정 보 보 호 학 회 지
제23권 제6호, 2013. 12

보안관제 기술동향 조사 및 차세대 보안관제 프레임워크 연구

신 휴 근*, 김 기 철**

요 약

최근의 사이버 위협은 공격자에 의해 지속적이고 지능화된 위협으로 진화하고 있다. 이러한 위협은 장기간에 걸쳐 이루어지기 때문에 보안체계를 잘 갖추고 있는 회사라 하더라도 탐지하는데 한계가 있다. 본 논문에서는 차세대 보안관제 프레임워크의 지향점을 네트워크 가시성 강화, 상황인식 기반 지능형 보안관제, 관련 업무조직과의 정보 통합 및 협업 강화로 제시하고 있으며 구조적, 수집·파싱, 검색·분석, 이상 탐지 등 총 9개 관점에서 이를 지원하는 필요 기술들을 분류하였다. 아울러 침투 경로 및 공격 단계와 내부 자원 간 연관성 분석을 통한 수집 정보 범위 설정, 사례 기반 상관분석 규칙 생성·적용, 정보연동, 업무처리, 컴플라이언스, 조사 분석 등 지원 기능의 연계를 보안관제 모델링의 필요 요소로 도출하였다.

Ⅰ. 서 론

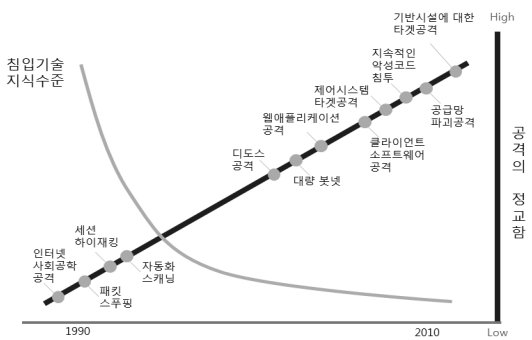
최근의 사이버 공격은 APT(Advanced Persistent Threat)로 알려진 지속적이고 지능화된 위협으로 진화하고 있다. APT 공격은 특정 회사를 공격 목표로 표적 공격과 국가 기밀 데이터 탈취를 목적으로 하는 사이버 스파이 활동, 그리고 정치·사회적 목적의 해킹인 핵티비즘(hacktivism) 등 다양한 목적으로 이용되고 있다. 이러한 위협은 정찰, 무기화, 유포, 악용 및 설치, 명령제어의 공격 절차로 장기간에 걸쳐 수행되고 백신, 침입탐지시스템 등 기존의 보안체계로는 탐지되지 않도록 치밀하게 준비되기 때문에 보안체계를 잘 갖추고 있는 회사라 하더라도 대응하기가 어렵고 공격에 무력화되고 있다.

본 논문의 목적은 사이버 위협에 대응하기 위한 전통적인 보안관제 방식의 한계점을 파악하고 새로운 보안관제 모델링을 제시하여 진화하는 사이버 위협을 효과적으로 탐지하고 대응하는데 있다.

Ⅱ. 관련 동향

2.1. 사이버 위협의 진화

카네기멜론 대학교의 연구[1]에 따르면 1990년대의 인터넷을 이용한 사회공학 공격, 패킷 스푸핑, 세션 하이재킹, 자동화된 스캐닝 등의 전통적인 사이버 위협이 2010년에 진입하면서 표적형 공격으로 진화하고 있다. [그림 1]에서 보는 바와 같이 클라이언트 소프트웨어



〔그림 1〕 공격의 정교함과 침입기술 지식수준의 관계
(출처: 카네기멜론대학 재구성)

* 금융결제원 금융정보보호부 (hkshin@kftc.or.kr)
** 금융결제원 금융정보보호부 (jeterkim@kftc.or.kr)

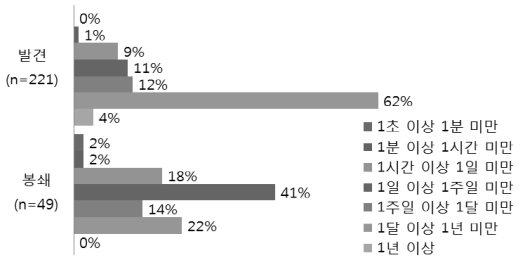
공격, 제어시스템 타겟 공격, 지속적인 악성코드 침투, 공급망 파괴 공격 등 흔히 APT로 알려진 지속적이고 지능화된 사이버 위협으로 발전하였고 2010년 이후로는 국가 주요 핵심시설을 공격 목표로 정교화된 사이버 위협으로 발전할 것으로 예측하고 있다.

실제 최근 국내·외에서 발생한 사이버 공격은 [표 1]과 같이 공격 준비기간만 수개월이 소요되는 등 은밀하고 정교해지고 있어 회사 내부에서 기존의 방식으로 공격을 탐지하기란 더욱 어려워지고 있다[2].

국내 금융·방송사를 대상으로 정교하게 계획된 3.20 전산장애사고 뿐만 아니라 해외에서 발생한 APT공격도 이와 같은 방법으로 이루어졌다. 오퍼레이션 오로라(Operation Aurora, 2010), 스턱스넷(Stuxnet, 2010), RSA OTP해킹(2011), 엘더우드 프로젝트(Elderwood Project, 2012), 레드 옥토버(Red October, 2012) 등이 대표적인 APT 공격 사례이다.

〔표 1〕 킬 체인(Kill Chain) 공격 단계 분류

공격 단계	수행 내용
정찰	- 공격자의 정체를 노출하지 않고 목표 대상에 대한 정보를 정찰하는 단계 · 이메일 주소, 연락처 및 기타정보에 대한 인터넷 검색 예) 컨퍼런스 프로시딩, 메일링리스트 등 · 사회적인 관계에 대한 소셜 네트워크 서비스 이용 · 핵심 이니셔티브 및 인력에 관한 회사 홈페이지 정보 참조 등
무기화	- 자동화된 공격 도구를 이용하여 원격 접근 트로이잔 등의 악성코드를 유포 가능한 상태로 제작하는 단계 · Adobe PDF, MS 오피스 파일 등
유포	- 목표 대상에게 무기화 단계에서 제작된 악성코드를 전달하는 단계 · 이메일 첨부파일, 홈페이지, USB, 애플리케이션 취약점 등이 주로 이용
악용 및 설치	- 목표 대상에게 악성코드가 전달된 후 공격 코드를 실행되는 단계 · 추가 악성코드 다운로드, 권한 상승 시도, 인증 정보 추출 등
명령제어	- 명령제어서버(C2)와 연결을 맺기 위한 단계 · 대부분의 APT 악성코드는 자가 작동하기보다는 공격자의 지령을 받아 공격 명령을 수행함 · 공격자는 동 단계를 통해 목표 대상에 대한 완벽한 제어권을 획득함 · 명령제어서버의 명령은 HTTP, HTTPS를 통해 전달됨
목표 직접공격	- 목표 대상에게 목적 달성을 위한 공격을 수행하는 단계 · 데이터 유출, 무결성 및 가용성 훼손, 타 기관 공격을 위한 중간경유지 활용 등



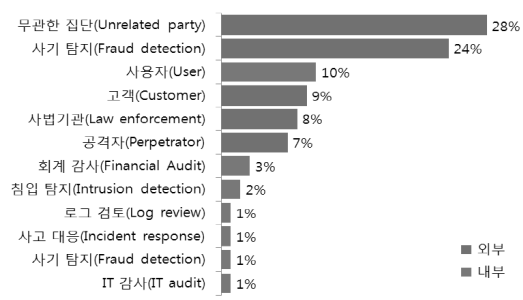
〔그림 2〕 발견, 봉쇄까지 걸린 시간

2.2. 현 보안체계의 한계

[그림 2]에서 보는 바와 같이 미국 Verizon社의 "2013년 데이터 유출사고 분석보고서(Data Breach Investigation Report, 2013 DBIR)"에 따르면 데이터 유출을 발견하기까지 한 달 이상 걸린 경우가 66%나 차지하였고 심지어 1년 이상 걸린 경우도 전체의 4%를 차지하였다[3].

