ETRI

2013
Electronics and
Telecommunications
Trends

사이버 보안 기술 특집

빅데이터를 활용한 사이버 보안 기술 동향

Technical Trends of Cyber Security with Big Data

김종현 (J.H. Kim) 네트워크보안연구실 선임연구원
임선희 (S.H. Lim) 네트워크보안연구실 선임연구원
김익균 (I.K. Kim) 네트워크보안연구실 실장
조현숙 (H.S. Cho) 사이버보안연구단 단장
노병규 (B.K. No) 한국방송통신전파진흥원 정보보호 PM

최근 외부 해킹으로 대량의 개인정보 유출, 대규모 시스템 장애 등 사고가 빈번히 발생하고 있다. 특히, 보안체계를 잘 갖추고 있던 조직들도 APT(Advanced Persistent Threat) 공격과 같이 지속적으로 특정 표적을 목표로 하는 공격 앞에 무력하게 당하는 사건들을 접하면서 많은 기업 및 조직들이 대응 방안 마련에 고심하고 있다. 본고에서는 사이버테러, 사이버전(戰), 핵티비즘 등의 공격방법으로 활용되고 있는 사이버 표적공격 위협에 대한 방어 기술로서 최근 관심을 받고 있는 빅데이터 처리 기술을 기반으로 다중소스 데이터 수집 · 분석을 통한 지능형 보안 기술에 대한 개념과 관련 기술 및 제품의 동향에 대하여 살펴본다.

Ⅰ. 서론

최근 국내 주요 금융권 및 방송사를 타깃으로 사이버 테러가 발생하여 총 3만 2,000대의 PC가 감염되어 정상적인 서비스 제공이 어려워졌으며 이로 인한 금전적 피해도 매우 큰 것으로 보고 되었다. 이런 유형의 공격은 특정 조직을 대상으로 장기간에 걸쳐 조직적으로 중요 정보를 탈취하기 때문에 공격 노출 시 피해 규모가 매우 크며, 악성코드뿐만 아니라 사회공학적 해킹(social engineering hacking) 등 활용 가능한 모든 수단을 동원하기 때문에 사전 탐지가 어려운 것이 특징이다.

최근 몇 년에 걸쳐 국내·외에서 많은 사례가 발견되고 있으며, 2010년 7월 이란 원자력 발전시설을 해킹한 스턱스넷(Stuxnet)의 경우 원자력 발전 시설의 원심분리기 중 20%가 가동 중단되었으며, 2011년 4월 국내 농협 전산망 자료 손상, 같은 해 7월 네이트 3,500만 명 개인정보 유출 등의 공격은 피해 규모가 클 뿐만 아니라 공격 탐지가 짧게는 2개월, 길게는 몇 년이 소요된다. 이와 같이 사이버 테러의 위험성은 우리가 생각하는 것보다 훨씬 더 심각하며, 최근에는 조직적인 해커 그룹이 특정 표적을 치밀하게 계획적으로 해킹함으로써 주요 정보 유출, 제어 시스템 공격, 사이버 무기화 등을 통해 사회적 혼란을 야기하고, 나아가서는 국가 안보를 위협하는 수준에까지 이르고 있다.

이에 대한 대응을 위해서는 지능형 보안 기술로써 빅데이터 분석 기술의 통합을 시도하고 있다. IT 기술의 진화로 빅데이터와 같은 대용량 데이터를 처리할 수 있는 컴퓨팅 파워 등이 마련되어 공격 로그 이벤트 및 내부 상황정보 등을 수집하고 상관관계를 분석함으로써 공격자의 의도를 파악해 공격의 최종 목표 달성을 막아내는 기술로 발전하고 있다. 또한, 보안 이벤트 또는 네트워크 트래픽 특성인자뿐만이 아니라, 시스템/네트워크/응용 프로그램의 구성정보, 상태정보 등을 포함한 다중 소스 데이터의 특징인자까지 포함함으로써 알려지지 않은 침해사고 증상에 대한 사전 예측이 가능한 사전 대응을 위한 보안 기술이 요구되고 있다. 특히, 공격 침투 과정으로 볼 때 제로데이(zero-day) 취약점과 사회공학적인 방법을 이용하고 일련의 정상행위를 가장하는 사이버 표적공격의 특성상, 기존 시그니처 데이터베이스 기반의 탐지 기술의 한계를 극복하기 위한 새로운 개념의 사이버 공격 특성인자 추출 및 모델링 정립이 필요하다.

빅데이터와 관련된 기본 분석 기술의 활용과 더불어 보안 분야에 특화된 연관성 분석 방법론이 필요하며, 이를 지원할 수 있는 대용량 누적 데이터 저장 및 처리를 위한 저장 공간 효율화 메커니즘 및 고속 처리 알고리즘 개발 등도 필요할 것으로 본다.

본고에서는 지능화되고 있는 사이버 위협과 방어 기술의 변화에 대해 알아보고, 최근 부각되고 있는 빅데이터 처리 기술을 활용한 보안분석 기술 및 관련 제품의 동향을 살펴보도록 하겠다.

