유하고자 하지만, SOC는 보안의 상징으로 과대 광고되어 아직까지는 실제적인 효용가치는 낮게 평가되고 있다[4]. 아무리 많은 비용을 투자하더라도 세계 수준의 보안 운영 센터(SOC)를 한 순간에 구축할 수 없기 때문에 점진적 구현 단계에 대한 계획을 수립하는 것이 매우 중요하다[5]. SOC를 구축하기위한 사람, 기술, 그리고 프로세스 간의 삼각 구조와 전형적인 SOC 조직을 나타내면 [그림 5]와 같다.

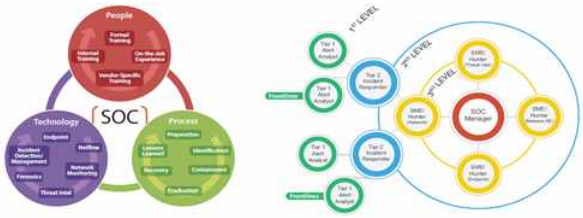


그림 5. 사람, 기술, 프로세스의 SOC 삼각 구조와 전형적인 SOC 조직

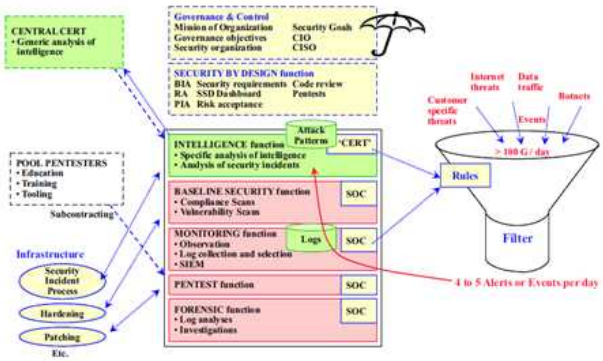


그림 6. SOC의 컴포넌트 및 토플로지

SOC의 역할은 [그림 6]에 나타낸 것과 같다. SOC의 기본 컴포넌트가 5가지 영역으로 나뉘질 수 있으며, 이들 영역은 Intelligence function, Baseline Security function, Monitoring function, Penetration Test function, 그리고 Forensic function 이다. SOC의 커널은 컴퓨터 응급 대응 팀(Computer Emergency Response Team, CERT)과 유사점을 갖는 Intelligence function 이며, 유능하고 숙련된 분석가가 내부 및 외부 당사자와 정보 교환, 위협 패턴 분석 및 결과 모니터링, 이벤트 필터링에 대한 규칙 정의 및 운영 요원과 보안 요원에게 지침을 제공한다. Baseline Security를 위한 SOC 분석은 서버, 운영 체제 및 네트워크 구성 요소 강화를 위한 운영 프로세스를 감독하고 취약성 및 준수 검사를 수행하여 강화 지침의 준수여부를 확인한다. 또한 알려진 취약성을 검사하고 우선순위가 높은 보안 패치에 대한 실제 지침에 따라 유지 관리 수준을 확인하며, 또한 이 기능은 엔드포인트 보호, 방화벽, IDS/IPS(Intrusion Detection and Protection System), PKI(Public Key Infrastructure) 등의 설정 및 운영 효율성을 감독하게 된다. SOC 모니터링 기능은 데이터 트래픽을 관찰하고 이상을 식별 및 탐지하기 위하여 대용량의 로깅 데이터 및 신호는 동적 규칙 세트를 사용하여 저장하고 필터링을 수행한다. 모니터링 기능의 주요한 기능 중의 하나는 관련 경고 또는 이벤트들만을 식별하는 방식으로 보안 정보 및 이벤트 관리자(SIEM)를 조정한다는 것이다. 침투 테스트(Penetration Test)는 보안 서비스 개발의 필수적인 부분과 운영 환경 내에

서 모두 사용되며, 침투 테스트를 통해 시스템이 공격에 어떻게 반응하는지, 시스템 방어의 침해 여부, 방어의 무효 인지, 시스템에서 어떤 정보를 얻을 수 있는지를 결정할 수 있게 된다. SOC의 전문 분석가는 포렌식 기능을 이용하여 데이터 트래픽 및 로깅 인프라 데이터의 세부 사항 등을 법 집행 기관을 위한 전자 증거를 수집하고 그러한 증거의 보관 및 연관성을 확보하는 데 도움을 제공한다.