또한 [그림 3]과 같이 데이터 유출사고의 약 76%정도가 외부 조직에서 발견되었고, 피해조직의 내부에서 발견된 비율 중 절반 이상이 최종 사용자에 의해 발견되었다. 이를 통해 많은 조직에서 시간과 돈을 투자하고 있는 탐지 방법들이 데이터 유출사고를 발견하는데 큰 도움이 되지 않고 있음을 알 수 있다.

국내의 경우도 마찬가지로 천만여명 이상의 고객정보를 유출한 옥션 사고(2008), SK컴즈 사고(2011)는 보안관제 체계의 부재로 인해 발생한 사고가 아니다. 대형사고 경험의 부족에서 기인한 문제로 볼 수도 있지만 관제 대상과 범위가 주로 네트워크 영역으로 한정되어 있고 외부로부터 유입되는 공격에 대한 모니터링에 집



〔그림 3〕 데이터 유출사고 발견 주체

중하는 보안관제 체계가 사고의 원인으로 파악되었다. 즉 내부PC를 대상으로 하는 공격이나, 패턴기반의 탐지를 우회하는 알려지지 않은 취약점을 이용한 APT공격, 사회공학적 공격 등에는 한계를 보인 경우이다.

2.3. 보안관제 기술의 발전

2.3.1. 솔루션 관점

인터넷기반 업무에 대한 보안 위협이 증가하게 된 1990년대 말부터 2000년 초반까지 침입탐지시스템(Intrusion Detection System), 침입방지시스템(Intrusion Prevention System) 등의 로그를 모니터링하게 되면서 보안관제가 본격적으로 시작되었다. 모니터링 대상 시스템과 로그가 증가하면서 이기종간의 로그를 통합 분석할 필요성이 증가하였으며 이 때 등장한 솔루션이 통합보안관리시스템(ESM)이다.

보안관제서비스는 패턴 기반의 실시간 탐지를 목적으로 하는 ESM과 통계 위주의 전체 로그 분석을 주된 목적으로 하는 SEM으로 구분되었으나 주로 ESM을 기반으로 본격적으로 성장하게 되었다. 이 후 국내에서는 외부의 위협을 내부와 연계해서 모니터링하는 위협관리시스템(TMS), 대시보드 형태의 분석화면을 제공하는 종합분석시스템 등이 등장하여 ESM을 보완해주는 역할을 하였으며 해외에서는 2000년대 중반부터 SEM과 SIM이 합쳐진 SIEM 솔루션이 본격화되어 현재까지 차세대 솔루션(NG-SIEM)으로 진화하고 있다.

향후 SIEM 솔루션은 차세대 보안 패러다임으로 부각되고 있는 시큐리티 인텔리전스(Security Intelligence)로 발전될 가능성이 높다. 가트너에 따르면 시큐리티 인텔리전스는 다양한 보안기술의 상호작용을 가능하게 하는 개념과 방법론으로써 다양한 소스로부터 정보를 통합하고 상호연관성을 갖는 상황(Context) 기반의 분석 기술로 해석되고 있다[4]. EMC RSA社는 과거의 기술과 사고의 연장선상에서 대응해서는 안되고, 보다 창의적인 보안 대응방법이 필요하며 이를 위해 빅데이터 분석을 중심으로 한 지능형 보안 시스템 구축의 필요성을 강조하였고 가트너는 빅데이터를 활용한 보안 분석기술을 통해 예전에 보이지 않았던 패턴을 발견하게 되고, 기존에 해결하지 못한 부분을 가능하게 하여 비즈니스의 가치를 높일 수 있다고 예측하고 있다[5][6].

2.3.2. 모니터링 대상 관점

과거 SIM 솔루션은 IT단위시스템의 장애처리를 위한 모니터링용으로 활용되었으며 각 시스템의 로그를 수집하고 분석하는데 중점을 두었다. 이후 SEM, ESM 솔루션의 등장으로 다양한 로그를 통합한 이기종 시스템들의 상관분석을 통해 알려진 위협에는 대응할 수 있었으나 최근에는 APT공격 등 알려지지 않은 공격이 주로 발생하게 되어 탐지가 어려워지게 되었다. 이때 새로운 대응 방식으로 시큐리티 인텔리전스라는 개념이 등장하게 되었다.

시큐리티 인텔리전스는 빅데이터 기반의 상황정보 분석 및 모니터링으로 유용한 정보를 찾아낼 수 있는 기술적 개념이다. 상황정보는 실세계에 존재하는 실체의 상태를 특징화하여 정의한 정보이며, 상황 인식(Context-Awareness)은 이러한 상황 정보가 상호 작용하여 현재 상황을 특성화할 수 있는 기술적 방법을 의미한다. 일반적인 상황 정보는 사용자 상황, 물리적 환경 상황, 컴퓨팅 시스템 상황, 사용자-컴퓨터 상호 작용 이력 등으로 분류할 수 있다[7].

가트너에서 예측하는 응용 보안기술의 하이프 사이클에서도 시큐리티 인텔리전스를 향후 5년에서 10년간 지속될 기대 기술로 예측하였다. 상황인식 보안(Context-Awareness Security) 역시 기대 기술로 회사의 입장에서는 이러한 기술들을 실제와 연계하여 다뤄볼 시급성이 요구되는 상황으로 분석할 수 있다[8].

시큐리티 인텔리전스로의 변화는 과거·현재의 가시화로부터 미래 예측으로의 진화를 의미한다. 미래 예측에는 대량의 데이터로부터 지식이나 유익한 규칙을 자동으로 학습하는 데이터 마이닝 기술이 유용한데, 시스템 단가의 하락, 하둡(Hadoop)의 등장, 클라우드 컴퓨팅 이용의 보편화로 인해 미래를 예측하기 위한 데이터 마이닝 기술의 구현이 가능해지고 있다.

2.3.3. 방어 전략 관점

최근의 정교화된 보안 위협은 정보보호솔루션을 네트워크 경계에 배치하거나 내부 자산에 엔드포인트 솔루션들을 배치하여 대응하는 단층적인(One Layer) 방안으로는 실효성을 거두기가 어렵다. 결국 효과적인 정보보호솔루션의 조합, 중요 시스템과 데이터에 대한 접근 차단 등과 같은 기술적인 보안과 더불어 정기적인

〔표 2〕 계층 방어 예시

공격 유형	공격 예시	1계층 방어	2계층 방어
수동적 공격	네트워크 스니핑	네트워크 암호화	애플리케이션 보안
능동적 공격	악성코드 삽입, 서비스 거부 인증정보 가로채기	경계선 보안	컴퓨팅 환경 방어
내부 공격	비인가 정보 접근, 수정, 파괴	물리적, 인적보안	접근통제, 감사
근접 공격	물리적으로 근접한 곳에서 공격	물리적, 인적보안	기술적 감시
배포 공격	악성코드가 탑재된 S/W 배포	신뢰된 S/W 배포	무결성 검증

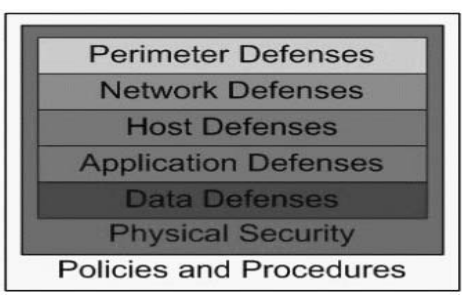
보안 인식 교육, 시스템 사용에 대한 명문화된 보안 지침 등과 같은 정책적인 보안이 상호 보완 해주는 구조로 정보보호 프로세스가 확립되어야한다[9].

계층 방어(Defence in Depth)는 미국 국가보안국(NSA)에서 2002년 9월 지침서[10]를 제작하여 배포하면서 소개되었다. 이 지침서에 따르면 공격자의 공격 유형은 수동적 공격, 능동적 공격, 내부 공격, 근접 공격, 배포 공격의 5가지로 분류할 수 있으며 각각의 공격 유형에 따른 계층 방어 예제 등은 [표 2]와 같다.