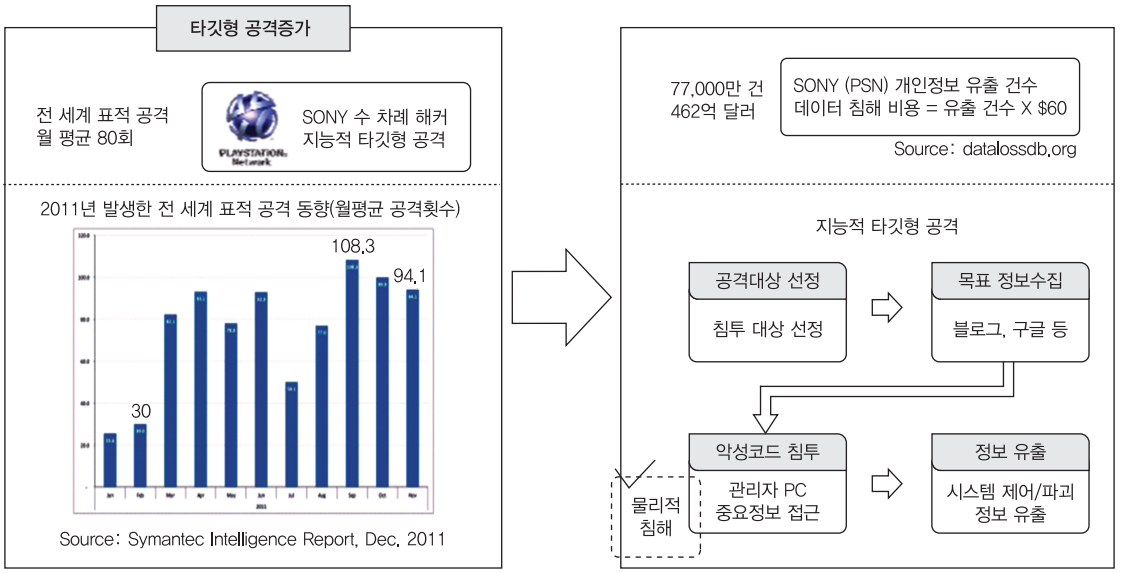
Ⅱ. 지능화된 사이버 공격과 보안 기술

1. 사이버 위협과 대응 기술의 변화

사이버 표적공격 위협이 심화되어 사회적 국가적 위험으로 야기될 것으로 예상되고 있으며, 사이버테러, 사이버전(戰), 핵티비즘 등의 공격방법으로 활용되고 있는 APT(Advanced Persistent Threat) 공격은 목표대상이 명확한 조직적 공격으로써 주로 정부나 기업을 대상으로 산업기밀이나 군사기밀, 고객정보 등의 정보 탈취를 목적으로 하고 있다.

또한, 주요 정보 유출, 제어 시스템 공격, 사이버 무기로 활용하는 사례가 전 세계적으로 확산되고 있고, 주요 정보시설을 겨냥한 사이버 표적공격 위협이 심화되어 더욱 큰 사회적 위험을 야기할 것으로 예상된다.

특히, (그림 1)에서 보듯이 전 세계 사이버 표적공격



(그림 1) 사이버 표적공격의 증가 추이

의 빈도는 월평균 80회 이상으로 보고되고 있고, 개인정보 유출 피해규모만을 보더라도 462억 달러 규모로 추정되고 있을 정도로 글로벌 기업의 주요 정보 유출이 심각한 수준에 이르렀다.

최근 해외 기업들을 대상으로 발생된 공격사례를 보면, 2011년에 미국의 글로벌 에너지 기업 5곳(쉘, 엑슨모빌, 마라톤오일, 코노코필립스, 베이커 휴즈 등)의 공격으로 가스와 석유 분야의 생산 시스템, 석유탐사 관련 제정문서, 산업 통제 시스템의 정보 유출 사고(일명: Night Dragon)가 발생하였으며, 대표적인 보안업체 중 하나인 EMC RSA가 사회공학적 기법에 의한 사이버 테러로 OTP(One Time Password) 제품인 시큐어 ID의 기밀 정보가 유출되는 사건이 발생되기도 하였다. 또한, 같은 해 7월 네이트의 데이터베이스에 저장된 3,500만 명의 개인정보 유출사고가 발생하였으며, 미국 방위산업 업체인 록히드 마틴(Lockheed Martin)을 공격한 사건을 분석 중에 국내 통신업체를 포함한 총 760여 개의 세계적으로 유명한 기업들을 대상으로 공격이 진행되었으며 이러한 공격들은 내부 개발자의 PC를 장기간 집중적으로 공격하여 내부자를 활용한 공격으로 확인되었다.

핵티비즘을 표방한 정치적 목적의 공격사례를 보면, 어노니머스(Anonymous), 룰즈섹(LulzSec) 등 핵티비즘을 표방한 공격자에 의한 침해사고가 발생 후 CEO가 사임한 미국 보안회사인 HBGary를 비롯하여 FBI, CIA 등의 정부기관, 소니 그룹의 다양한 계열사 등이 공격을 당했고, 특히 소니 PSN(Play Station Network)의 경우 1억 명의 고객정보가 유출되고, 2개월간 서비스를 제공하지 못하는 등의 큰 손해가 발생하였다.

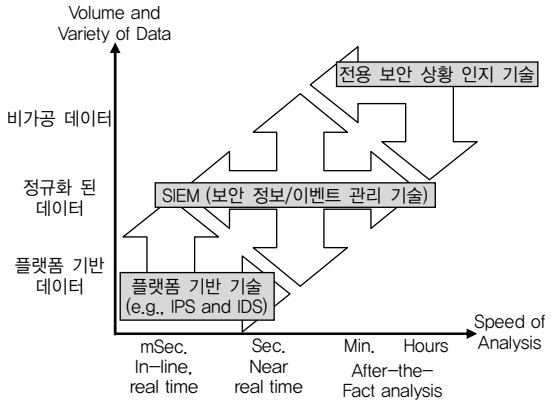
또한, 사이버 공격 무기로 발전되어 전쟁행위로서 사이버 공격이 주요 이슈로 등장하고 있으며, 스턱스넷, 듀크(Duqu) 공격 이후, 2012년 플레임(Flame)이라는 악성 프로그램의 출현으로 새로운 국면을 맞이하게 되었다. 이러한 사이버 무기는 쉽게 한 국가를 위험에 빠뜨릴 수 있기 때문에 IT 측면에서의 침해 및 데이터 유출 문제뿐만 아니라 사회적인 혼란과 물리적·인적 피해로까지 연계가 가능하다고 여겨진다. 관련 사례로서, 미국 국방부가 국가 기간 망을 위협하는 중대한 사이버 공격에 대하여 전쟁 행위로 간주하고 무력 대응할 방침이며, 송전망 차단과 같은 사이버 공격은 국가 주도 하의

공격으로 간주하며, 사실상 선전포고로서 전쟁의 구성 요건에 해당된다고 발표하였다.