각 SOC는 자신이 속한 조직만큼 고유하기 때문에 결과에 영향을 미치는 요인을 이해하는 것이 중요하며, SOC는 모든 내부 운영, 프로세스, 기술 및 직원을 포함 할 수 있으며 외부 공급 업체 관리 서비스에 크게 의존하거나 외부 직무 및 내부 역량의 혼합이 될 수 있다. 더불어 조직은 비용, 기술 가용성, 단일 지점 대 다지점의 글로벌 위치, 24 시간 보장 및 지원 등의 중요성을 고려해야만 한다.

1. 시스코의 OpenSOC

시스코의 OpenSOC 프로젝트는 확장 가능한 고급 보안 분석 도구를 제공하기 위한 Apache Hadoop Framework기반의 협업 오픈 소스 개발 프로젝트와 동시에 공동 작업 소스 커뮤니티를 제공한다. OpenSOC은 데이터 센터의 네트워크 트래픽, 데이터의 소비, 그리고 모니터링 하도록 설계된 Big Data 보안 분석 프레임워크이며, 확장 가능하고 대규모로 작동하도록 설계되었다[6].

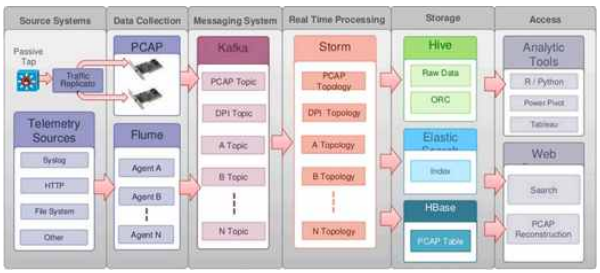


그림 7. 시스코의 OpenSOC - Stitching Things Together

OpenSOC 프레임워크는 OpenSOC를 연결하여 모든 원격측정 소스를 모니터링하기 위한 확장 가능한 스파우트 및 파서를 제공하며, 모든 원격 측정의 스트림을 위한 확장 가능한 프레임워크와 이상 탐지 및 실시간 규칙 기반 경고를 제공한다. 또한, 맞춤형 유지 시간의 Hadoop 기반 스토리지, Elastic Search가 지원되는 원격 측정 스트림에 대한 자동화된 실시간 색인, Hive가 지원하는 Hadoop에 저장된 데이터에 대한 원격 측정 상관 관계 및 SQL 쿼리 기능, 그리고 ODBC/JDBC 호환성 및 기존 분석 도구와의 통합 기능 등을 제공한다. OpenSOC는 OpenSOC-Streaming 저장소와 OpenSOC-UI 저장소로 구성되며, OpenSOC-Streaming 저장소에는 원격 측정 메시지, PCAP 재구성 서비스 및 기타 다양한 데이터 서비스를 처리, 강화, 색인 및 코어 레이팅하는 토폴로지가 존재하며, OpenSOC-UI 저장소에는 로그 및 네트워크 패킷 분석을 수행하고 경고 및 오류를 표시하는 UI가 존재한다.

2. IBM의 Security Operation Operating Model & SIEM Functional Model

사이버 보안 공격의 산업화 시대에는 사이버 보안의 변화 속도를 이해하기 어려우며, SOC의 가치는 클라이언트가 채택한 유스케이스와 규칙 및 사용 가능한 데이터와 직접적으로 연관되고 있다. IBM 또한 SOC 모델과 SIEM의 기능 모델을 제안하였으며, [그림 8]은 침해사고 이전(위협)과 이후(보안사고)의 관계를 나타내고 있으며, [그림 9]는 IBM의 Security Operation Operating Model을 표현하고 있다. Security Operation Operating Model은 Technology, Operations, 그리고 Strategy의 3 계층으로 구성되며, 특히 Technology 계층의 SIEM은 [그림 10]의 SIEM Functional Model을 참조한다[7].