또한 계층 방어를 성공적으로 구현하기 위해서는 3가지 주요 방어 요소인 사람(People), 기술(Technology), 운영(Operation)이 유기적으로 상호작용하여야 함을 소개하고 있다.

현재에 이르러 계층 방어는 보안 아키텍처의 기본 구조로 자리 잡게 되었으며 [그림 4]와 같은 형태의 계층형 방어 체계를 구축하는 것이 일반화되어 있다.

퍼리미터, 네트워크, 호스트, 애플리케이션, 데이터의 5가지 방어 체계는 물리적 보안과 보안정책이 기반이 되어야 비로소 계층 방어의 모델로 완성된다. 5가지의



〔그림 4〕 Defense in Depth 보안 모델

방어 체계는 다음과 같이 각각의 계층에 필요한 보안 솔루션을 설치하거나 보안 기술을 이용하여 구현할 수 있다[11].

- 퍼리미터(Perimeter) 방어: 내부 네트워크와 신뢰되지 않은 외부 네트워크의 인터페이스 지점으로 인터넷, 비즈니스 파트너, 가상사설망, 전화선 등의 네트워크 퍼리미터가 포함됨. 라우터, 방화벽, 네트워크 침입탐지시스템, 프록시 서버, 원격접근서버 등을 설치하여 방어
- 네트워크(Network) 방어: 내부 네트워크를 보호하기 위해 무선랜 보안, IPSec, 네트워크 세그먼트 기술을 사용하여 보안성, 가용성, 확장성, 관리성, 신뢰성 등의 서비스를 제공
- 호스트(Host) 방어: 서버보안, 개인방화벽, 패치관리시스템, 안티바이러스, 감사로깅 등의 보안 솔루션을 설치하여 클라이언트 및 서버를 방어
- 응용프로그램(Application) 방어: 웹서버, DB서버, 이메일서버 등을 보호하기 위해 웹 방화벽, DB보안, 메일서버 보안 등의 솔루션을 설치하거나, 소프트웨어 개발 보안 등을 통해 중요자료에 접근 가능한 응용프로그램을 방어
- 데이터(Data) 방어: 접근 통제, 무결성 검증, 암호화, 백업 등을 통해 시스템에 저장되어 있는 중요자료를 방어

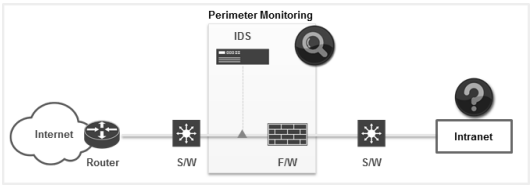
계층형 방어 체계가 기술적, 시스템적으로 완벽히 구축되었더라도 운영중에 발생할 수 있는 시스템 오류, 휴먼 에러들이 예측할 수 없는 곳에서 발생할 수 있다. 따라서 모든 상황 정보를 수집하고 정기적으로 분석하는 추가적인 절차가 필요하며 이를 보안관제 시스템과 연동해야 한다. 즉 시스템 현황을 한눈에 파악할 수 있어야 하며 접근 통제 정책, 사용자 인증 정책, 물리적 보안 등이 5가지 방어 체계에서 생산하는 다양한 로그와 함께 연동되어야 계층 방어 체계가 성공할 수 있다.

Ⅲ. 보안관제 프레임워크

3.1. 보안관제 고도화 방향

3.1.1. 네트워크 가시성(Visibility) 강화

[그림 5]에서 보듯이 퍼리미터 보안관제는 네트워크



〔그림 5〕 퍼리미터 보안관제 네트워크 구성

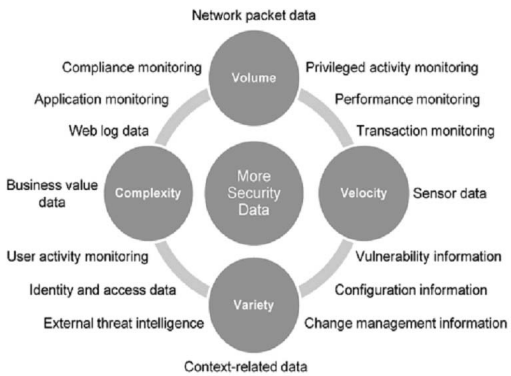
기반으로 동작하는 정보보호솔루션을 네트워크 경계에 배치하여 내부 자산에 대한 침해 행위에 대응하는 전통적인 방어 방식이다. 침투 및 공격 방식이 비교적 단순했던 과거에 내부 자산의 구성 환경이 복잡하지 않은 작은 기업에서 적용할 수 있는 방식이나 진화된 공격 방법을 복합적으로 사용하는 최근의 보안 위협에 대해서는 효과적인 보안관제 방식으로 보기는 어렵다.

네트워크 경계 영역과는 다르게 내부 네트워크는 그 구조가 매우 복잡하며 업무의 가용성 확보가 우선시되어 접근 제어를 통제하는 방화벽 외에 추가적인 보안솔루션이 부족한 상태이며 존재하더라도 엔드포인트 솔루션들이 주로 배치되어 있는 상태이다.

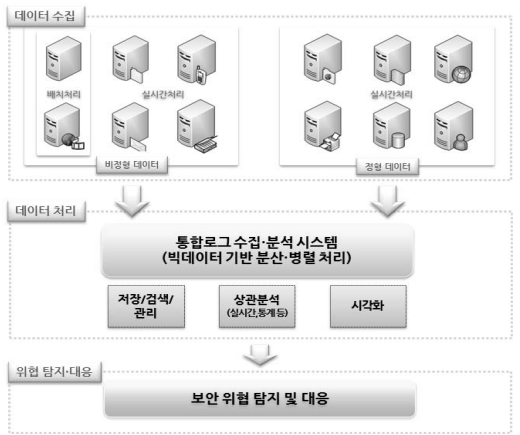
퍼리미터 보안관제 방식을 채택한 기업은 공격자가 퍼리미터 방어선을 우회하게 되는 경우 내부 네트워크에서 발생하는 어떤 이상 징후도 포착할 수 없는 네트워크 가시성이 매우 낮은 상태라 할 수 있다.

경계와 내부를 포함한 네트워크 전반에 대한 가시성을 강화하기 위해서는 네트워크 곳곳의 상태를 파악할 수 있는 다양한 정보의 수집이 필요하다. 해당 정보는 보안솔루션 로그에 국한되지 않으며 [그림 6]과 같이 네트워크 시스템, 서버, 애플리케이션 등 다양한 자원에서 산출되는 정보가 그 대상이 될 수 있다.

하지만 많은 기업의 IT 보안조직은 보안 로그를 제외



〔그림 6〕 보안관제를 위한 정보의 확대[12]

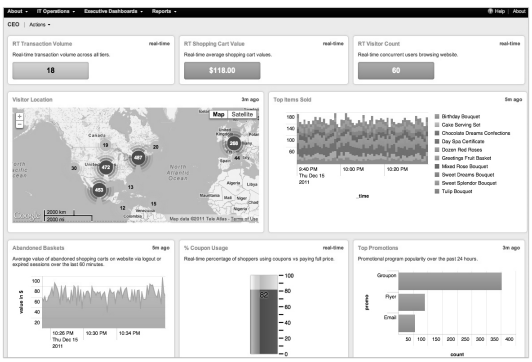


〔그림 7〕 빅데이터 기반의 통합로그 수집・분석 체계

한 정보에 대한 접근이 인가되어 있지 않으며 접근 권한이 있더라도 해당 정보들에 대한 관리 권한이 업무 조직에 할당되어 있어 통합 관리가 이루어지지 않고 있다.

보안 목적으로 해당 정보들을 활용하기 위한 제도적인 뒷받침과 더불어 [그림 7]과 같이 네트워크와 엔드포인트 등에 존재하는 수많은 플랫폼, 애플리케이션에서 발생하는 비정형 데이터(Unstructured Data)를 포함한 다양한 형태의 대량 정보를 구조화하여 저장하고 이 정보들 간의 관계를 분석하여 보안 위협을 파악할 수 있는 빅데이터 기반의 통합로그 수집・분석 체계가 마련되어야 한다. 빅데이터 기반의 통합로그 수집・분석 체계는 빅데이터 기술의 발전에 맞추어 SIEM 솔루션과 결합되어 구현되고 있다.