이러한 사이버 위협의 새로운 방어 기술로서 보안 인텔리전스(security intelligence) 기술이 최대 이슈로 등장하고 있다. 현재까지의 사이버 위협 방어 기술은 방화벽, IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)와 같은 경계 영역 보안 제품을 비롯해 안티바이러스, 데이터베이스 암호화, 내부정보 유출방지 기술이 주류를 이루고 있으며, 이기종 보안 제품의 로그를 관리하는 통합보안 관리 기술이 적용되어 왔다. 특히, 방화벽, 침입탐지/방지 시스템 및 안티바이러스 기술은 시그니처와 블랙리스트 기반 탐지 방법을 10Gbps급의 고성능 네트워크에 적용하기 위한 high-end 플랫폼 기술 개발에 역점을 두고 있다. 예로서, 2008년도부터 10G급 고성능 IPS 솔루션들이 국내 네트워크 보안 시장에 도입되면서 고성능 처리가 가능한 보안장비가 분산 서비스 거부(Distributed Denial of Service: DDoS) 등의 대용량 트래픽 공격을 차단하고, 대용량 인터넷 인프라의 확산에 따라 인터넷서비스 사업자(Internet Service Provider: ISP), 학내 망 등을 중심으로 적용되었다.

하지만, 가트너 등의 관련 분야 예측에서도 보듯이 IDS/IPS와 같은 플랫폼 기반 분석 기술로는 APT 공격 기법에 대응하기는 역부족이기 때문에 다양한 소스의 대용량 데이터를 분석할 수 있는 전용 보안 분석 기술이 필요하며, 이는 (그림 2)에 나와 있듯이 SIEM(Security Information & Event Management) 제품 발전 방향과 일치하고 있다.

또한, IDC의 Security Software Forecast[2]에 따르면, 사이버 위협 방어 기술의 변화는 통합되고 중앙집중화된 보안관리 기술을 바탕으로 잠재적 위협을 예측할 수 있는 예측형 보안 기술이 요구되고 있으며, 보안 인텔리전스 서비스가 최대의 이슈로 등장할 것으로 예측하고 있다. 더 상세히 설명하면, 핵티비스트들에 의한 제로데이 공격, 폴리모픽 바이러스, APT 공격과 같이 보안 위협은 빠르게 다변화하고 있으며 특정 목표를 타깃으로 함에 따라, 별개로 운영되어 오던 기업의 보안 인프라들을 유기적으로 연계하여 통합 관리함으로써 보안 위협에 대한 인텔리전스를 확보하고 향후 발생될 수 있는 잠재적 위협을 예측하는 지능형 보안 기술로 발전할 것이며, 기존의 네트워크 행위 분석이나 SIEM 외에도 휴먼 인텔리전스(human intelligence), 보안 인텔리전스 전문 업체가 제공하는 위협 데이터, 휴릭스틱 엔진 등 다양한 소스로부터 발생하는 정보를 분석하여, APT와 같이 알려지지 않은 보안위협을 사전에 예측하고 방어하는데 초점을 두고 있다.

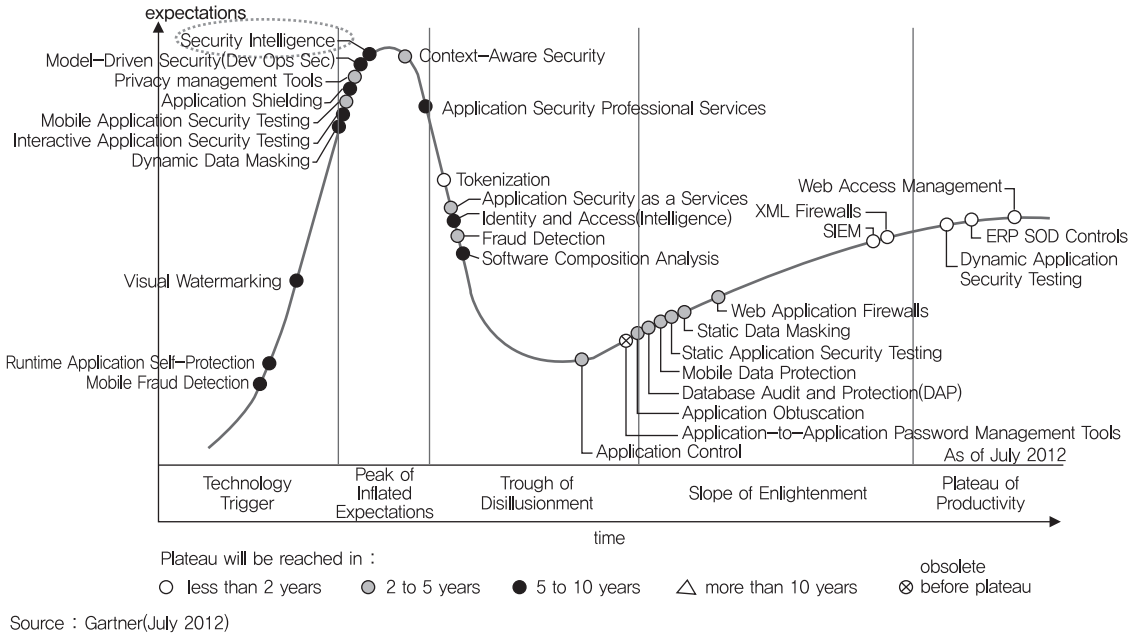


(그림 2) 사이버 보안에서 SIEM의 역할[1]

