통합 보안관제 체계에 관한 비교 연구

팀　　명 :　　혼자이조
지도 교수 :　양환석 교수님
팀　　원 :　　김은지

2021. 10. 24
중부대학교 정보보호학과

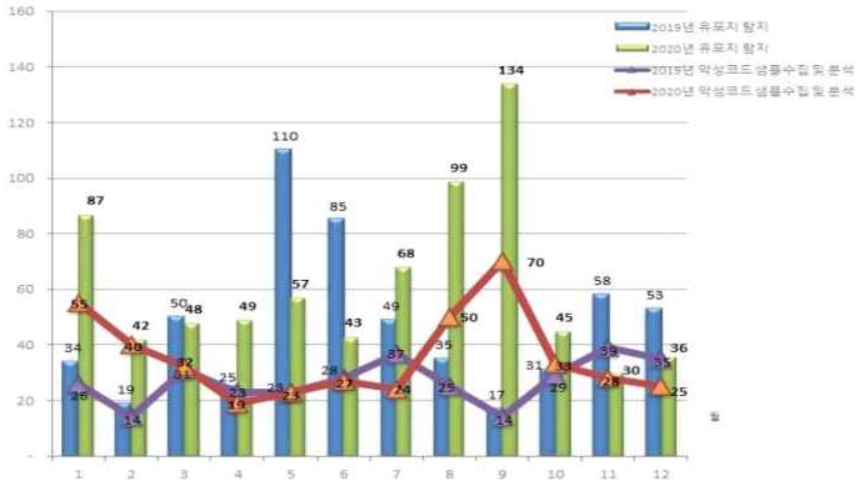
목 차

그 림 목 차

1. 서론

1.1 연구의 배경 및 목적

4차 산업혁명의 시대를 살아가고 있는 지금 사이버공간은 어디를 특정할 것 없이 모든공간에서 악성코드에 의한 위협으로 두려움에 떨고 있다. 이번 코로나의 펜데믹과 함께 IT환경의 급격한 성장과 인터넷 사용대상의 확대를 기반으로 악성코드에 의한 피해 범위와 규모 역시 급격하게 증가하고 있다.



<그림1> 2020년 악성코드 탐지 · 대응 동향

한국인터넷증흥원의 2020년 하반기 사이버 위협 악성코드 은닉사이트 탐지 동향 보고서에 따르면 악성코드 유포지 탐지 및 대응 현황은 2020년 상반기 대비 26%증가, 2019년 하반기 대비 70%증가 된 추이를 그림 1을 통하여 확인이 가능하다[1].

이러한 공격이 늘어난 이유는 악성코드의 종류도 증가할 뿐 아니라 초보자가 쉽게 사용할 수 있는 악성코드 서비스를 뒷 시장에서 싼 가격으로 제공하여 전보다 많은 사람들이 공격할 수 있으며, 기존의 악성코드가 다양한 형태로 변화하여서 다양한 보안 시스템 및 백신 등을 우회하고, 더욱더 지능적으로 변화되어서 탐지하기도 어렵고, 늘어나는 로그의 양에 따라서 대응 시간도 늘어나 대응이 더욱 힘들어지고 있다[2]. 늘어난 보안 로그를 통해서 여러 로그들 간의 연관 관계를 분석하여, 정확한 판단을 할 수 있는 상호 연관분석이 필요하기에 각 장비의 담당자들의 로그 분석 노하우도 모두 적용되어야 하고, 공격으로 인한 또 다른 피해가 발생하기 전에 신속한 조치를 위해서 로그의 분석을 매우 신속하게 이루어져야 한다. 이러한 일을 보안전문가들인 사람들로 대체하기에는 현실적인 한계에 부딪히고 있다. 보안전문가들의 오래도록 축적된 기술과 그에 관한 노하우를 대체하는 방안은 오래전부터 연구되어왔지만, 사람의 창의성과 판단력을 대체하기 위해서는 하나의 알고리즘이 아닌, 수많은 데이터들의 분석과 적용으로 인한 올바른 판단을 할 수 있어야 한다.

이처럼 사이버위협은 기술적으로 지속적인 발전이 이루어지고 있다. 더불어 사이버 범죄, 테러와 같은 위협도 조직화 고도화됨과 더불어 복잡하고 다양한 형태로 진화하고 있다. 결과적으로 지속적이고 고도화, 다양화가 되는 사이버공격 기술에 선제적이고 효과적인 대응을 위해, 그리고 대량의 위협 이벤트들을 분석하여 대응하기 위해서는 인공지능 기술에 기반한 대응이 유용하다. 이러한 추세가 의미하는 것은 기존의 통합보안 관제 솔루션의 진화를 요구하고 있다는 것이다[3].

1.2 연구의 내용 및 범위

국내의 정보보호 기술 트렌드가 어떻게 바뀌는지에 대해 쓴 본 논문의 내용은 다음과 같다. 제 2장에서는 통합보안관제 업무 및 서비스의 프로세스를 살펴보았다. 제 3장에서는 지금 까직 나온 보안관제가 어떤 기법을사용하였는지에 대해 분석하였다. 제 4장에서는 본 내용들을 정리하고 향후 보안 분야에 발전이 어떻게 흘러갈지, 그리고 어떻게 바뀔지에 대해 적어보았다.

2. 통합보안관제의 업무

보안관제란 기본적으로 기업의 각종 보안 이벤트 및 시스템 로그 등을 관제 센터에서 24시간 236일 실시간으로 모니터링 하고, 분석을 통해 발생한 문제점에 대해 대응책을 제시하여 미래 보안사고를 예방하는 기능을 수행한다. 보안관제는 네트워크나 시스템에 설치된 에이전트와 정보수집 서버, 통합 관제용 시스템 이렇게 세 가지의 요소로 구성이 되어 있으며, 무중단의 원칙과 전문성의 원칙, 정보공유의 원칙이 세 가지의 수행의 기본 원칙이다.