하지만 광범위한 정보의 통합 수집만으로 네트워크 가시성이 강화되었다고 할 수 없다. 1956년 인지심리학과 기억법에 대한 조지밀러의 연구에 의하면 인간의 뇌는 단기적으로 처리할 수 있는 한계가 있음이 발견되었



〔그림 8〕 수집 정보에 대한 다양한 시각화 기법 적용

다. 이러한 단기 기억의 한계는 특정 정보를 7±2 크기의 의미덩이(Chunk)로 만들어 기억함으로써 극복될 수 있다.

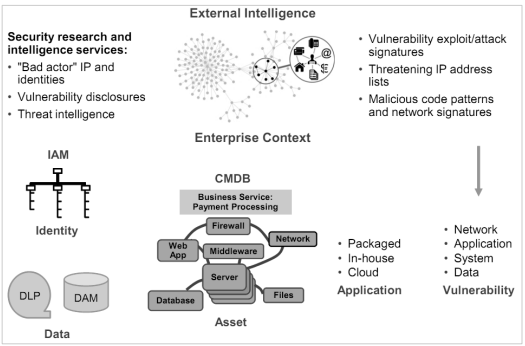
네트워크 가시성 강화 측면에서 의미덩이를 만드는데 사용하는 효율적인 방법은 시각화(Visualization)이다. 수집된 수많은 정보를 단순히 테이블 형식으로 표현하기보다 [그림 8]과 같이 추세와 흐름을 기준으로 의미덩이로 표현된 차트나 그래프 등 시각화된 형식으로 제공할 경우 해당 정보의 본질을 효과적으로 파악하는데 도움이 된다.

3.1.2. 상황인식 기반 지능형 보안관제(Context-Aware Security Intelligence)

다양한 소스로부터 발생한 정보를 통합하고 상황 관점에서 상호연관성을 분석하는 상황인식 기반 지능형 보안관제의 필요성이 강조되고 있다.

가트너는 [그림 9]와 같이 보안관제를 위해 필요한 상황 정보를 사용자, 자산, 취약점 및 설정 상황 등으로 구분하고 있다.

- 사용자 상황 정보 : 사용자의 역할, 고용상태, 접근권한 등의 정보는 이벤트 발생시 접근의 정상 여부에 대한 판단 기준을 설정하는데 도움을 줄 수 있다. 따라서 계정 및 권한 관리 시스템(IAM), 운영체제, DBMS, 응용 프로그램 등 다양한 위치에 저장되어 있는 사용자 상황 정보와 SIEM의 수집 정보를 통합한 상관분석 규칙 설정, 분석, 리포팅 등을 구현할 필요가 있다. 특히 SIEM이 IAM의 사용자 정책 설정 내용과 이벤트를 참조하는 것에서 더 나아가 정상 접근에 대한 경계를 보다 명확히 설정하여 이 정보를 SIEM과 연동하는 방향으로 개선되어야 한다.
- 자산 상황 정보 : 플랫폼에서 실행중인 프로그램, 비즈니스 프로세스 등을 포함한 자산 정보는 사용자 이상 행위의 위험 수준을 판단하는데 도움을 줄 수 있다. 자산 정보는 IT 관리・운영조직에서 관리하는 자산 관리 시스템, 비즈니스 연속성 관리 프로그램 등을 통해 수집될 수 있으며 이 정보는 항상 최신으로 유지되어야 한다.
- 취약점 및 설정 상황 정보 : 동 정보는 보안 위협의 영향 범위를 판단하는데 도움을 줄 수 있다. SIEM은 침입탐지시스템과 침입방지시스템에서 발생한 경고에 대한 후처리를 위해 취약점 진단 스캐너와 연동될 수 있다.
- 데이터 상황 정보 : 표적 공격의 주요 목적 중 하나가 중요 정보의 데이터 유출이므로 데이터 상황 정보는 표적 공격을 탐지하는데 중요하다. 데이터 상황 정보를 제공하는 솔루션은 패턴 정책 기반으로 데이터에 대한 접근을 모니터링하는 DLP(Data Leakage Prevention)와 DBMS에서 데이터의 접근을 모니터링하는 DAM(Database Access Monitoring) 등이 있다. SIEM은 상기 솔루션과 연동함으로써 상관분석 규칙, 와치리스트(Watchlist)와 통합하여 모니터링을 수행해야 한다.
- 응용프로그램 상황 정보 : 응용프로그램 취약점이 표적 공격에 이용되고 응용프로그램의 비정상 행위가 데이터 유출 등 침해사고의 지표가 될 수 있기 때문에 응용프로그램 상황 정보는 매우 중요한 정보이다. 동 상황 정보를 활용한 모니터링 방식은 [표 3]과 같다.
- 외부 위협 상황 정보 : 최신 외부 위협 정보는 발생한 이상 행위의 위험 수준을 판단하는데 도움을 줄 수 있다. 예를 들면 외부 IP로 발생한 소량의 아웃바운드 트래픽은 모니터링 과정에서 간과되기 쉬우나 해당 IP가 봇넷과 관련되어 있다는 외부 위협 정보와 연동되면 위험 분석에 큰 도움이 된다. 외부 위협 정보는 블랙리스트, 와치리스트, 상관분석 규칙 등과 연동되어 활용될 수 있다.



〔그림 9〕 모니터링을 위한 다양한 상황정보[13]

3.1.3. 관련 업무조직과의 정보 통합 및 협업 강화

표적 공격을 탐지하기 위해서는 IT 조직 및 업무조직

〔표 3〕 응용프로그램 상황 정보를 이용한 모니터링 방식

구 분	방 법
행위 모니터링	· 자체 개발한 응용프로그램과 패키지 프로그램의 이벤트 포맷을 정의하여 SIEM과 연동 · 네트워크 기반 또는 에이전트 기반으로 동작하는 별도 솔루션을 이용
예외 상황 모니터링	· 모니터링 대상 응용프로그램의 데이터와 트랜잭션 생성 절차에 대한 이해를 바탕으로 다양한 경계 및 임계치 설정 ※ 응용프로그램에 대한 전반적인 지식을 가진 직원에 의한 지속적인 모니터링(행위/예외 상황 리포트 검토 등) 필요

의 정보를 통합하여 활용하고 관련 조직 간의 협업을 강화할 필요가 있다.

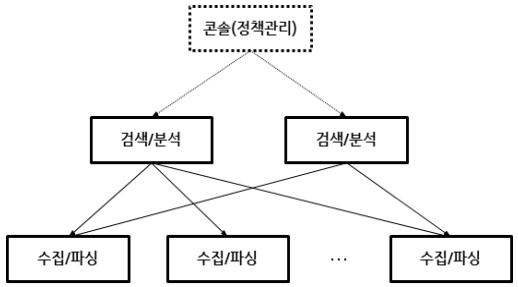
정보 통합관점에서 IT 보안조직은 IT 운영조직의 구성관리 데이터베이스에서 관리되고 있는 자산정보, 서비스뷰, 서비스 의존도를 위험관리 및 영향 평가에 활용해야 한다. 또한 계정 관리 프로세스 및 정책의 무결성을 보장하고 유출사고와 관련된 권한 변경 시도를 발견하기 위해 관리자의 행위를 모니터링해야 하며 사용자 역할과 행위 및 데이터 접근 행위를 통합 관리함으로써 사용자 역할에 위배되는 예외사항의 발생 여부를 확인해야 한다.

표적 공격의 주목적 중 하나가 데이터 유출이므로 중요 데이터를 식별하고 데이터의 접근과 이동을 모니터링하는 DLP를 SIEM과 통합함으로써 데이터에 대한 접근을 모니터링해야 하며 아울러 응용 계층이 주된 공격 경로로 활용되고 있으므로 보안 모니터링 인프라 통합에 필요한 높은 우선순위의 애플리케이션을 식별하고 시나리오 기반으로 응용 계층을 모니터링해야 한다.