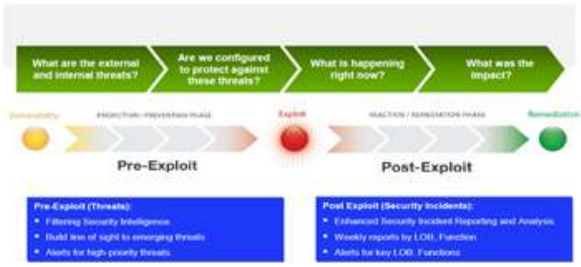


그림 8. IBM의 보안 위협과 보안 사고의 보안 분석

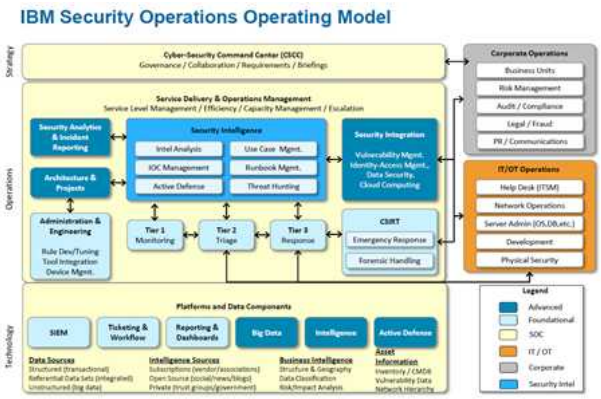


그림 9. IBM의 Security Operations Operating Model

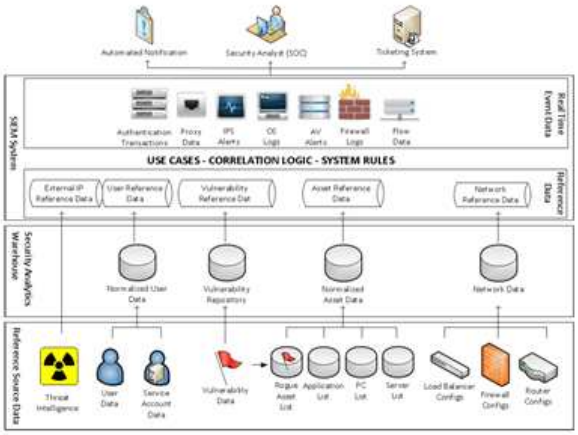


그림 10. IBM의 SIEM Functional Model의 개념도

3. 오픈소스 Apache Metron

오픈소스 Apache Metron은 OpenSoc이라는 Cisco 프로젝트에서부터 시작하였으며, Apache Metron은 다양한 보안 데이터 피드를 수집, 처리 및 저장하여 사이버 이상(cyber anomaly)을 탐지하고 조직이 신속하게 대응할 수 있도록 하는 사이버 보안 응용 프로그램 프레임 워크이다[8]. Apache Metron은 핵심 능력(Core Capabilities)과 핵심 기능적 주제들(Core Functional Themes)로 구분되며, [그림 11]의 왼쪽은 Apache Metron의 Core Functional Capabilities를 나타낸 것이다.

Metron 프레임워크는 보안 데이터 레이크/저장소(security data lake/vault), 추가 가능한 프레임워크(pluggable framework), 보안 응용(security application), 위협 지능 플랫폼(threat intelligence platform)의 4가지 핵심 능력을 제공한다. 보안 데이터 레이크/저장소는 Metron 플랫폼이 오랜 시간 동안 풍부한 원격 측정 데이터를 저장하는 비용 특면의 효율적인 방법을 제공하며, 데이터 레이크는 검색 분석을 지원하고 운영 분석을 검색하고 쿼리가 가능한 메커니즘을 제공하는 기능 엔지니어링을 수행하는 데 필요한 데이터 모음을 제공한다. Pluggable Framework는 Metron 플랫폼이 일반적인 보안 데이터 소스(pcap, netflow, bro, snort, fireye, sourcefire)를 위한 풍부한 파서 세트를 제공할 뿐만 아니라 새로운 데이터 소스에 대한 새로운 사용자 정의 파서를 추가하기 위한 추가 가능한 프레임워크를 제공하며, 원시 스트리밍 데이터에 보다 많은 상황 정보를 제공하는 강화 서비스, 위협 인텔 피드용 추가 확장 기능 및 보안 대시 보드를 사용자 정의하는 기능을 제공한다. Apache Metron은 보안 응용으로 표준 SIEM과 비슷한 기능(경보, 위협 지능 프레임워크, 데이터 소스를 수집하는 에이전트)을 제공하지만 SOC 분석가가 일반적으로 사용하는 패킷 재생 유틸리티, 증거 저장소 및 헌팅 서비스도 제공한다. Threat Intelligence Platform은 이벤트가 스트리밍되는 동안 실시간으로 적용할 수 있는 일종의 비정상 탐지 및 기계 학습 알고리즘을 사용하는 차세대 방어 기술들을 제공한다.