2.1 통합보안관제 프로세스

일반적으로 보안관제 업무 프로세스는 5단계로 구분화하고 있다. 첫째, 중요 시스템, 네트워크 및 웹 서비스 등의 취약점을 사전에 파악하여 침해 사고를 방지하고 사고 발생 시 신속하게 대응해서 피해를 최소화 할 수 있는 예방 업무이다. 이는 사이버위협 경보를 사전에 공지하여 방어토록 하며, 최신 위협 및 해킹 등 보안동향 정보를 제공하고 침입차단시스템, 침입탐지시스템, 웹 방화벽 등 보안 시스템에 대한 보안 정책 및 시스템 자원의 최적화를 통해 효율적인 사이버공격 탐지를 지원할 수 있도록 한다. 또한, 모의훈련 실시, 정보보안에 대한 인식 제고를 위한 제고도 포함한다고 볼 수 있다.

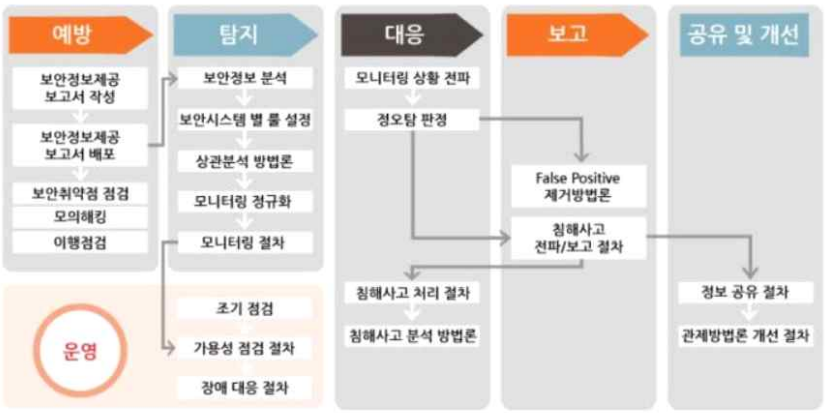
둘째, 공격자의 행위를 빠르게 잡아내기 위해 보안 시스템에 대한 24시간 365일 감시하는 탐지 업무이다. 네트워크 트래픽 정보 및 내부 정보를 탈취하기 위한 사이버공격 시도 행위를 사전에 알아내는 행위로서 네트워크 피킷 및 다양한 보안 이벤트 등을 종합적으로 상관 분석하여 재발 방지 및 확산을 방지하기 위한 방안을 강구한다.

셋째, 기관의 시스템 환경을 고려한 보안 정책 설정 및 보안관제 업무 시 발견된 비정상 네트워크 및 시스템에 대한 초기 대응 그리고 사이버 공격 발생 시 신속히 조치 대응하는 대응 업무이다. 해당 기관의 시스템 환경을 고려하여 보안 정책을 설정하고 보안 관제 업무 시 발견된 비정상적인 네트워크 및 시스템에 대해 기술적 및 정책적으로 대응할 수 있도록 하며 사이버 공격 발생 시 관련 사실을 해당 기관에 통보하고 피해 시스템의 유무 파악 및 정상적으로 운영될 수 있도록 전문 기술 지원과 유사한 공격을 방지할 수 있도록 보안 관제 업무에 활용할 수 있게 한다.

넷째, 관제 일지, 취약점 정보, 침해 사고 대응 분석 보고서 등을 보고 및 관리하는 보고 업무이다. 보안관제 업무 수행 시, 정기보고서 및 수시보고서를 통해 현재의 상태를 관리하고 보안사고 및 장애 발생 시, 관련 처리 보고서를 작성 및 보고함으로써 발생한 사고의 원인, 대응, 결과를 통해 향후 대책을 마련할수 있다.

마지막은 정보공유 원칙에 따라 타 기관에게 정보를 제공하는 공유 및 개선 업무이다. 사이버 공격으로 인한 피해가 타 기관으로 확산되는 것을 방지하기 위하여 관

계 법령에 위배되지 않는 범위에서 보안 관제 관련 정보를 공유하고 해당 보안 문제가 발생되지 않도록 기술적이고 정책적으로 개선 조치하여 보안 사고가 발생되지 않도록 예방할 수 있도록 한다.



<그림2> 보안관제 업무 프로세스 5단계

2.2 통합보안관제 서비스

보안관제 서비스는 고객의 특성을 고려하여 3가지의 유형의 서비스 제공 형태를 가졌으나 최근에는 클라우드 관제 분야까지 확대하고 있어 4가지의 유형의 서비스를 제공한다.

첫째, 원격 관제 서비스는 대상기관이 보안관제에 필요한 관제시스템을 스스로 구비하여 대상기관의 침입차단시스템 등 보안장비중심의 보안 이벤트에 대하여 상시 모니터링을 수행하는 서비스이다. 그러나 원격 관제 서비스는 인력관리에 대한 부담과 저렴한 단가 대신 서비스가 한정되어 있기에 침해/장애가 발생 시 보고는 바로 가능하지만 즉각적인 조치가 어려워 조치를 위한 인력이 필요해 시간으로 인한 실시간 대응의 어려움이 있다.

둘째, 파견 관제 서비스는 대상기관이 직접 자체적으로 보안관제 시스템을 구축하여 관제 업체로부터 전문 인력만 파견받아 관제 업무를 수행하는 형태이다. 그렇기에 대상기관에 특화된 관제서비스를 제공하며 침해/장애 발생 시 즉각적인 조치가 가능해 업무 연속성 및 효율성이 늘어나지만 인력관리가 필요하며 다른 서비스보다 단가가 높다.