또한 인가된 사용자의 권한을 통해 데이터 유출 사고가 발생하고 있으므로 협업 강화관점에서 IT 보안조직이 생성한 인가된 사용자의 행위 모니터링 리포트를 관련 업무 조직의 도메인 전문가에게 공유하여 검증받을 필요가 있다. 아울러 IT 보안조직에서는 자원 및 데이터 접근, 시스템 변경 등 작업 행위의 이상 여부를 명확히 구분할 수 없으므로 기록된 작업 행위는 변화 관리 리포트로 관리되어 업무조직의 도메인 전문가에게 검증받아야 한다.

3.2. 필요 기술

3.2.1. 구조적 측면



〔그림 10〕 다중 노드 기반의 분산 병렬처리 시스템 구조

[그림 10]과 같이 수집과 분석 기능이 상호 영향을 주지 않도록 수집 · 파싱, 검색 · 분석, 콘솔(정책관리) 등의 역할을 계층적 · 독립적으로 처리하는 다중 노드 기반의 분산 · 병렬처리 구조를 갖추어야 한다.

또한 신규 서비스 출현, 새로운 보안기술의 접목 등 횡적, 종적으로 확대되어가는 네트워크 구조에 따른 모니터링 환경 변화를 최소화하고 수집 및 분석 성능을 향상시키기 위해 스케일 아웃(Scale Out) 관점의 수평적 확장 구성이 가능해야 한다.

3.2.2. 수집 · 파싱 관점

[표 4]와 같이 네트워크 가시성을 강화하기 위해 다양한 위치, 시스템, 영역, 프로토콜 등의 관점에서 수집 대상을 확장할 필요가 있다.

트래픽 정보 관점에서 네트워크 가시성을 강화하기 위한 수집 대상별 특징은 [표 5]와 같다.

아울러 수집 정보원의 다양한 특성, 설치 및 운영 환경을 지원할 수 있도록 [표 6]과 같이 여러 가지 수집 수단을 제공할 필요가 있다.

〔표 4〕 수집 정보 특징의 변화

구 분	기 존	향 후
수집위치	경계(Perimeter)	경계(Perimeter), 내부(Intranet) 구간 등
대상 시스템	보안솔루션	보안솔루션, 네트워크, 엔드포인트(서버/PC)
수집영역	보안 영역	보안 및 업무(운영 등) 영역
프로토콜	3 ~ 4계층	4 ~ 7계층(컨텐츠 포함)
방 향	유입트래픽 위주	유입 · 유출트래픽
형 태	정형데이터 (시그니처 중심)	정형/비정형데이터, 원본로그 (콘텐츠 및 컨텍스트 중심)
수 단	Agent / Agentless	

〔표 5〕 수집 정보별 특징

구 분	대상 정보	특 징
SNMP	MIB 기반	· 네트워크 세그먼트간 네트워크 사용량(bps 등), 에러량, 처리속도, 응답시간 등 통계정보 확인 · 네트워크 장비의 자원(CPU, MEM 등) 사용률 · 트래픽 흐름, 유형, IP별 사용량 등 트래픽의 특성을 확인하는데 한계가 있음
방화벽 세션 로그	트래픽 5 튜플 정보	· 5 튜플(tuple) 패킷 정보 기반 접근제어 결과(허용/차단) 확인 · 정책이 적용되는 역방향의 패킷전송 크기에 대한 확인이 어려움
네트워크 플로우 (L4)	L4 플로우 정보	· 네트워크 플로우 정보 기반 비정상 행위 탐지 및 새로운 애플리케이션이 유발하는 트래픽 확인 · 포트정보를 기반으로 애플리케이션을 구분하여 트래픽 사용량을 측정할 수 있음 · 정상 포트 정보로 위장한 트래픽의 흐름을 모니터링하는 데 한계가 있음
네트워크 플로우 (L7)	L4 플로우 정보, 응용 정보	· 애플리케이션 페이로드를 포함한 트래픽 플로우 정보 · 페이로드를 이용하여 애플리케이션 흐름에 대한 가시성이 높아짐 · 타 보안 정보(이벤트, 취약점, 자산 등)와의 상관분석을 통해 오탐을 줄이고 위험도 판단의 정확성을 향상시킬 수 있음
전체 트래픽	패킷 전체	· 모든 네트워크 트래픽의 실시간 저장 및 인덱스 생성 · 수집된 트래픽을 재조립함으로써 세션/컨텐츠 단위의 분석과 재현에 활용할 수 있음 · 네트워크에 대한 광범위한 가시성을 확보하나 이상 탐지 기법과 조합하지 않는 경우 분석에 많은 인력과 시간이 소요

〔표 6〕 수집 방법별 특징

구 분	비 고
수집 정보원 또는 Syslog 서버(결합 기능)에 설치된 에이전트 이용	Agent
수집 정보원의 Syslog 송신 기능 이용	Agentless
수집 정보원의 데이터베이스 폴링(Polling) 이용 (데이터베이스 View Table 활용)	
수집 정보원에서 제공하는 API 호출	

3.2.3. 검색 · 분석 관점

수집된 빅데이터로부터 유의미한 데이터를 효율적으로 추출하기 위해서는 사용자가 이해하기 쉬운 대화형 쿼리 중심의 검색 분석 기능이 제공되어야 한다.

또한 상관분석 규칙에 이벤트 로그, 트래픽, 취약점, 자산 등 다양한 유형의 정보를 활용함으로써 이상 행위 판단의 정확성을 제고할 필요가 있으며 규칙 생성시 필요한 지원 기능은 [표 7]과 같다.

〔표 7〕 상관분석 규칙에 필요한 주요 기능

구 분	기 능
시 간	· 절대적 시간(Absolute Time) 지정 · 상대적 시간(Relative Time) 지정 · 시간 간격 지정
조 건	· AND, OR, NOT, EQUAL, Gt(le) Than 등 · 임계치(Threshold) 기준
문자열 매치	· 일반 문자열 기준(substring, upper 등) · 정규표현식(Regular Expression)
필터링	· 최상위/최하위 정보 선택 · TOP N 정보
보 기	· 경고(Alert)의 가독성 강화를 위한 별명(Alias) · 정렬(Sorting)
연 동	· 외부 데이터 참조
통 계	· 통계적 기능(Count, Average, SUM, MAX 등)
처리 구조	· 실행 주기(Execution Duration) · 직렬 처리(Serial Processing)

아울러 상기 방법에 의해 생성한 상관분석 규칙을 실시간 데이터뿐만 아니라 과거 데이터 분석에도 적용함으로써 탐지되지 않은 잠재적인 내부 보안 위협을 파악하는데 활용할 수 있다.

3.2.4. 이상 탐지 관점

사이버 공격을 탐지하기 위한 방법은 비정상 공격 행위에 대한 패턴을 이용하는 패턴 기반 탐지 방법(Rule-based Detection)과 정상 행위에 대한 베이스라인(Baseline)을 기준으로 유의미한 공격 행위를 찾는 이상 탐지 방법(Anomaly Detection)으로 분류할 수 있다.

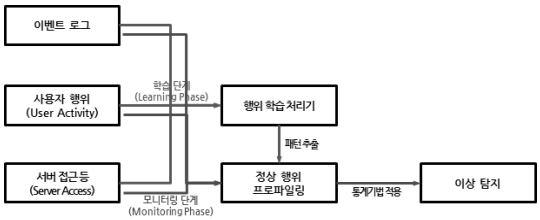
두 가지 탐지 방법은 [표 8]과 같이 각기 장단점을 가지고 있으므로 이를 조합하여 탐지 정책을 수립하되 알려지지 않은 패턴을 이용한 표적 공격의 탐지 확률을 높이기 위해 이상 탐지 방법을 조합해야 한다.