2. 지능형 보안의 개념

지능형 보안의 개념은 APT 공격과 같은 알려지지 않은 치명적인 공격에 대응하기 위해 주요 IT 기반 주요시설의 네트워크, 시스템, 응용 서비스 등으로부터 발생하는 데이터 및 보안 이벤트 간의 연관성을 분석하여 보안 지능을 향상시키는 차세대 보안정보 분석 기술로 해석되고 있다. 이는 (그림 3)의 응용보안 기술 하이프 사이클에서도 나와 있다.

IT 환경이 급변하고 있는 상황에서 더욱 은밀하고 정



Source : Gartner(July 2012)

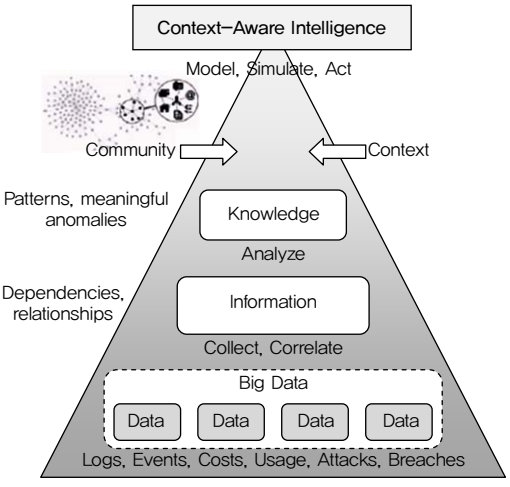
(그림 3) 응용 보안 분야의 기술 하이프 사이클[3]

교한 사이버 공격이 이루어지고 있어 기존 보안 방식이 한계를 보이므로 단순히 하나의 위협 요소를 차단하는 것이 아닌 상관관계를 파악하여 은밀하게 진행되는 공격을 탐지하는 것이 중요하다.

가트너 그룹이 정의하는 지능형 보안은 다양한 보안 기술의 상호작용을 가능하게 하는 개념과 방법론으로써 다양한 소스로부터 정보를 통합하고 상호연관성을 갖는 콘텍스트 기반의 분석 기술로 해석하고 있으며(그림 4 참조), 단기적으로는 context aware security 형태로 표현되어 향후 5년에서 10년간 지속될 보안 기술로 평가하고 있다[1].

따라서, 기존의 보안 제품들이 활용하고 있는 패턴 기반의 공격 제어 기법의 한계를 넘어서 내부 네트워크의 다양한 특성 인자들(시스템 프로세스, 활동성, 네트워크 트랜잭션 등)의 연관성 분석을 통하여 알려지지 않은 새로운 공격을 탐지하는 기술로 발전할 것으로 예측하고 있다.

표적공격 방어를 위해 네트워크 및 시스템 보안 제품군을 통합한 보안 이벤트 정보 관리기술을 제공하고 있으며, 이를 바탕으로 빅데이터 처리 기술을 활용한 지능형 보안 기술에 대한 연구가 본격화되고 있다.



〈자료〉: Gartner, Mar. 2012.

(그림 4) 콘텍스트 기반 지능형 보안을 위한 빅데이터의 활용[1]

Ⅲ. 빅데이터 분석 기술의 활용

본 장에서는 빅데이터를 활용한 보안 기술의 동향을 소개한다.

1. 빅데이터 분석 기술

다양한 응용 분야로 활용되는 빅데이터 분석 기술이 IT 분야 최대 이슈로 등장하였으며, 빅데이터를 데이터 용량에 따른 분류가 아니라 기존의 데이터베이스 처리 방식으로 해결할 수 없는 데이터의 세트로 정의하고, 이러한 데이터를 처리할 수 있는 기술이나 역량을 보유한 기업이나 국가가 미래에 경쟁력을 갖게 될 것으로 예측하고 있다. IDC의 빅데이터 관점은 데이터베이스가 아니라 업무수행에 초점을 맞춘 것으로 다양한 종류의 대규모 데이터로부터 저렴한 비용으로 가치를 추출하고 데이터의 초고속 수집, 발굴, 분석을 지원하도록 고안된 차세대 기술 및 아키텍처로 정의하고 있다. 가트너 그룹의 빅테이터 관점은 데이터 볼륨의 증가, 데이터 입출력 속도의 증가, 데이터의 다양성의 증가 등의 3가지 특징을 빅데이터의 문제로 정의하고 있다[4].

빅데이터와 관련된 각국의 활동과 공공 데이터 활용 사례를 보면, 일본의 정보폭발 프로젝트 경우에는 정보폭발이 진행되면 대량의 정보를 다루어야 하는 저장, 검색의 문제가 대두되므로 새로운 검색엔진 개발을 위한 정보관리, 융합, 활용을 위한 인프라 스트럭처와 휴먼 커뮤니케이션 인프라스트럭처 연구를 목표로 하고 있다. 미국 국토안보부의 비주얼 애널리틱스 경우는 기존의 정보 시각화 분석 이론을 결합한 것으로 전반적인 사건의 진행상황을 바로 파악할 수 있고 새로운 대처에 따라 결과가 어떻게 변하는지를 봄으로써 기존의 파악하지 못하던 안보의 위협이나 감시대상의 변화를 쉽게 인지하도록 하여 새롭게 발생할 가능성이 있는 보안문제들을 해결하는 연구에 목표를 두고 있다[5].