셋째, 자체관제 서비스의 경우 보안관제시스템의 구축 및 관제 전문 인력을 양성하여 자체적으로 운영 및 관리하는 관제 형태이다. 내부기밀 유지와 보안관련 기술을 보유할 수 있다는 장점이 있으나, 자체적으로 하기에 하지만 전문성의 결여로 수행 품질이 떨어질 수 있다는 단점이 있다.

넷째, 클라우드 관제는 서버와 데이터베이스 등 IT 자원을 인터넷 접속을 통해 사용하는 클라우드 환경에 대한 관제이다. 대상기관은 클라우드 내에서 일어나는 보안

위협을 모니터링 하여 온프라미스 환경과 동일하게 보안관제 서비스를 받을 수 있다. 보안관리 영역에 대한 직접 관리 부담을 줄이고, 모니터링 요원, CERT 등 관제 전문인력이 제공하는 보안관제서비스를 제공받을 수 있다는 장점이 있지만 다른 서비스에 비해 리스크가 크다는 단점이 있다.

보안관제 서비스에서 사소한게 없다고 할 정도로 모든 업무 하나하나가 매우 중요하며, 한가지가 소홀해지면 바로 보안의 구멍이 생겨버릴 수 있기에 보안관제 요원들은 다양한 탐지시스템을 통해서 사이버 공격을 신속하게 탐지와 대응 할 수 있어야 한다. 정보수집 단계에서 이기종의 보안 장비에서 나오는 다양한 보안 로그를 수집하고 모니터링과 분석 단계에서는 수집된 다양한 경보 발생에 따른 침해사고 및 해킹 패턴을 기반으로 분석하고, 생성된 보안 데이터와 내·외부에서 수집된 최신 보안 위협 정보를 상세히 분석한다. 대응과 조치 단계에서는 앞에서 분석된 이벤트에 대한 원인 및 대응책을 마련해 기술적·정책적으로 대응 방안을 마련하여 이벤트에 대한 대응이 이루어진다. 마지막 보고 단계에서는 침해사고 처리 및 장애 처리 결과를 보고서로 작성하여 관련 부서별로 전달한다.

<그림3> 보안관제 서비스 프로세스

3. 통합보안관제 체계의 비교

3.1 ESM 보안관제 체계

<표 1> ESM의 핵심 기능

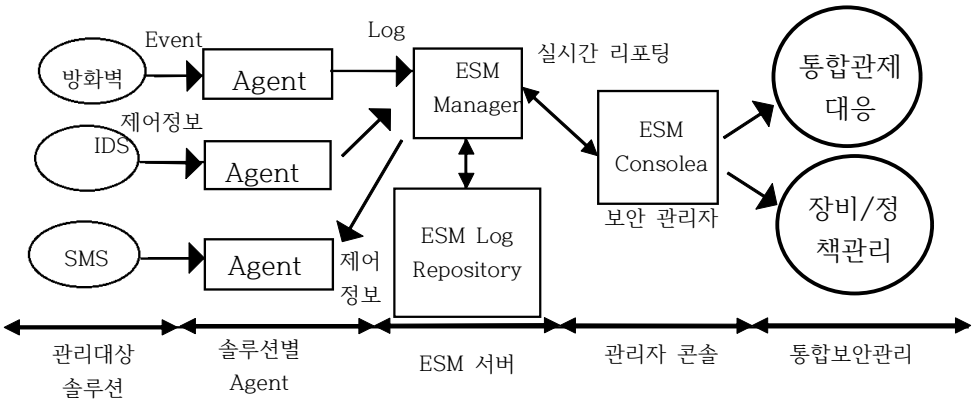
3.1.1 ESM(Enterprise Security Managemet)보안 관제 개요

ESM 보안 관제는 일반적으로 보안 시스템들을 하나의 통합 뷰로 관리하고 유사한 보안 정책을 통일하여 적용하고, 상호간의 연관분석을 통해 각 보안 시스템들의 상호 운용성, 관리성 및 보안성을 최대화하여 위험요소를 최소화하는 관리 솔루션이다. 방화벽, IDS, IPS, 등에서 나오는 정보를 수집하여 대응이 필요한 데이터에 대해 알림을 주고 통계 데이터나 그래프, 리포트 등을 제공한다. 관제 시스템에 개별

적으로 탑재를 시켜서 전사 보안정책에 따라 중앙 통제도 할 수 있다. 조직에서 하루 동안 수천 개 이상 생성되는 이벤트, 보존 기한이 각기 다른 수십 가지의 로그 형식, 수작업으로 수개월이 걸리는 조사와 분석 작업, 경고가 없거나 너무 많은 오탐 정보, 수작업으로 분석되는 장비 간의 상관관계, 이벤트의 바다에 숨어버린 중요 이벤트, 발각되지 않고 진행되는 대부분의 공격 등과 같이 수많은 데이터를 어떻게 보관하고 어떻게 처리할 것인지에 대한 어려움을 겪고 있다. ESM은 이러한 고민을 해결하고 흩어져 있는 로그 관리를 통합 모니터링 체계로 구축함으로써 효과적인 관리와 보안사고 대응이 가능하도록 해주는 솔루션으로 표 1과 같은 핵심 기능을 제공한다.