그림 11. Apache Metron의 Core Functional Capabilities와 플랫폼의 논리적 컴포넌트의 다이어그램

Metron의 핵심 기능적 주제는 4 가지로 분류되며, Metron 커뮤니티 그룹이 형성됨에 따라 새로운 기능과 개선 사항들이 플랫폼(Platform), 데이터 수집(Data Collection), 데이터 처리(Data Processing), 그리고 UI(User Interface) 등의 4 가지 주제들에 대해서 우선적으로 적용될 것이다. Apache Metron의 아키텍처는 크게 Metron Components와 논리적 아키텍처로 구성되며, 특히 Metron Components는 Metron 모듈과 도메인 스픽 언어(domain Specific Language)로 구성된다. Apache Metron의 논리적 아키텍처는 [그림 11]의 오른쪽과 같이 간략하게 나타낼 수 있으며, Telemetry Event Buffer, Process(Parse, Normalize, Validate and Tag), Enrich, Label, Alert and Persist, UI Portal and Data & Integration Service, 그리고 fast Telemetry Ingest와 Telemetry Ingest로 구성된다.

IV. Security Information & Event Management (SIEM)

최근의 고도화/대규모화되는 네트워크 인프라를 통한 다양한 보안 위협을 조기에 탐지 및 대처하기 위해서는 체계적인 수단이 필수적이다. 이를 위하여 각종 보안 장비, 네트워크 인프라, 서버/스토리지 장비 및 서비스 응용들로부터 생성되는 로그, 패킷 등 대량의 이벤트 데이터를 수집하고, 이에 대하여 BigData(빅데이터) 솔루션을 활용한 보안 분석을 수행하는 보안 관제 체계가 필요하다. 이러한 역할을 담당하는 상용(commercial) 중심의 솔루션이 보안 정보 및 이벤트 관리(Security Information and Event Management: SIEM)로 널리 호칭된다.

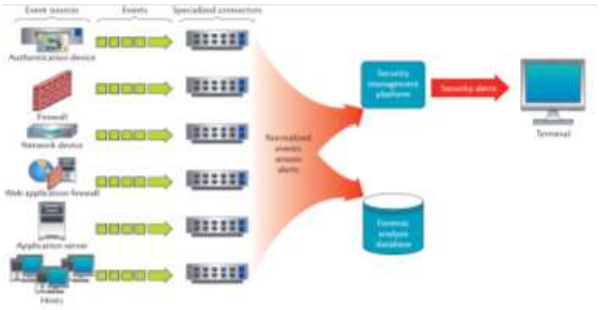


그림 12. 대표적인 SIEM 솔루션의 구조

[그림 12]에 제시한 바와 같이 SIEM은 가상/실제 네트워크들, 서비스 응용들, 시스템 로그들과 이벤트 데이터를 수집한 후에 이를 분류하고 분석해서 빠른 리포팅을 제공하고, 추가 개입이나 변경된 대응이 필요한 경우는 경고를 수행한다[9]. 또한 SIEM 솔루션이 제공하는 보안 도구들은 기관/기업의 IT 조직에서 보안 관련한 중심 역할을 하는 보안운영센터(security operations center: SOC)의 핵심적인 역할을 담당하고 있다. SIEM 솔루션들은 소프트웨어, 장비(appliances) 또는 관리 서비스 형태로 판매하며, 이들은 보안 데이터(security log)를 기록하고 규정 준수(compliance)를 위한 보고서 생성에도 사용된다. 정리해보면 SIEM의 핵심 기능들은 사용자 및 서비스 권한, 디렉토리 서비스 및 기타 시스템 구성 변경을 모니터링하고 도움을 제공하는 것이며, 추가로 로그 감사/검토 및 사건(incident)별 응답 등을 제공하기도 한다.

1. SIEM의 솔루션 동향

체계적인 정보 수집/분석을 통한 보안 관제를 담당하는 솔루션인 SIEM은 보안 정보 관리(Security Information Management: SIM)와 보안 이벤트 관리(Security Event Management: SEM)를 결합하면서 발전 및 점진적인 진화를 거치면서 유사한 범주로 파생되는 추세를 지속적으로 형성하고 있다. 예를 들면 SIEM 기능을 보완하기 위해 Cloudera 등에서는 데이터 저장 용량 및 분석 유연성을 확장하여 Apache Hadoop, Apache Spark 과 같은 빅데이터 플랫폼을 접목하고 있다[11]. 음성 중심 가시성(voice-centric visibility) 또는 vSIEM(voice SIEM)의 필요성은 이러한 진화의 사례이다.