웹의 창시자라고 할 수 있는 팀 버너스리는 'Raw Data Now'라는 연설을 통하여 기존의 인터넷을 문서의 연결뿐 아니라 데이터의 연결을 가능하게 하자는 링크드 데이터 보급을 강조하였고, 빅데이터를 고속으로 수집, 분석하는 것으로 'forecast'보다 가까운 미래를 예측하는 'nowcast' 가 가능하다고 보고 있다[4].

다양한 응용 분야에서 데이터 분석의 기반 기술로써 활용이 가능한 빅데이터 분석의 핵심 기술들은 다음과 같다.

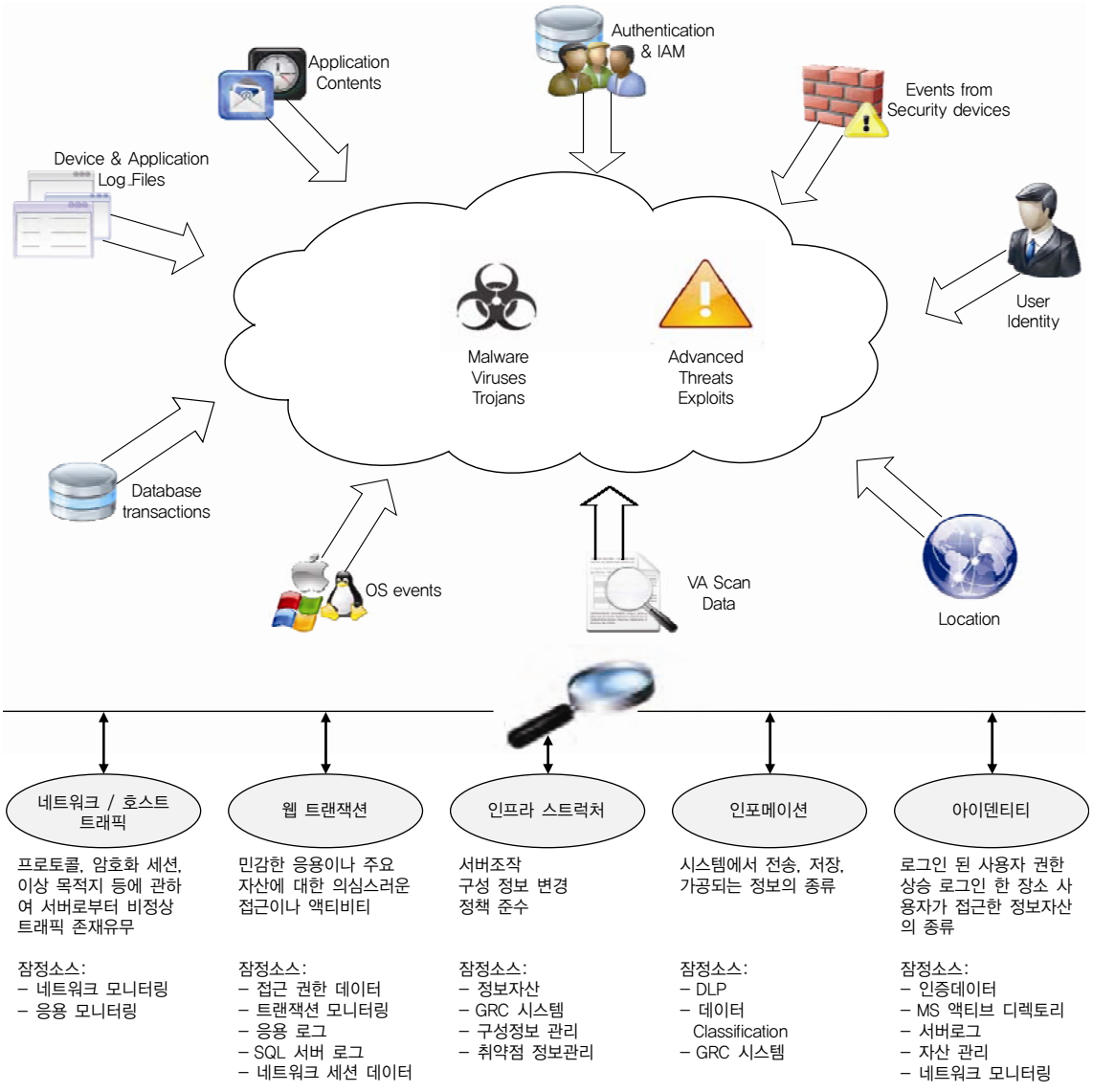
- 연관성 규칙 학습(association rule learning): 대용량 데이터베이스 내의 다양한 변수로부터 흥미있는 주제의 관련성 즉, 연관성 규칙을 찾기 위한 기술로써 잠재적 규칙을 만들어 내고 테스트하는 일련의 알고리즘으로 구성됨.
- 분류(classification): 이미 분별된 데이터를 포함하는 학습데이터 세트를 기반으로 새로운 데이터가 속해있는 카테고리를 식별할 수 있는 데이터 마이닝의 방법 중 한 기술
- 군집화(cluster analysis): 유사성에 대한 특성 등이 사전에 알려져 있지 않은 상태에서 유사한 개체들의 작은 그룹으로 분할하기 위한 통계적 방법으로써 예를 들면, 타깃 마켓팅을 위해 자기유사성(self-similarity)을 가진 그룹으로 고객을 그룹핑하는 데 사용됨.
- 데이터 융합 및 통합(fusion & integration): 단일소스에서 분석한 결과보다 더 정확하고 효율적인 통찰력을 얻기 위하여 다중 소스로부터 데이터를 통합하고 분석하는 기술
- 데이터 마이닝(data mining): 데이터베이스 관리와 통계 및 기계학습 방법을 결합하여 대용량 데이터 세트에서 특정 패턴을 추출하는 기술
- 앙상블 학습(ensemble learning): 기계 학습의 분류 방법을 통해 여러 개의 분류기(classifier)를 생성하고 그것들의 예측을 결합함으로써 새로운