분류	핵심기능	설명
보안성	통합 View	보안 관리 도메인의 전체적 상황 정보 전달
	정규화	서로 다른 보안 솔루션 수집 정보의 일반화 분석 가능한 형식으로 변환
	상관분석	보안 솔루션의 이벤트 간의 연관성 추론 이벤트 간의 공간적, 시간적 연관 관계 해석
	정책 관리	다양한 보안 솔루션에 대한 일관적인 보안 정책 적용 보안 정책의 적용 현황에 대한 분석과 감시
운영	접근제어	보안 관리자별 관리 도메인의 분류와 접근 권한 제어
	그룹관리	보안 관리 조직의 역할에 적합한 그룹생성 및 접근제어
	경량에이전트	서로 다른 환경의 보안 솔루션에 대한 이벤트 수집을 위해서 작은 Footprint 기반의 에이전트
	데이터 전송	보안이벤트에 대한 중복 및 누락으로부터 일관성 유지

3.1.2 운영



<그림4> ESM 구성도

방화벽, IDS, SMS와 같은 다양한 보안 솔루션의 정보를 통합 보안 관리 시스템인 Agent에서 솔루션별로 이벤트 로그들을 수집 및 판단 후 마스터 서버에 이벤트 로그수집 및 모니터링을 한다. 그렇게 받은 로그들을 ESM 서버에 있는 마스터 서버에서 정보 처리 결과나 이벤트 로그를 Repository에 저장을 하거나 Agent에 명령을 하달한다. 마스터 서버에서 나온 정보 처리 결과를 보안 관리자가 확인하거나 실시간으로 확인하여 일관된 사용자 I/F 및 다양한 분석과 정보를 제공한다. 보안 관리자가 실시간 리포팅 중 문제가 생길 시 무제가 생긴 장비/정책 관리를 하거나 관련된 공격을 빠르게 대응을 할 수 있다.

3.1.3 특징

모든 기술에는 장점과 단점이 존재한다. ESM의 장점은 크게 3가지가 있다. 첫째, 하나의 콘솔로 관리할 수 있다. 원래는 VPN이나 IDS 등의 보안 솔루션을 사면 서로 다른 기종이기에 개별적으로 도입을 해왔지만, ESM은 기종에 상관없이 기업이 개별적으로 도입해온 각종 보안 솔루션을 서버단에서 하나의 콘솔로 관리를 해줄 수 있기에 원래도 부족했던 보안부서의 인원의 부담을 덜고, 다양한 보안 기능을 한곳에서 사용할 수 있다. 둘째, 중복투자와 같은 자원 낭비를 줄일 수 있다. 시스템 자원관리, 망 관리 시스템 등 서로 다른 기종의 보안을 관리해야 하는데, 그렇게 되면 각 기종에 맞는 솔루션을 설치해야 한다. 각 기종에 여러 인원이 붙어 있어야 했지만, 하나의 콘솔로 관리를 하게 되면 관리하던 인원이 줄어 사람이 필요한 곳으로 보낼 수 있게 되며 각 기종의 보안 솔루션 설치에 따른 중복투자를 하지 않게 된다. 셋째, 전체 정보통신 시스템에 대한 보안 정책을 수립할 수 있다. 이전까지는 필요한 보안 영역마다 보안 제품을 들여놔 전체적인 관리가 이뤄지지 않아 효율성은 하락하고 공격에 대한 위험도가 높은 편이었다. 그렇기에 각 기종들을 한곳에서 관리하게 되면 전체적으로 관리를 할 수 있게 되기에 공격에 대한 위험도가 낮아진

다. 이러한 장점도 있지만, 위험할 수도 있는 단점들도 있다. 첫째, 위협탐지 능력이 단순하다. IP, Port등 시그니처 중심의 네트워크 계층 탐지를 하지만 단순 패턴 기반으로 탐지하며 알려진 공격 위주로 분석을 한다. 알려지지 않은 공격 경우 확인이 안 되어 정상이라 넘어갈 수 있다. 게다가 단시간 범위만 분석할 수 있으며 최대 기간은 1일이다. 둘째, 로그를 ESM이 받아들일 수 있는 포맷으로 제공을 해야 한다. 셋째, 데이터 보존 기간이 짧다. 원본 로그는 보관을 안 하고, 보관이 되어 있는 로그들은 짧으면 1개월 길면 2개월이기 때문에 만일 문제가 생겨 다시 확인해야 하는 경우 기간이 지나버리면 문제의 로그는 확인할 수 없다.