〔표 8〕 패턴 기반 탐지와 이상 탐지 방법의 비교

구분	패턴 기반 탐지 방법	이상 탐지 방법
장점	· 알려진 공격 방법 및 조건으로 공격을 식별하는데 용이 · 특정 모니터링 방법과 정책을 구현하는데 용이	· 정상과 차이를 보이는 부분을 식별하는데 용이 · 새로운 공격 방법을 발견하는데 용이
단점	· 특정 환경에 적용하기 이전 커스터마이징 필요 · 이전에 확인되지 않은 조건을 탐지하는데 부적합	· 오탐을 줄이기 위해 광범위한 튜닝이 필요 · 비구조적 환경에서 사용하는데 부적합
비고	· 안티 바이러스, 침입탐지 · 방지시스템 등	· 패턴 기반 이상 탐지 · 통계 기반 이상 탐지

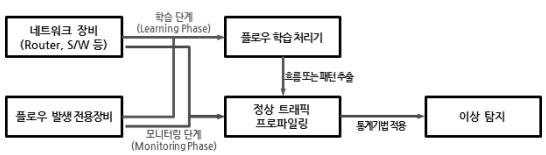
이상 탐지 방법은 플로우 정보, 사용자, 서버 등과 같은 비연속적인 이벤트 소스에서 정상 행위를 프로파일링 하는 학습 단계가 선행되고 학습이 완료된 이후 정상치와 차이가 발생하는 부분으로 이상 행위를 탐지하는 모니터링 단계가 수행된다. 정상치와의 차이를 구별하는 방법에 따라 패턴 기반 이상 탐지와 통계 기반 이상 탐지로 구분할 수 있다.

패턴 기반 이상 탐지 방법은 보안시스템 등에서 발생한 로그 이벤트를 기준으로 이상 행위를 탐지하며 [그림 11]과 같은 프로세스로 수행된다.



〔그림 11〕 패턴 기반 이상 탐지 프로세스

통계 기반 이상 탐지 방법은 평상시 트래픽에 대한 프로파일링 정보를 기준으로 네트워크 트래픽 관련 정보(Flow 등)로부터 이상 행위를 탐지하며 [그림 12]와 같은 프로세스로 수행된다. 트래픽에 대한 프로파일링 정보 수집은 트래픽의 흐름(출발지 IP와 목적지 IP의 조합) 또는 패턴(서비스 포트 등)을 기준으로 수행될 수 있다.



〔그림 12〕 트래픽 기반 이상 탐지 프로세스

3.2.5. 애플리케이션 및 데이터베이스 행위 정보 관점

고도화된 해킹 공격의 주요 목표인 데이터 유출 행위 등을 탐지하기 위해 애플리케이션 및 데이터베이스 접근에 대한 모니터링이 필요하다.

애플리케이션(패키지, 자체 개발 포함)에서 발생하는 행위 로그 정보를 수집하고 이를 사용자 상황 정보와 통합 분석함으로써 애플리케이션 수준의 공격 및 부정사용을 탐지하고 컴플라이언스 리포팅에 활용할 수 있다.

또한 DBMS 모니터링, 파일 무결성 모니터링, 데이터 유출 방지 기능 등 데이터 접근 행위 관련 로그를 수집함으로써 데이터 유출 시도를 모니터링할 수 있다.

3.2.6. 외부 위협 정보 활용 관점

범국가적으로 조직화되고 있는 사이버 공격에 대응하기 위해 국내를 포함하여 글로벌하게 수집된 위협 정보를 와치리스트에 추가하여 상관분석규칙 및 검색 조건 등 보안관제에 활용할 필요가 있다.

위협 정보의 주요 정보원은 보안업체 보안연구조직, 보안관리서비스제공자(MSSP), 국내·외 위협 정보 제공 사이트 등으로 분류할 수 있다.

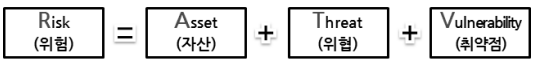
3.2.7. 모니터링 및 이력 관리 관점

표, 그래프, 차트 등 다양한 방식의 표현을 통해 보호대상 자산에 대한 전체적인 위협 현황을 대시보드로 표현할 수 있다.

또한 업무부서 도메인 전문가와의 정보 공유 등 모니터링 업무 강화를 위한 협업의 목적으로 다양한 모니터링 리포트의 생성을 지원해야 한다.

3.2.8. 취약점 및 자산 관리를 통한 위험 관리 관점

주기적인 취약점 스캔을 통해 열린 포트, 관련 취약점 등 내부 보호 자산에 대한 정보를 프로파일링할 수 있다. 프로파일링 정보는 경고 발생시 상관분석을 통해 관련 접근의 위험도를 평가하고 네트워크 운영상에 발



〔그림 13〕 위험 관리 지수 계산식

생할 수 있는 시스템 환경 변경 등의 관리적 취약점을 모니터링하는 데 활용될 수 있다.

또한 IT 관리조직의 자산관리 관련 시스템(프로젝트 관리시스템, 형상관리시스템 등)과 연동하여 자산 중요도, 운용환경(운영체제, 설치 애플리케이션 등)의 정보를 항상 최신으로 유지할 필요가 있다.

[그림 13]과 같이 취약점 정보와 자산정보는 위험 관리 관점의 모니터링 체계를 구축하는데 도움이 된다.

3.2.9. 디지털 포렌식 관점

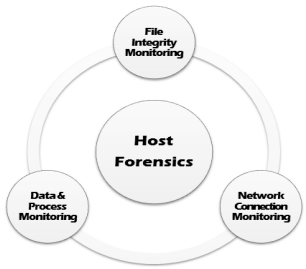
침해사고 발생시의 변화(파일 변조, 악성 프로세스 및 소켓 생성)를 모니터링하기 위해 [그림 14]와 같은 포렌식 기법을 보안관제에 활용할 수 있다.

- 서버 무결성 정보 수집
  - 서버 중요 폴더 또는 파일의 무결성 정보 모니터링
- 서버 상태 정보 스냅샷
  - 서버에서 생성 중인 프로세스와 소켓정보 등 서버 상태 정보를 주기적으로 모니터링함으로써 서버의 상태 변화를 모니터링
- 서버 로그 정보 수집
  - 권한 상승, 원격 접속, 로그인 실패 등을 모니터링할 수 있는 syslog (securelog), sulog, loginlog 등의 시스템 로그 정보 모니터링

3.3. 보안관제 모델링

3.3.1. 공격 벡터(Attack Vector)의 증가

금융회사 및 방송사를 대상으로 3.20 전산장애사고가 발생한 후 APT 등 고도화된 표적 공격을 막기 위한 방법으로 망분리가 대안 중 하나로 주목받고 있다. 망분리를 적용하게 되면 네트워크의 구조적인 변화로 인해 다른 보안 조치를 추가로 구현하지 않더라도 많은 보안 목적을 달성할 수 있게 된다. 그러나 망분리 후에도 여전히 존재하는 공격 벡터를 구축 시점에 함께 제거하지 않는다면 중요 자산이 위치한 내부망에 대한 침투 위험은 여전히 존재하게 된다.



〔그림 14〕 호스트 포렌식 분석 기법의 활용

하지만 망분리 이후에 존재하는 공격 벡터는 홈페이지를 통한 대고객 서비스 제공, 내·외부망간 자료 송수신, 인터넷을 통한 정보 수집, 개인 모바일 기기의 업무활용 등 정상적인 업무 수행에 반드시 필요하고 향후에도 더욱 확대될 가능성이 높다. 이와 같이 일부 유형의 공격 벡터는 원천적인 제거가 어려우므로 엄격한 통제 및 모니터링을 통해 발생 가능한 리스크를 최소화할 필요가 있다.