가설(hypothesis)을 학습하는 방법

- 유전 알고리즘(genetic algorithm): 자연 세계의 진화과정에 기초한 계산 모델로서 최적화 문제를 해결하는 기법
- 시각화(visualization): 데이터 분석의 결과를 표현하고 이해의 수준을 향상하기 위하여 이미지, 다이어그램, 애니메이션 등에 사용되는 기술

2. 빅데이터를 활용한 보안분석 기술

빅데이터를 활용한 보안 분석(big data security analytics)은 데이터 분석 기술의 고도화 측면에서 기존에 해결하지 못한 공격위협 분석을 가능하게 할 것으로 예측되고 있다. 네트워크 경계망 보안을 우회하는 사이버 공격능력이 향상됨에 따라 지능형 보안 시스템을 통한보안 상관관계 분석을 위해서는 빅데이터를 활용한



(그림 5) 빅데이터에 기반한 보안 분석 기술[6]

보안 분석 기술 개발이 선행적으로 필요하다고 여겨지고 있다.

현재 100% 완벽한 보안은 없으며 과거의 기술과 사고의 연장선상에서 대응해서는 안되고, 보다 창의적인 보안 대응방법이 필요하며 이를 위해서는 빅데이터 분석을 중심으로 한 지능형 보안 시스템 구축이 필요하다. 가트너 그룹에서는 빅데이터 분석을 활용한 보안 분석을 통하여 예전에 보이지 않았던 사고패턴을 발견하고, 정보 보안을 포함한 기업경영에 대한 선명한 통찰력을 제공함으로써 기업의 비즈니스 가치를 높일 수 있다고 예측하고 있다[5]. 과거 사이버 위협 방어 기술의 핵심 기술은 알려진 공격에 대한 공격 시그니처 데이터베이스를 확보하고 고성능 패턴매칭 알고리즘을 구현하여 얼마나 빨리 비교할 수 있느냐에 달려 있었지만, 복합 데이터 처리 기술의 발달로 내부 망에서 발생하는 다중 소스의 누적 데이터에 대한 특성인자를 정의하고 연관성 분석을 할 수 있는 보안 기술로서 빅데이터를 활용한 보안 분석 기술이 부각되고 있다.

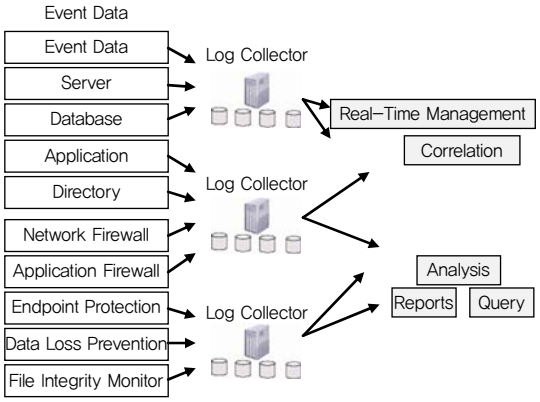
앞에서 언급한 빅데이터를 활용한 보안 분석 기술은 다음과 같다((그림 5) 참조).

- 실시간 모니터링(real-time monitoring): 시스템 구성요소에 대한 공격상황을 추적하고 분석하거나 응용 프로그램 상에서 사용자의 활동성을 모니터링하기 위하여 다양한 소스로부터 데이터를 수집 관리하는 기술
- 위협에 대한 지능(threat intelligence): 비정상적인 활동을 보다 정확히 인식할 수 있게 하는 다양한 위협과 공격 패턴에 대한 최신 정보 체계이다. 예로서, 외부 IP에 대한 소량의 outbound 트래픽이 정상 트래픽으로 위장되어 간과될 수 있는 경우에 이를 공격 제어와 관련된 위협 정보로 인지하는 기술
- 행위 프로파일링(behavior profiling): 비정상에 대한 조건들이 잘 정의되어 있을 경우에 일련의 특정 조건들을 찾기 위한 연관 규칙을 정의하는 것이 가능하며, 규칙기반 방법론으로는 모든 비정상 행위를 탐지하기 힘들기 때문에 행위 프로파일링 기반의 이상징후(anomaly) 탐지분석은 주요 기술 중 하나임.
- 데이터 및 사용자 모니터링(data & user monitoring): 사용자 및 데이터의 콘텍스트를 포함한 데이터/사용자의 활동성을 모니터링하는 것은 침투 탐지 및 오용 탐지에 필수 기술이며, 특권 사용자와 민감한 데이터 접근을 모니터링 하는 데 기본적으로 요구
- 응용 모니터링(application monitoring): 응용 프로그램의 취약점은 표적공격의 주요 타깃이므로 비정상 응용 프로그램의 활동성 모니터링 기술
- 분석(analytics): 빅데이터 분석의 전통적인 방법론인 머신러닝, 데이터 마이닝, 네트워크 마이닝 기법 등을 활용하여 다양한 소스 정보의 특성을 분석하고 이상 유무를 판단하는 빅데이터 보안 분석의 핵심 기술