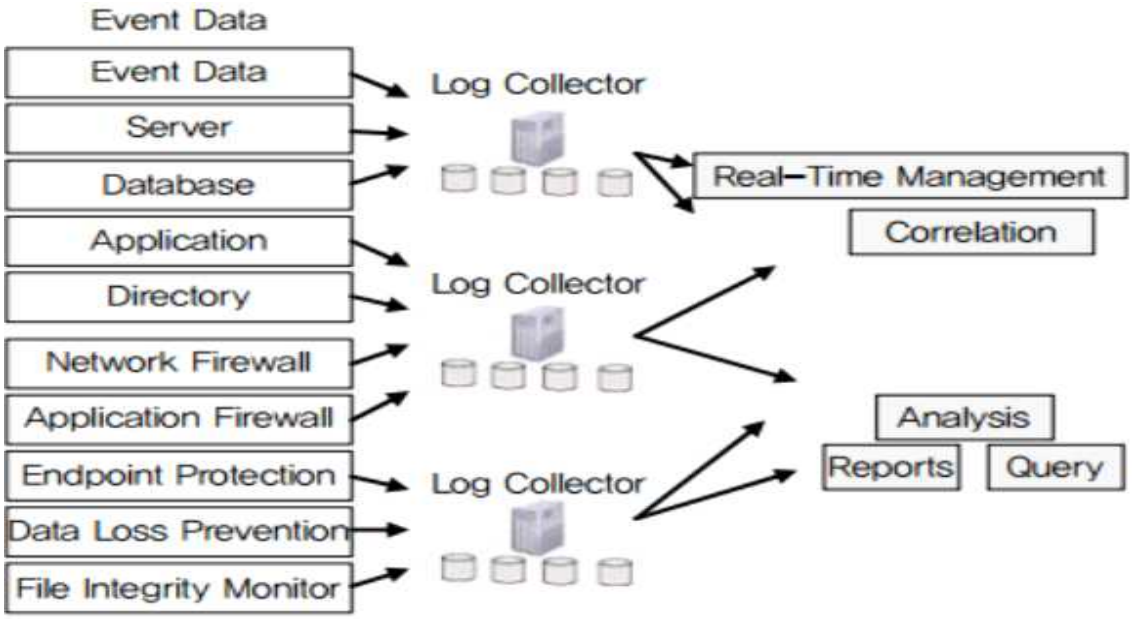
3.2. SIEM 보안관제 체계

3.2.1 SIEM(Security Information and Event Management)보안 관제

SIEM보안 관제는 여러 다양한 종류의 장비 로그 및 이벤트들을 수집 · 저장함에 따라 대량의 방대한 데이터가 쌓이게 되고 이를 빅데이터 분석기술을 활용하여 상관분석이 가능하다. 그러나 각 장비에서 기하급수적으로 증가하고 있는 로그 및 보안이벤트의 분석 측면과 웹사이트 해킹, 랜섬웨어 감염, 개인 정보유출, 모바일을 이용한 소셜 네트워크 계정 탈취시도 등 다양한 유형의 사이버 공격 측면을 고려할 경우 보다 적극적인 대응을 요구하고 있다.

3.2.2 운영

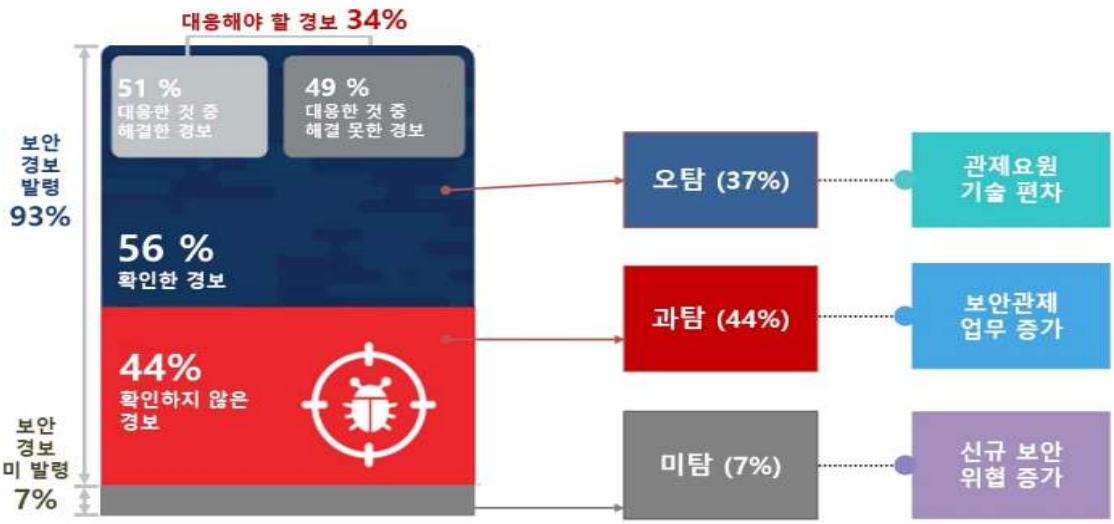
이벤트 데이터, 서버, 데이터 베이스의 로그를 수집하여 로그의 내용과 기능에 알맞게 카테고리로 보내서 실시간 관리하거나 Correlation을 통해 이벤트 간의 연결을 만들어 준다. <그림 5>에 쓰여 있는 이벤트 데이터 밑에 적힌 네트워크 방화벽, 애플리케이션, Directory, 애플리케이션 방화벽, 앤드 포인트 보안, 데이터 손실 방지 시스템, 파일 무결성 모니터뿐만 아니라 관련 다른 로그들을 관련 카테고리에 맞게 나누어 수집 후 필요한 업무에 보내 그 로그들을 분석하거나 조사 또는 문제가 있는 로그 경우에는 보고를 하거나 해결책을 찾아 문제를 해결한다. 이런 식으로 SIEM는 조직 애플리케이션, 보안 장치와 호스트 시스템에 의해 생성되는 로그 및 이벤트 데이터를 수집하고, 그 데이터를 하나의 중앙 집중식 플랫폼으로 통합하는 방식으로 기능한다.



<그림 5> SIEM 구성도

3.2.3 특징

SIEM은 다음과 같은 장점과 단점을 지니고 있다. 먼저 장점으로는 첫째, 방대하게 발생한 데이터를 자동으로 수집하여 관리한다. 자동으로 로그가 수집 및 관리가 되어 부족한 인력에 부담을 덜어준다. 둘째, 경보와 알림이 발생한다. 중요한 이벤트에 대하여 경보나 알림이 발생하여 분석가들에게 우선순위를 매길 수 있도록 도와줘 문제를 빠르게 해결한다. 셋째, 사건 및 비정상 탐지가 가능하다. 자동으로 공격이라 의심되는 행위를 표시하여 분석에 소요되는 시간을 획기적으로 줄여준다. SIEM의 단점은 총 세가지가 있다. 첫째, 빅데이터 로그 분석기술이 포함된 솔루션이 아니라면, 침해사고로 이어질 수 있는 위협시도에 대한 결과분석이 어려운 문제점을 들 수 있다. 또한, 보안부서의 부족한 인력으로는 적게는 수십만 건 많게는 수십억 건 이상 발생하는 보안이벤트를 누수 없이 모두 분석한다는 것은 사실상 불가능한 것이 현실이다. 둘째, 사이버위협에 대응하는 전문 보안 인력의 기술 수준 편차로 인해 사이버 공격이 정상적인 행위로 판단되거나, 정상적인 행위가 사이버위협으로 판단이 될 가능성이 존재한다. 이는 <그림 6>을 통하여 확인할 수 있다. 셋째, 지능화, 복잡도가 점점 높아지고 있는 APT와 같은 사이버 공격은 현재의 패턴, 시그니쳐 등 문자열 일치로 탐지하는 데에는 한계가 있다. 또한, 이들 분석은 많은 시간이 필요하다.