최근에는 보다 많은 기관과 기업들이 표적 공격과 데이터 유출을 조기에 탐지할 필요성을 인식하고 있으며, 사전/사후 이벤트 데이터에서 노이즈 성격의 신호들을 정렬하면 SIEM 기능을 통한 고급 프로파일링 및 분석에 새로운 파급력을 추가할 수 있을 것이다. 이러한 상황에 대해서 Gartner는 2016년 8월에 “2016 Magic Quadrant for SIEM” 문서를 공개하였으며[12], [그림 13]과 같이 새로운 SIEM 솔루션 업체들이 보안 정보 및 이벤트 관리를 위해 특별히 설계된 다양한 종류의 기법들을 제공 및 경쟁하고 있음을 보여준다. 또한 상위 13개 SIEM 벤더들(IBM Security, Hewlett Packard Enterprise, Splunk, Intel Security, LogRhythm, EMC(RSA), AlienVaul, TrustWave, MicroFocus(NetIQ), AccelOps, EventTracker, SolarWinds, BlackStratus)의 솔루션들에 대한 장단점들을 세부적으로 구분 및 설명하고 있다.

그림 13. 2016 Gartner Magic Quadrant for SIEM

또한 Gartner의 보고서에 따르면 SIEM 시장은 이미 성숙단계에 있으며 주요 SIEM 벤더의 60%가 2017년까지 사용자 및 엔티티 행동 분석(User & Entity Behavior Analytics: UEBA) 기반 보안 솔루션을 통합할 것으로 예상하고 있다[13]. UEBA란 사용자, 장비, 소프트웨어 등의 이상 행동을 문맥 분석(context analysis) 수준에서 파악함으로써 보안 위협을 탐지하는 것이다. 가트너의 보고서에서 언급한 주요 기업 중 이러한 문맥 분석을 통한 보안을 제공하는 사례로는 HPE, IBM, Intel Security, Splunk, LogRhythm 등이 있다.

2. SIEM 솔루션의 사례 연구

가. Cybrary.IT

Cybrary.IT의 SIEM 개념은 모든 응용 프로그램 또는 네트워크 방화벽 등은 이벤트 발생에 대한 로그를 생성하게 되며, 각 애플리케이션에서 생성 된 로그를 중앙화된 SIEM으로 푸시하게 된다. 또는 모니터링 되어야하는 다른 응용 프로그램에 수집기를 설치 및 구성하여 응용 프로그램의 로그를 SIEM 도구로 푸시하게 된다. SIEM은 수집된 원시 로그를 분

석하고 필요한 정보만을 추출하게 된다. 또한 일반적으로 로그의 크기는 회사의 네트워크 트래픽 속도를 기반으로 한다. 따라서 빅데이터 분석은 또한 SIEM에서 중요한 역할을 하게 된다.

나. LogRhythm

LogRhythm는 “침입이 발생했을 때 빠른 대응이 중요하다”는 모토로 위협 관리 워크플로우를 [그림 14]와 같이 표현하고 있으며, 데이터 운영(data-driven) 및 기계학습(machine learning) 분석 방법을 통하여 고급 위협 요소를 탐지한다[14]. 또한 위협의 탐지 절차(Forensic Data, Discover, Qualify)와 대응 절차(Investigate, Neutralize)를 통한 양극단간 보안 지능 플랫폼을 지원하며, 위험 기반 우선순위 알고리즘(risk-based-priority algorithm)은 위험 요소와 위협 요소를 적용하여 자동으로 경보의 특성에 따라 위험도가 가장 높은 문제를 해결하는 데 시간을 할애할 수 있게 하고 있다.

그림 14. LogRhythm의 위협 관리 워크플로우의 가속화

다. ManageEngine

ManageEngine의 SIEM 솔루션은 네트워크 장치, 시스템 및 응용 프로그램에 대한 네트워크 보안 인텔리전스 및 실시간 모니터링을 제공한다. IT 관리자는 SIEM 솔루션을 통한 정교한 사이버 공격을 완화시키고 보안 사고의 근본 원인을 확인, 사용자 활동을 모니터링 및 데이터 침해를 방지하므로써 가장 중요한 요구사항인 규정 준수 요구 사항을 충족할 수 있다.