Ⅳ. 지능형 보안 기술 및 제품 동향

1. 관련 기술 동향

최근 지능형 사이버 보안 기술은 다양한 소스의 대용량 데이터를 활용하여 네트워크 및 시스템 이벤트를 하나의 연동된 보안 인프라로 구성하는 통합 보안관리 기술을 목표로 하고 있다. 빅데이터 분석 기술을 활용한 내부자 행위 분석 기술에 대한 연구와 제품 개발이 본격화되었으며, 보안 인텔리전스를 위한 빅데이터 분석 기술 도입은 Splunk를 비롯한 SIEM 선두주자들이 새로운 공격 위협에 대응하기 위한 새로운 기술로 활용되고 있다[7]. 특히, SIEM 기술이 대표적인 통합 보안 관리 기술로써 내부 망에 대한 위협 상황 감시 기능을 제공하



(그림 6) SIEM 의 전형적인 구조도[8]

고 내부행위 감시기술로써 연구가 활성화되고 있으며, 내부 다중 영역 트랜잭션의 정보 흐름 분석을 통한 프로파일링 기반 이상행위 감시 기술은 국외에서도 연구개발 초기 단계이다[8].

또한, (그림 6)에서 보듯이, SIEM은 방화벽, IDS/IPS, 안티바이러스 등의 보안장비와 서버, 네트워크 장비 등으로부터 통계 정보, 보안 이벤트 정보를 함께 가져와서 이들 정보 들 간의 연관성 분석을 통해 보안 상황 인지, 신속한 사건 대응과 로그 관리를 수행하는 기능을 제공한다 .IT 및 보안 환경이 복잡해지면서 보안 정보 및 이벤트 관리 솔루션은 조직 내의 보안 인프라에서 필수 요소로 부상하고 있고 SIEM은 효율적인 통합 로그 관리, 위험탐지, 사고대응, 포렌식(forensic) 및 보안 관련 컴플라이언스에 중요한 역할을 담당할 것이다.

이와 관련된 해외 프로젝트는 사이버 표적공격 심화와 기존 보안 기술의 문제 해결을 위해 2010년부터 미국 DARPA에서는 내부자 행위 분석을 위한 CINDER (Cyber-INsiDER) 프로그램을 진행하고 있으며, 혁신적인 사이버 방어 및 사고검출 기술을 개발하기 위한 사이버 보안 기반기술로써 사이버 게놈(cyber genome)을 정의하고 응용 소프트웨어, 데이터의 흐름, 사용자들 간의 상관관계와 그 속성을 식별 및 표현하는 기술에 대한 연구를 진행하고 있다[9],[10].

또한, 사이버 보안의 중요성이 강조되면서 국가적 프로젝트로서 2010년 사이버 보안 강화법 수정안(Cyber Security Enhancement Act of 2010)을 발표하고 최근에는 실전투입용 사이버무기 개발을 위한 대규모 프로젝트 '플랜 X'를 추진 중에 있다. 미국 정부가 '플랜 X'에 돌입하게 된 것은 미국 군부의 심장부라 불리는 록히드 마틴이 해킹공격을 받아 군사기밀이 대량 유출되어 자국 국방기밀에 대한 위협이 있다고 판단되었기 때문이다. 이 프로젝트는 대규모 사이버 전력증강 계획으로서 2017년까지 많은 예산을 투입하여 추진할 계획이다.

2. 관련 제품 동향

SIEM의 전문기업들은 글로벌 대표 기업에 인수 합병되어 보안 토털 솔루션을 제공하는 형태의 글로벌 트렌드로 진화하고 있으며, ArcSight를 인수한 HP, Q1 Labs를 인수한 IBM, NitroSecurity를 인수한 McAfee 등이 대표기업으로서 관련 제품을 출시 중이며 특히, Splunk와 같은 신생 기업이 빅데이터 분석 기술을 이용한 지능형 보안 솔루션을 통해 시장 점유율을 높여가고 있다.

가. IBM의 QRadar

강력한 SIEM 기술을 제공하는 Q1 Labs를 인수한 IBM은 QRadar를 all-in-one 솔루션으로 적용하여 다양한 소스의 수집과 네트워크 및 응용계층의 행위 분석을 제공하며, NetFlow 데이터 처리와 소스로부터 수집된 모든 이벤트를 포함하는 정밀 분석까지 가능하다. 또한, 기업 내부 시스템에 대한 신종 바이러스의 침투, 정보 유출 및 위변조 등과 같은 보안 사고에 대한 해결책을 제시하고 있다[11].

나. McAfee의 ESM

McAfee는 NitroSecurity를 인수하여 SIEM 시장에 진출하였고 McAfee ESM(Enterprise Security Management)은 in-line 네트워크 모니터링을 수행하는

SIM(Security Information Management)과 SEM (Security Event Management) 기능을 통합한 어플라이언스 제품으로, 데이터 및 보안 이벤트에 대한 응용 프로그램 콘텍스트 및 콘텐츠를 얻기 위해 DPI(Deep Packet Inspection) 기능을 수행하며, 이벤트 정보와 보안 정보를 수집하고 연관성 분석을 할 수 있는 통합보안관리 기능을 제공하고 있다[12].

다. HP의 ArcSight SIEM

HP ArcSight SIEM 플랫폼은 보안 및 위험 정보를 수집, 분석 및 평가하기 위한 통합보안관제 제품이다. 또한, 부분적으로 상관관계 분석 최적화, 저장 및 검색 엔진으로 오라클 데이터베이스를 대체하여 자사의 중소 고객을 위해 단순화된 DB 엔진을 제공한다. ArcSight SIEM 플랫폼은 기업 이벤트 정보를 수집, 분석, 관리하기 위한 통합 시스템으로써 각종 센서로부터 수집한 이벤트 정보를 효율적인 검색, 상호 연관성 분석, 통계보고를 위해 하나의 구조체 형식으로 정규화하는 기능을 제공한다[13].