<그림 6> 위협탐지 누수(미탐 · 오탐)

3.3 지능형 통합보안관제

3.3.1 지능형 관제

지능형 통합보안관제란 기존에 있는 통합보안관제에 인공지능의 학습 능력을 합쳐 사람이 확인하고 판단을 내려야 하는 수동만 해야하는 일들을 자동으로 돌릴 수 있게 되었고, 비정상 행위 예측결과가 시각화되어 실시간 경보 기능이 발생 시 이벤트를 한 화면에 제공해 대시보드에 탐지된 이벤트에 대해서 항목별로 제공이 가능하다. 또한, GUI기반 모델링, 자동 모델링 기능 구현을 통해 비전문가 및 전문가 사용 편리성이 제공된다. 기존에 있는 원본 로그들과 이력 데이터 등을 수집하여 학습시켜주면 지도학습으로 인해 기존에 파악된 공격이나 위협을 정확하게 판단해 빠르고 신속하게 대처를 하며, 기존에 없던 위협이나 공격이 생기면 비 지도학습 기법을 통해 추가 학습을 하여 지속적인 개선이 이루어진다.

3.3.2 운영

<그림 7>과 같이 물리, 정보통신(IT), OT(ICS/SCADA) 보안 시스템에서 발생하는 각종 디지털 정보를 하나의 플랫폼에서 빅데이터를 활용하여 수집 및 분석하고, 머신러닝 기반의 지도·비지도 학습을 통해 고위험도 이벤트를 집중분석 하여 관제에 적용함으로써, Rules, 보안위협, 취약점, 자산중요도 등의 결과를 시각화하여 보여준다. 그렇게 시각화되어 나온 결과들로 인해 바로 확인 후 실시간 침해 처리를 하거나, 바로 볼 수 있기에 범위 확대 및 시간 단축을 할 수 있으며, 알려지지 않은 위협을 탐지하여 대비할 수 있다[4].

<그림 /> 지능형 통합보안관제 시스템

3.3.3 특징

지능형 보안관제에는 4가지의 장점이 있다. 첫째, 사이버 공격을 효율적으로 탐지할 수 있다. 탐지한 대용량 보안 로그를 실시간·장기적으로 가시화해 개별공격자 이상 행위, 공격자 간 상관관계·구조 등을 자동으로 분석한다. 이를 통해 개별 IP가 발생시킨 전체 보안 로그를 분 단위로 확인하고 공격행위를 가시화하기 때문에 지능형 지속 공격(APT)과 같은 지속·연속적으로 발생하는 사이버 공격을 효율적으로 탐지할 수 있다. 둘째, 인력 부족을 해결할 수 있다. 실시간으로 발생하는 사이버위협 이벤트들의 분석·대응과 관제 업무 프로세스의 절차를 개선하고 자동화를 도입하기에 전보다 많은 인력이 필요 하지 않는다. 셋째, 공격에 대한 대응 속도를 높일 수 있다. 정상·비정상 이벤트에 대한 지도학습을 통해 매일 기하급수적으로 생성되는 이벤트를 위험한, 덜 위험한, 위험하지 않은 순으로 선별함으로써, 공격에 대한 대응 속도를 높일 수 있다. 보안관제 요원들은 일일이 보안이벤트를 분석하는 어려움을 해소하고, 고위험군 경보에 대한 대응 속도를 높일 수 있다. 마지막 넷째, 데이터를 기반으로 이상 행위 및 악성코드를 탐지하기 때문에 미탐을 최소화할 수 있다. 트리거 조건 설정을 통한 룰 기반 탐지 방식과는 다르게 평상시 행위 및 사전학습된 데이터를 활용해 이상 행위, 악성코드 여부를 탐지하므로, 룰 기반 탐지로 인한 미탐 제약사항들을 해소할 수 있다. 또한, 대규모 이벤트의 홍수 속에서 사람이 놓칠 수 있는 이벤트들을 기계적으로 찾아내 미탐 발생을 줄인다. 단점으로는 지능형 보안관제여서 나올 수밖에 없는 2가지가 있다. 첫째, 성향적 오류와 오버피팅 오류가 나올 수 있다. 성향적 오류는 부족한 데이터로 인해 부정확한 값이 도출되는 오류를 말하고, 오버피팅은 너무 많은 데이터를 고려할 경우 즉, 사소한 값의 변화에 민감하게 반응하여 오히려 나쁜 결과값을 보여주는 것을 말한다. 이와 같이 인공지능은 시간, 신속성, 효율적인 인력운용 등이 높아 여러 방면에서 활용 가능한 기술이지만 데이터의 양(Quantity)과 질(Quality)에 따라 생각지 않은 엉뚱한 결과가 나올 수 있는 오류가 존재한다. 둘째, 시간과 비용이 많이 든다. 지도학습 러닝은 어떠한 데이터를 줄 때 출력값도 함께 주는 방식으로, 이런 값들을 통해서 기계학습을 하는 알고리즘이다. 주로 인식, 분류, 진단. 예측 등의 문제 해결에 적합하지만 좋은 결과가 나오기 위해서는 더 많은 데이터와 결과를 알려주어야 하기에 시간과 비용이 많이 든다.

3.4. 각 보안관제 비교

ESM, SIEM, 지능형(AI)의 특징, 운영과 같은 세 가지의 체계에 대해 알아보았다. 각 체계에서 다른 점이 분명히 존재하기에 관리·분석대상, 핵심 용도, 위험탐지 특징, 수집 · 저장, 수집·분석 아키텍처, 탐지오류, 사용자로 항목을 나누어 각 체계가 각 항목에서 무엇이 다른지 밑에 있는 <표 2>를 통하여 확인할 수 있다.