특히, IT 보안을 위해 테라바이트의 로그 데이터를 관리하면서 대부분의 SIEM 솔루션에 공통적으로 적용되는 14 가지 중요한 기능들([그림 15] 참조)과 로그 분석기 소프트웨어를 사용하여 하나의 중앙 위치에서 수집, 분석, 상관, 검색, 보고 및 보관을 수행하여 테라바이트 단위의 시스템 생성 로그 관리 프로세스를 자동화할 수 있다. 이 이벤트 로그 분석기 소프트웨어는 로그를 지능적으로 분석하고 사용자 활동 보고서, 과거 추세 보고서 등과 같은 다양한 보고서를 즉시 생성함으로써 파일 무결성을 모니터링하고 로그 포렌식 분석을 수행하며 권한 있는 사용자를 모니터링하고 다양한 규제를 준수할 수 있도록 지원한다.

그림 15. ManageEngine의 SIEM 개념도

라. SPP

SPP는 [그림 16]과 같이 Splunk[15] 툴을 이용하여 시스템 전반의 데이터 및 정보를 중앙 집중화하고 분석하고 모니터링하며, IT 환경에 완전히 새로운 시각을 제공한다. SPP는 Splunk 툴을 이용하여 엔터프라이즈에 존재하는 다양한 데이터 소스를 인덱싱함으로써 뛰어난 유연성을 제공하며, 결과적으로 거의 모든 시스템을 Splunk에 연결할 수 있으며, Splunk에서 데이터를 처리하게 된다. 또한 Splunk 툴은 다양한 시스템과 데이터 세트에서 작업을 수행할 수 있을 뿐만 아니라 모든 유형의 회사 규모로 확장이 가능하다. 하나 이상의 Splunk 서버를 사용하여 부하 분산 및 고가용성을 포함하여 요구 사항에 따라 시스템의 크기를 조정할 수 있는 확장성을 제공한다.

그림 16. SPP의 SIEM 개념과 다양한 데이터 소스의 인덱싱과 데이터 처리 과정

마. SIEMonster Stack AWS

SIEMonster의 고급 상관 엔진(Advanced correlation engine)은 동적 자산/필드 수집기를 사용하여 모니터링 되는 자산에 특정한 이벤트를 집계할 수 있으며, [그림 17]은 SIEMonster Stack AWS의 아키텍처를 나타낸다. 고급 상관 엔진은 주요 지표와 함께 다중 색인 데이터 집계를 사용하여 네트워크의 잠재적인 이상 증상을 분석한다. 이러한 기능을 통해 특정 자산과 관련된 모든 이벤트를 분석할 수 있으므로 보안 운영자는 비정상적인 활동에 대해 쿼리 및 경고를 발생시킬 수 있다. 키 필드는 각 이벤트 로그(event log)로부터 추출되며, 이 필드 이름은 표준화된 형식으로 수정 및 키 데이터

가 추출되어 상관 목록에 동적으로 추가되며, 이 필드에 대한 새로운 상관 색인이 작성된다. 이 목록 데이터는 쿼리의 일부로 사용되어 특정 자산을 추적하게 되며, 자산은 사용자, 서버/워크스테이션, VPN 액세스 포인트, 지리적 위치/IP 주소, 방화벽, 웹 프록시 로그 등이 될 수 있다.

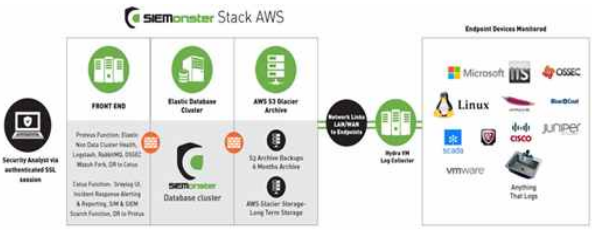


그림 17. SIEMonster Stack AWS의 아키텍처

V. 결론

최근 악성코드를 이용한 봇넷 DDoS 공격은 트래픽 규모가 막대했을 뿐만 아니라 수십만 대의 사물인터넷 기기를 악용했다는 점에서 보안 업계에 큰 충격을 주었다. 많은 보안 사고의 발생에 따라 SOC(Security Operation Center)과 SIEM(Security Information & Event Management)에 대한 많은 관심이 집중되고 있으며, 이에 따른 다양한 연구들과 정보 보안 업계의 다양한 상업화 제품들이 출시되고 있고, 이러한 상황을 반영하듯이 미국의 NIST에서는 Cybersecurity Framework에 관한 문서를 발간 및 개정을 진행하고 있다. 본 연구에서는 NIST의 Cyberseurity Framework의 고찰과 SOC 및 SIEM 보안 기술 및 솔루션의 동향에 대해 살펴보았으며, 더불어 실시간 빅데이터 보안으로 오픈소스 Apache Metron을 간략하게 소개하였다.