라. Splunk

Splunk는 대부분 가용성 중심의 로그 관리와 분석을 제공하기 위해 IT 운영과 응용 프로그램 지원 분야 등에 적용되고 있지만, 기업 보안 모니터링과 분석, 사용 케이스(use case)를 지원하도록 미리 정의된 함수를 제공하기 위해 Splunk 실시간 상호 관계, 그리고 Splunk 애플리케이션 등을 제공하고 있다.

Splunk는 SIEM 제품과의 통합을 통하여 엔터프라이즈 인프라의 완벽한 모니터링 기능을 제공하고 심층적인 연관성 분석을 위해 정보의 일부를 SIEM과 연동하여 처리하는 구조를 제시하고 있다[14].

V. 결론

최근의 사이버 테러는 과거처럼 몇몇 해킹 집단의 과시용 행위가 아닌 사회적 혼란을 야기하고 국가 안보를 위협하며 개인에게 금전적으로 피해를 주는 등 다양한 목적으로 자행되고 있다. 따라서 우리는 보안 문제점 및 사고 대응 방법에 대한 인식을 새로이 해야 한다. 앞으로, 다양한 사이버 테러 기법 분석과 연구 등을 통해 피해를 줄이거나 이를 원천 봉쇄할 수 있는 지능형 보안 기술로써 빅데이터 분석 기술의 통합을 시도하고, 공격 로그 이벤트 및 내부 상황정보 등을 수집하여 상관관계를 분석함으로써 공격자의 의도를 사전에 인지하고 차단할 수 있는 보안 기술이 요구되어야 한다.

또한, APT 공격에 대한 대응을 위해서는 조직 내부 구성원들의 체계적인 대응이 무엇보다 중요하다. 이를 위해 조직에서 운영하는 보안 솔루션도 각각의 기능을 갖는 개별 보안 솔루션들의 운영 조합이 아닌 조직 내 보안 체계 분석을 통한 보다 체계적이고 고도화된 개념의 지능형 보안 솔루션을 구성하고, APT 공격을 막기 위한 예방 및 대응이 필요하다.

국내외 주요 기업 및 제품 특성을 분석한 결과, 해외 주요제품의 지능형 보안 분석 기술에 비하여 국내 기술의 경쟁력이 현저히 낮은 상태이므로 국내에서도 지능형 보안 분석 기술에 대한 연구 개발이 조속히 필요한 시점으로 판단된다.

용어해설

APT 공격 특수한 목적을 가진 조직이 하나의 표적에 대해 다양한 IT 기술을 이용하여 지속적으로 정보를 수집하고 취약점을 파악하여 이를 바탕으로 피해를 끼치는 공격

핵티비즘(hacktivism) 정치 · 사회적 목적으로 이루기 위해 해킹하거나 목표물인 서버 컴퓨터를 무력화하고 이런 기술을 만드는 운동. 해커(hacker)와 정치행동주의를 뜻하는 액티비즘(activism)의 합성어로 단순히 컴퓨터 보안장치를 풀고 침입하는 해커와는 차이가 있음. 핵티비즘의 특징은 항상 정치적 동기를 포함한다는 것, 정부정책의 급속한 변화를 강력히 요구한다는 것, 심각하지 않은 탈법을 지향한다는 것, 비폭력주의로 제 3자를 위협에 노출시키지 않는다는 것 등이 있음.

약어 정리

APT	Advanced Persistent Threat
CINDER	Cyber-INsiDER
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DPI	Deep Packet Inspection
ESM	Enterprise Security Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISP	Internet Service Provider
OTP	One Time Password
PSN	Play Station Network
SEM	Security Event Management
SIEM	Security Information & Event Management
SIM	Security Information Management
SVM	Security & Vulnerability Management

참고문헌

[1] M. Nicolett and K.M. Kavanagh, "Magic Quadrant for Security Information and Event Management," Gartner Group, May 2012.

[2] IDC, "Korea Security Software 2012-2016 Forecast Update 2011 Review," May 2012.

[3] J. Feiman, "Hype Cycle for Application Security, 2012," Gartner Group, July 2012.

[4] J. Manyika et al., "Big Data: The Next Frontier for Innovation, Competition, and Productivity," Mckinsey Global Institute, May 2011.

[5] N. MacDonald, "Information Security Is Becoming a Big Data Analytics Problem," Gartner Group, Mar. 2012.

[6] S. Curry et al., "Big Data Fuels Intelligence-driven Security," RSA Security Brief, Jan. 2013.

[7] M. Nicolett and K.M. Kavanagh, "Critical Capabilities for Security Information and Event Management," Gartner Group, May 2012.

[8] M. Nicolett and J. Feiman, "SIEM Enables Enterprise Security Intelligence," Gartner Group, Jan. 2011.

[9] "R&D Support of DARPA Cyber Genome Program," General Dynamics, Mar. 2010. http://publicintelligence.net/hbgary-general-dynamics-darpa-cyber-genome-program-proposal/

[10] Wikipidia, Cyber Genome Project. http://wiki.echelon2.org/wiki/Cyber_Genome_Project

[11] IBM, http://www-01.ibm.com/software/tivoli/products/security-operations-mgr/

[12] McAfee, http://www.mcafee.com/us/products/siem/

[13] HP, http://www8.hp.com/us/en/softwaresoluions/

[14] Splunk, http://www.splunk.com/