항목	ESM	SIEM	지능형
관리 • 분석대상	보안 시스템, 서버 시스템, 로그, Event, 경고 등	보안 시스템, 네트워크 장비, 어플리케이션 로그, 서버 시스템, 로그, Event, 경고 등	보안 시스템, 서버 시스템, 정보통신, OT, 로그, Event, 경고 등
핵심 용도	보안 위협 발생 시 대처, 시스템별 가용성 체크	• 보안 위협 예측 및 모니터링 • 지능화, 고도화, 신종 보안 위협에 대응	• 보안 위협 예측 및 모니터링 • 지능화, 고도화, 신종 보안 위협에 자동 대응
위험 탐지 특징	• 단순 패턴 기반 탐지 • 알려진 공격 위주 분석, 단기간 범위 분석	• 연관성 분석 및 탐지 • 정상상태에서의 정보 위협 등 장시간 범위 분석 수용 • 다양한 룰, 시나리오 적용(프로세스, 활동성 등)	• 정상상태에서의 정보 위협 등 장시간 범위 분석 수용 • 자동 분석 및 자동 탐지
수집 • 저장	• 모니터링에 필요한 Event 정보 • 정형 데이터 기준, 원본 로	• 모든 자원의 로그 및 정보 Event 통합 수집 • 정형/비정형	• 모든 자원의 로그 및 정보 Event 통합 수집 • 기존에 모아

	그 보관 안 함	데이터 수용, 원본 로그 보관	둔 원본 로그와 이력 데이터 등을 수집 • 정형/비정형 데이터 수용, 원본 로그 보관
수집 • 분석 아키텍처	• Agent, API 위주 데이터 수집 • 중앙처리 구조	• Agent 이외 다양한 프로토콜을 활용한 데이터 수집 • 상관 분석 및 리포트	• Agent 이외 다양한 프로토콜을 활용한 데이터 수집 • 기존에 존재하는 데이터를 통해 판단하며 스스로 학습하는 구조
사용자	보안관리자, 관제요원 위주	보안관리자, 각 업무 시스템별 담당자, 관제요원 등	보안관리자, 각 업무 시스템별 담당자, 관제요원 등
탐지 오류	오탐 • 과탐 비교적 많음(Event 위주 탐지)	오탐 • 과탐 비교적 없음(대용량 데이터 위주 탐지)	오탐 • 과탐 비교적 없음 그러나 성향적 오류와 오버피팅 오류가 있음(대용량 데이터 위주 탐지)

<표 2> 각 체계의 비교

4. 결론

본 논문에서 국내 통합보안관제 체계가 어떻게 바뀌었으며 각 체계에 대한 분석과 장단점을 분석하였다. 또한, 각 체계들을 비교하여 어떤 일에 무슨 체계를 쓴 것이 더 좋은지도 알아보았다. 앞으로의 사이버침해는 더 고도화되고 더욱 정교하며, 지금까지 경험하지 못했던 전략적인 보안 위협이 등장할 것이며, 그에 따른 많은 정보와 자산의 피해로 막대한 시간과 자본이 손실될 위험한 상황에 직면하고 있다. 이전에도 사이버 공격이나 보안에 관한 연구는 다양하게 이루어져 왔지만, 기업과 공공기관, 개인 등의 사용자를 노리는 보안 위협은 앞으로 증가 될 것으로 예상되며 이에 따라 기술에 발전의 속도만큼 사이버상의 보안 위협은 종료와 공격 방식이 빠르게 진화하고 있기 때문에 방대한 데이터를 통합적으로 분석하고 빠른시간에 선제적으로 대처할 수 있는 통합관제 체계를 빠른 시일내에 구축하고 운영돼야 한다. 현재 인공지능을 활용한 통합보안관제에서는 무엇보다 데이터가 중요하며, 이러한 데이터는 내부 데이터뿐만 아니라 외부의 보안 이슈까지도 함께 적용되어야 한다. 그러나 아직은 인공지능에 대한 부작용도 고려돼야 하고 보안 위협이 지능화되고 또 방대하게 늘어나는 만큼 기존 보안관제 운영 방식인 사람이 직접 보안 위협 정보를 찾아내고 분석 또는 대응하는 수동적인 이벤트 처리 방식의 한계를 보완해서 다양한 통합 보안관제 서비스에 활용이 가능하도록 표준화 및 공유 체계를 위한 표준적인 보안관제 연구가 지속되어야 한다고 생각한다.

5 별첨

5.1. 참고 문헌

[1] "악성코드_은닉사이트_탐지_동향_보고서(20년_하반기)", 한국인터넷진흥원, 2020
[2] "Ransomware_Special_Report", 한국인터넷진흥원, 2021
[3] 김기영, 김종현, "빅데이터 환경에서 통합 보안관제를 위한 이종 보안 정보 이벤트 수집 및 공유기술 동향", 한국정보기술학회지, 2012
[4] "인공지능을 활용한 보안기술 개발 동향", 국경완, 공병철

5.2. 발표자료

통합보안 관제 체계에 관한 연구

2021 . 10. 24

지도 교수 : 양환석 교수님

TEAM : 혼자이조

김은지

1

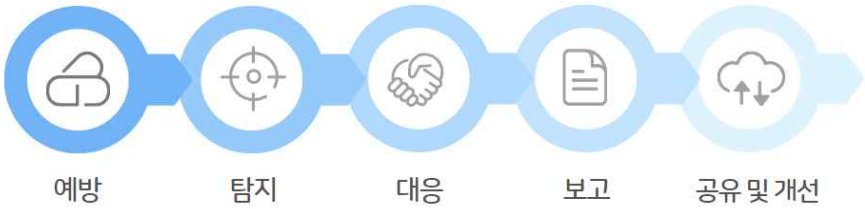
목차

- ▸통합관제 보안
- ▸ESM 보안 관제
- ▸SIM 보안관제
- ▸지능형 보안 관제
- ▸각 관제의 비교
- ▸결론

2

통합관제 보안 (1/2)