3.3.2. 기업 환경에 따른 수집 정보 범위 설정

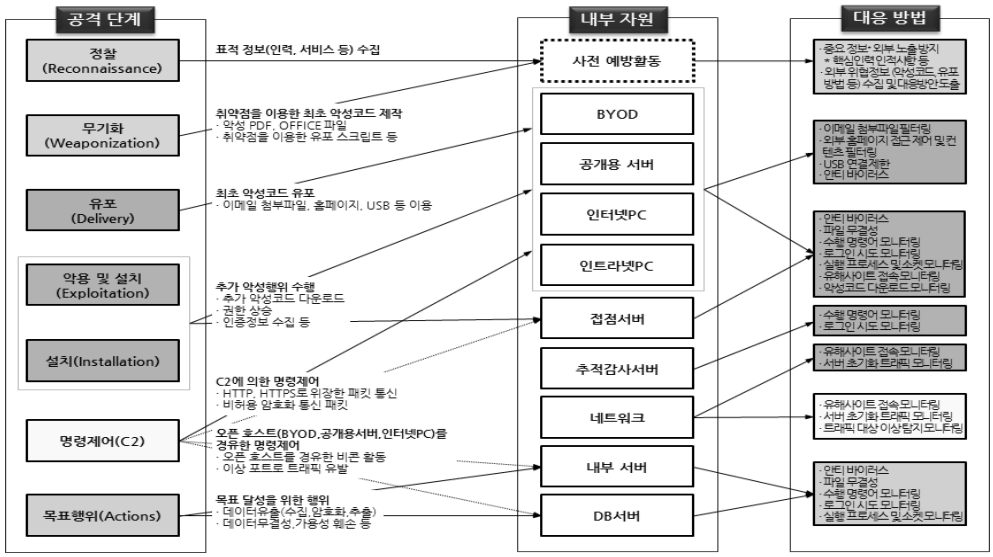
[그림 15]와 같이 공격 단계, 내부 자원, 대응 방법의 연관성 분석을 수행하였다.

침투 초기 단계라 할 수 있는 정찰, 무기화, 유포는 서버 해킹(Server Hacking), 스피어 피싱(Spear Phishing), 워터링 홀(Watering Hole), 무선 해킹(Wireless Hacking), 분리성 미디어(Removable Media) 등 5가지 경로에서 주로 발생한다.

정찰 및 무기화 단계는 공격대상 기업이 직접적으로 관련되어 있지 않기 때문에 명확한 대응방법이 존재하지 않으나 봇넷, 악성코드와 같은 외부 위협 정보에 대한 지속적인 수집과 관련 패턴 적용 등 예방활동 차원의 대응이 필요하다.

동 연관성 분석을 통해 보안관제 목적에서 수집해야 할 정보의 범위를 [표 9]와 같이 도출하였다. 수집 대상 정보는 정보보호솔루션, 호스트(서버 및 PC), 네트워크 등의 시스템 관점과 자산 및 취약점 프로파일링 등의 정보 관점으로 분류하였다.

내부 PC를 이용한 APT 침투 사례가 빈번히 발생하여 PC에 대한 로그 수집의 필요성이 증가하고 있으나 본 논문에서는 중요 단말기로 분류된 시스템 운영 PC로 대상을 한정하였다.



〔그림 15〕 공격단계, 내부자원, 대응 방법간 연관성 분석

〔표 9〕 수집 필요 정보 범위

분 류		대상 로그
정보보호 솔루션	공통	감사로그(로그인 정보 등)
	방화벽	접근로그, 에러로그
	IDS/IPS/WAF	침입탐지/차단로그
	유해차단	외부 사이트(유해사이트 등) 접근 로그
	APT	APT 탐지로그(유입실행파일 검증)
	DLP	프로그램(패치 포함) 설치 정보, 응용프로그램 접속 로그, 매체사용로그 등
	Anti-Virus	악성 프로그램 탐지/삭제 로그
	네트워크 접근제어	네트워크 비정상행위 탐지로그, 시스템 정보변경 로그, 업데이트 파일 배포 로그 등
	DB보안	데이터베이스 질의 및 응답 관련 로그
	USB통제	USB 연결정보
	패치관리	업데이트 파일 배포정보
	서버보안	시스템 접속로그, 중요파일 실행로그, 서버보안 데몬 실행 로그(시작, 종료)
	무결성검증	중요 파일 생성 및 변경 로그
	WIPS	무선 침입탐지/차단로그
서버	공통	각종 시스템로그, 프로세스 및 소켓 연결 정보
	WEB	응용로그(접근로그, 에러로그)
	MAIL	메일 필터링로그
	DB	감사로그, 질의 및 응답 관련 로그
	추적감사	시스템 로그인 로그, 수행 명령어 로그
PC	운영	보안감사, 시스템 로그 등 Windows 로그
네트워크	Router/SW 트래픽분석	네트워크 트래픽 플로우정보(L4,L7 등)
자산관리		중요도, OS, Application 등 자산 정보
취약점 프로파일링		오픈 포트, 취약점 등 스캔 정보

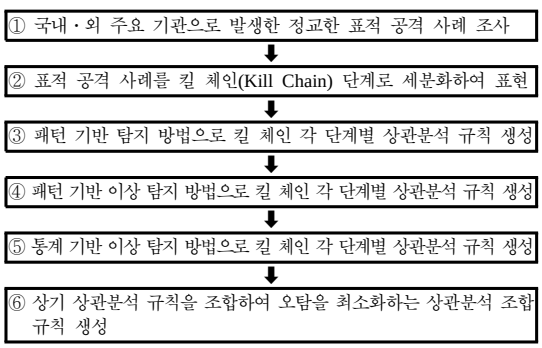
기업의 네트워크 구조와 내부 자원의 종류에 따라 수집 필요 정보의 범위는 상이할 수 있다.

3.3.3. 사례(Use Case) 기반 상관분석 규칙 생성 · 적용

SIEM을 이용한 정교한 표적 공격의 탐지는 다양한 침해사고 관련 지식을 반영한 상관분석 규칙의 관리와 발생한 경고의 체계적인 처리에 달려있다.

우선 상관분석 규칙은 국내 · 외 주요 기관으로 발생한 정교한 표적 공격 사례를 바탕으로 패턴 기반 탐지 방법(Rule-based Detection)과 이상 탐지 방법(Anomaly Detection)을 조합하여 생성해야 한다.

본 논문에서 제안하는 상관분석 규칙의 생성 절차는 [그림 16]과 같다.



〔그림 16〕 상관분석 규칙 생성 절차

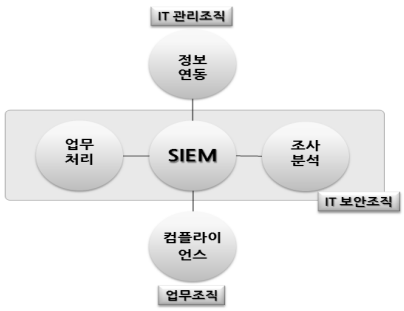
상기 절차를 통해 상관분석 규칙을 생성할 때의 주요 원칙은 아래와 같다.

- 공격 경로로 빈번히 사용되나 공격 형태가 다양하고 변수가 많아 패턴 기반 상관분석만으로는 미탐(False Negative)의 가능성이 높은 공격 단계는 이상 탐지 기반의 상관분석을 조합하여 구성
- 다만 패턴 기반 이상 탐지 방법과 통계 기반 이상 탐지 방법은 사용자 패턴 규칙의 복잡도와 프로파일링에 따라 시스템 연산을 증가시킬 수 있으므로 패턴 기반 탐지 방법의 정확성이 저하되는 공격 단계에 적용할 것을 권장

사례 기반 상관분석 규칙 생성 적용 예시는 [표 10]과 같다.