REFERENCES

[1] "실시간 탐지와 빅데이터 분석을 하나로 - 보안 재앙 막는 최전선 컨트롤 타워 'SIEM'," *IDG*, 2017년 1월 26일

[2] 김진보, 김미선, 서재현, "사물인터넷 서비스 접근 제어를 위한 리소스 서비스 관리 모델 구현," *스마트미디어저널, Vol. 5, no.3*, pp.9-16, 2016년 9월

[3] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," Draft Version 1.1, Jan. 10, 2017.

[4] Stef Schinag, Keith Schoon, and Ronald Paans, "A framework for designing a Security Operations Centre (SOC)," *2015 48th Hawaii International Conference on System Sciences*, 2015, pp.2253-2262.

[5] Alissa Torres, "Building a World-Class Security Operations Center: A Roadmap," *SANS*, 2015.

[6] Cisco's OpenSOC, http://opensoc.github.io/

[7] IBM's Security Operation Operating Model, http://portland.issa.org/wp-content/uploads/2015/03/IBM-SIEM-Security-and-SOC-Optimization.pdf

[8] Apache Metron, http://metron.incubator.apache.org/

[9] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *IEEE Security & Privacy*, vol. 12, no. 5, 2014.

[10] ENISA (European Union Agency for Network and Information Security), https://www.enisa.europa.eu/

[11] Mosaic Security Research, "Log Management & Security Information and Event Management (SIEM) Software Guide," *Mosaic Security Research*, (accessed May 2014).

[12] Kelly M. Kavanagh, Oliver Rochford, Toby Bussa, "2016 Magic Quadrant for SIEM," Aug. 2016.

[13] ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union), "Common Requirements of Internet of Things," Y.2066, June 2014.

[14] LogRhythm, https://logrhythm.com/.

[15] Splunk, https://www.splunk.com/.

저 자 소 개

차병래

2004년 국립 목포대학교 컴퓨터 공학과(공학박사).
2005년 3월 ~ 2009년 2월 호남대학교 컴퓨터공학과 전임강사.
2009년 9월 ~ 현재 광주과학기술원, 정보통신공학부 연구조교수.
2012년 5월~현재 제노테크(주) 대표.
<주관심분야 : 정보보안, IDS, Neural Networks, Cloud Computing, Secure VoIP, SDX 등>

최명수

2009년 목포대학교 전자공학과 공학박사
2009년 목포대학교 해양텔레매틱스기술개발센터 박사후연구원
2010년 목포대학교 정보산업연구소 연구전임교수
2015년 ~ 현재 제노테크(주) 기업부설연구소 연구소장
<주관심분야: IoT, Neural Network, Cloud Computing, VoIP, NFC>

강은주

1995년 서울대학교 수학과(이학박사)
1996년 3월~ 현재 호남대학교 정보통신공학과 교수

<주관심분야 : 코딩이론, 암호학, 정보보안 등>

박 선

2007년 인하대학교 컴퓨터정보공학과 공학박사
2008년 호남대학교 컴퓨터공학과 전임강사
2010년 전북대학교 인력양성사업단 박사후 과정
2010년 목포대학교 정보산업연구소 연구전임교수
2013년 ~현재 광주과학기술원 전기전자컴퓨터공학부 연구조교수
<주관심분야: 정보검색, 데이터마이닝, 해양IT정보융합, 클라우드 컴퓨팅, IoT, 스토리지 시스템>

김종원

1997년 University of Southern California 연구 조교수
1999년 Technology Consultant for VProtect Systems Inc.
2000년 Technology Consultant for Southern California Division of InterVideo Inc.
2001년 광주과학기술원 전기전자컴퓨터공학부 교수
2008년 ~ 현재 광주과학기술원 전기전자컴퓨터공학부 교수
<주관심분야: Future Internet, SDN & NFV, SDI>