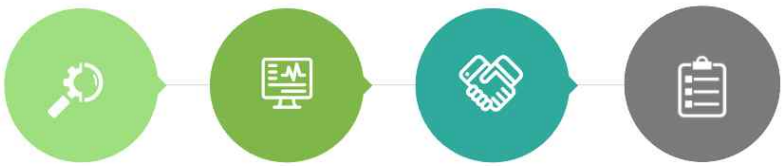
▸업무 5단계



3

통합관제 보안 (2/2)

▸서비스



원격 관제 서비스

보안장비 중심의 보안 이벤트에 대하여 상시 모니터링을 수행하는 서비스

파견관제 서비스

전문 인력을 파견받아 업무를 수행하는 서비스

자체관제 서비스

자체적으로 운영 및 관리 하는 관제 형태

클라우드 관제 서비스

클라우드 환경에 대한 관제 서비스

4

ESM 보안관제 (1/2)

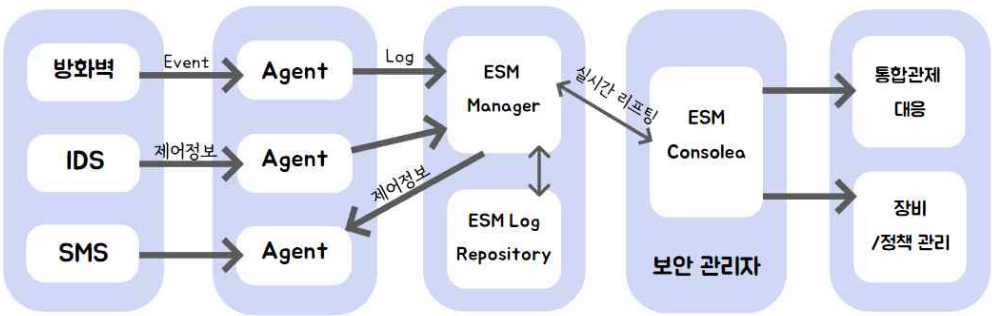
▸ 특징

하나의 통합뷰로 관리
유사한보안 정책 통합 후 적용
위험요소를 최소화

5

ESM 보안관제 (2/2)

▸ 구성도



6

SIEM 보안관제 (1/2)

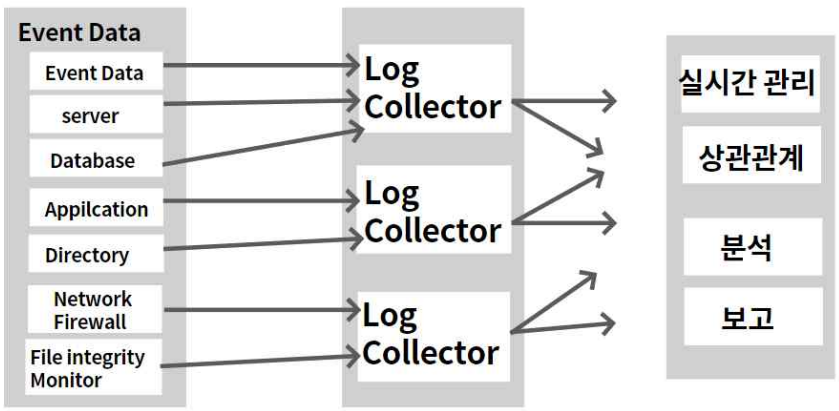
▸개요

방대한 데이터를 수집 저장
빅데이터 분석 기술로 상관 분석 가능
사이버 공격 측면을 고려 해 적극적인 대응 요구

7

SIEM 보안관제 (2/2)

▸구성도



8

지능형 보안관제 (1/2)

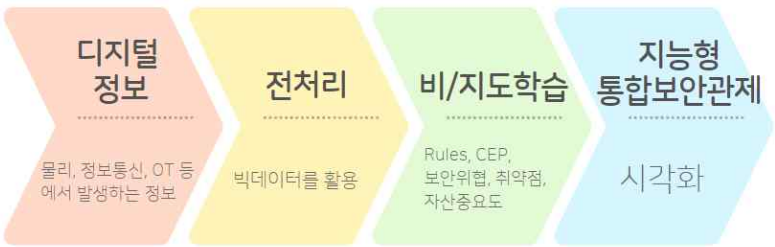
▸ 개요

사람이 해야할 일을 자동으로 돌림
비정상 행위 예측 결과가 시각화
비전문가 및 전문가에게 사용의 편리성 제공
지속적인 개선이 이루어짐

9

지능형 보안관제 (2/2)

▸ 구성도



10

비교

▸비교 분석 표

항목	관리 분석대상	핵심용도	아키텍처	사용자	탐지오류
ESM	로그, 경고 Event 등	보안 위협 발생시 대처, 가용성 체크	중앙 처리 구조	보안관리자, 관제 요원 위주	비교적 오탐/과탐이 많음 (Event 위주 탐지)
SIEM	네트워크 장비, 보안시스템, 로그, 경고 등	보안 위협 예측 및 모니터링, 신종 보안 위협에 대응	상관 분석 및 리포트	각 업무 시스템별 담당자, 관제요원 등	비교적 오탐/과탐이 적음 (대용량 데이터 위주 탐지)
지능형	보안시스템, 정보통신, OT, 로그, 경고 등	보안 위협 예측 및 모니터링, 신종 보안 위협에 대응	머신러닝	각 업무 시스템별 담당자, 관제요원 등	성향적 오류, 오버피팅 오류가 있음

11

감사합니다.

12