〔표 10〕 사례 기반 상관분석 규칙 생성 예시

공격 단계	수행 내용	탐지
정찰	표적 공격에 활용할 공격 벡터 선정	×
무기화	명령제어서버(C2) 구축 워터링 홀 공격에 사용할 홈페이지 선정 및 공격 표적 공격용 악성코드 제작	△
유포	워터링 홀 공격에 의해 인터넷PC 악성코드 감염	△
	이메일 첨부파일을 이용한 악성코드 유포 <규칙1> 일반 악성코드를 내부 사용자에게 유포 첨부파일 검증시스템에서 악성코드 탐지 관련 이메일 수신자PC를 감시목록에 등록하고 이상 행위(내부 스캔 등) 탐지 최근 한 달 동안 동일 해시 값의 첨부파일을 수신한 사용자PC의 이상 행위(내부 스캔 등) 검색 <규칙2> 제로데이 악성코드를 내부 다수 사용자에게 유포 최근 해시 값을 가진 악성코드 유포가능 유형(실행파일, 문서파일 등) N개(임계치)의 첨부파일 탐지 이메일 열람 시점에 감시목록 또는 외부 동일 IP로의 접근 시도 탐지(이메일 수신자 PC에서 백신 탐지이력 없다고 가정) 관련 이메일 수신자 PC를 감시목록에 등록하고 이상 행위(내부스캔 등) 탐지	○
악용 및 설치	인트라넷 홈페이지 정보(도메인,IP,인증정보 등) 수집 인트라넷 홈페이지에서 파일 업로드 취약점 확인 <규칙> 내부PC에서 N개(임계치)의 다수 서버IP로 이상 행위(내부 스캔 등) 탐지 내부PC에서 특정 서버IP로 웹 취약점 공격 시도 관련 이벤트 탐지 내부PC(접근권한이 없는 사용자PC)에서 특정 서버로 관리적 목적의 서비스(텔넷, FTP 등) 이용 시도 탐지 특정 서버에서 중요 명령실행 및 무결성 이벤트 검증	○
	인트라넷 홈페이지 웹쉘 업로드 및 접근 인트라넷 홈페이지 변조(악성 스크립트 삽입) <규칙> 특정 서버에서 웹 소스 무결성 이벤트 탐지 해당 시점 전후(1분)에 웹 로그 중 접근 빈도가 높지 않은 단일IP URI에 대한 정보 획득	○
	인트라넷 홈페이지에 접근한 PC의 악성코드 감염	△
명령 제어	인터넷PC와 인트라넷 홈페이지가 악성코드 명령제어서버와 통신 및 악성코드(이미지 형태) 다운로드 <규칙> 인터넷PC 또는 인트라넷 홈페이지가 외부 위협 정보에 속한 IP와 통신한 이벤트 탐지 서버에서 외부 IP로 초기화된 트래픽 탐지 이미지로 위장한 악성코드 유포가능 유형의 파일 다운로드 시도 탐지	○
목표 행위	중요 서버 로그인 및 명령실행 테스트 <규칙> 최근 한 달 동안 중요 서버에 접근(관리포트)한 이력이 없는 IP에서 중요 서버 로그인 탐지 권한상승(su) 등 중요 명령 실행 탐지 [컴플라이언스] 도메인 전문가가 명령 실행에 대한 정상 여부 확인	○
	다수 내부PC가 인트라넷 홈페이지에서 디스크파괴 악성코드(이미지로 위장) 다운로드 운영PC가 인트라넷 홈페이지에서 중요서버 파일삭제 스크립트 다운로드 운영PC가 중요서버 파일삭제 스크립트 실행 <규칙> 이미지로 위장한 악성코드 유포가능 유형의 파일 다운로드 시도 탐지 권한상승(su), 파일삭제 등 중요 명령 실행 탐지 운영PC 보안감사로그에서 같은 시점에 N개(임계치)의 동일 명령 실행 시도 탐지	○



〔그림 17〕 SIEM과 주변 지원기능의 연계

3.3.4. SIEM을 지원하는 주변 기능

SIEM 기반의 효과적인 보안관제를 위해서는 [그림 17], [표 11]과 같이 정보연동, 업무처리, 컴플라이언스, 조사 분석 등 지원기능을 구축하여 SIEM과 연동할 필요가 있다.

Ⅳ. 결 론

본 논문에서는 APT 등 고도화된 표적 공격을 탐지하기 위한 방법으로 네트워크 가시성 강화, 지능형 상황관제, 관련 업무조직과의 협업 강화 등의 3대 방향성을 바탕으로 한 이상 탐지, 애플리케이션 및 데이터베이스 행위 정보 관점 등 총 9개의 관점에서 필요 기술을 정리하였다.

3대 방향성과 9개 필요 기술을 통해 정리한 보안 개념은 1990년대부터 연구가 시작되었으며 2006년부터 SIEM이라는 솔루션으로 집약되어 구현되기 시작되었다. 최근 대량의 정보로부터 가치를 추출하고 결과를 분석하는 빅데이터라는 기술과 접목되면서 구현의 완성도가 높아지고 실제 업무에 활용할 수 있을 수준으로 현실화되어가고 있다.

〔표 11〕 지원기능의 주요 내용

구분	내 용
정보 연동	· IT 관리조직의 자산 정보 연동(최신 유지) · 내 · 외부 취약점 정보 연동 ⇒ 내부(취약점 스캐너를 이용해 수집된 취약점 정보) ⇒ 외부(내부 자산 정보를 기초로 한 최신 취약점 정보)
업무 처리	· 통합로그 수집 · 분석시스템에서 도출된 분석대상 결과물에 대한 처리절차(접수, 처리, 승인)
컴플라이언스	· 모든 인가 사용자의 행위에 대한 모니터링 필요 · (IT보안조직) 인가 사용자 행위 모니터링 리포트를 개발 · 생산 · (업무조직) 도메인 전문가에 의한 리포트 검증 및 결과 회신 ※ 관련 업무조직에서 보안업무영역에 대한 지원 필요
조사 분석	· 침해사고(의심 포함)에 대한 신속한 분석 지원

본 논문에서는 고도화된 표적 공격에 대응하기 위한 보안관제 모델로 패턴 기반 탐지와 이상 탐지 방법 등을 조합한 사례(Use Case) 기반 상관분석 규칙의 활용과 정보연동, 업무처리, 컴플라이언스, 조사 분석 측면에서의 지원 기능을 포함한 보안관제체계를 제시하고 있다.

끝으로 강조하고 싶은 점은 보안관제 인프라와 더불어 보안관제를 효과적으로 수행하기 위한 정보보호 정책의 수립과 조직 간의 협력, 정보보호 담당 직원들의 역량 강화, 전 직원의 보안의식 고취 등이 동시에 만족되어야 진화하는 보안 위협으로부터 기업의 중요 자산을 안전하게 지켜낼 수 있다는 점이다.

참고문헌

[1] Carnegie Mellon University, "Trusted Computing in Embedded Systems", 2010.

[2] E.M. Hutchins, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11)*, pp. 113–125, 2010

[3] Verizon, "2013 Data Breach Invesigation Report", 2013.

[4] 김동한, "빅데이터 환경에서 지능형 로그 관리 플랫폼으로 진화하는 보안 정보/이벤트 관리(SIEM) 동향", *정보통신산업진흥원 주간기술동향*, 2013년 8월.

[5] 노병규, "지능형 사이버보안 기술 동향 및 이슈", *한국방송통신전파진흥원, PM Issue Report 2013 제1권 이슈3*, 2013년.

[6] 최대수, "빅데이터 환경에서 차세대 통합보안 기술", *Software Convergence Symposium 2013*, 2013년 1월.

[7] 임신영, 허재두, "상황인식 컴퓨팅 응용 기술 동향", *전자통신동향분석 제19권 제5호*, 2004년 10월.

[8] Gartner, "Hype Cycle for Application Security",

2013.
[9] "전산시스템 계층적 방어체계로 위험 분산시켜야!", 보안뉴스, http://www.boannews.com/media/view.asp?idx=21727
[10] National Security Agency, "Information Assurance Technical Framework (IATF) document, Release 3.1", September 2002.
[11] Microsoft, "Security Content Overview", http://technet.microsoft.com/en-us/library/cc767969.aspx
[12] Gartner, "Information Security Is Becoming a Big Data Analytics Problem", 2012.
[13] Gartner, "Effective Security Monitoring Requires Context", 2012.

〈저자소개〉

신 휴 근 (Hyu Keun Shin)
정회원

2002년 2월 : 아주대학교 정보및컴퓨터공학부 학사
2004년 2월 : 아주대학교 정보통신대학원 석사
2004년 3월~현재 : 금융결제원 금융정보보호부 정보보호기술팀 과장
<관심분야> 침해사고분석, 보안관제기술

김 기 철 (Kichul Kim)
정회원

2001년 2월 : 동국대학교 컴퓨터공학과 학사
2013년 2월 : 고려대학교 정보보호대학원 석사
2002년 4월~현재 : 금융결제원 금융정보보호부 정보보호기술팀 과장
<관심분야> 정보보호관리체계, 보안성평가