https://doi.org/10.5392/JKCA.2021.21.10.059

인공지능 기술의 통합보안관제 적용 및 사이버침해대응 절차 개선

Application of Integrated Security Control of Artificial Intelligence Technology and Improvement of Cyber-Threat Response Process

고광수, 조인준
배재대학교대학원 사이버보안학과

Kwang-Soo Ko(kremlin7@naver.com), In-June Jo(injune@pcu.ac.kr)

요약

본 논문에서는 통합보안관제에 인공지능 기술을 적용하고, 기존 보안관제와 인공지능 보안관제의 대응절차를 일원화한, 개선된 통합보안관제 절차를 새롭게 제안하였다. 현재의 사이버보안관제는 사람의 능력 수준에 의존도가 매우 높다. 그래서 사람에 의해 여러 이기종 장비에서 발생하는 다양한 로그를 분석하고, 급증하는 보안이벤트를 모두 분석·처리한다는 것은 사실상 무리가 있다. 그리고 문자열과 패턴 일치로 탐지하는 시그니처 기반의 보안장비는 APT(Advanced Persistent Threat)와 같은 고도화·지능화된 사이버공격을 정확히 탐지하기에 기능상 부족한 면이 있다. 이러한 문제들을 해결하기 위한 방안으로 인공지능 지도·비지도학습 기술을 사이버공격 탐지 및 분석에 적용하고, 이를 통해 수 없이 많이 발생하는 로그와 이벤트의 분석을 자동화하여, 고도화된 사이버공격의 지속적인 발생을 예측·차단할 수 있도록 하여 전반적인 측면에서 대응수준을 높였다. 그리고 보안관제에 인공지능 기술을 적용한 후 AI와 SIEM의 중복 탐지 등의 문제점을 일원화 된 침해대응 프로세스(절차)로 통합·해결함으로써 개선된 통합보안관제 서비스 모델을 새롭게 제안하였다.

■ 중심어 : | 통합보안관제 | 인공지능 | 지도·비지도학습 | SIEM |

Abstract

In this paper, an improved integrated security control procedure is newly proposed by applying artificial intelligence technology to integrated security control and unifying the existing security control and AI security control response procedures. Current cyber security control is highly dependent on the level of human ability. In other words, it is practically unreasonable to analyze various logs generated by people from different types of equipment and analyze and process all of the security events that are rapidly increasing. And, the signature-based security equipment that detects by matching a string and a pattern has insufficient functions to accurately detect advanced and advanced cyberattacks such as APT (Advanced Persistent Threat). As one way to solve these pending problems, the artificial intelligence technology of supervised and unsupervised learning is applied to the detection and analysis of cyber attacks, and through this, the analysis of logs and events that occur innumerable times is automated and intelligent through this. The level of response has been raised in the overall aspect by making it possible to predict and block the continuous occurrence of cyberattacks. And after applying AI security control technology, an improved integrated security control service model was newly proposed by integrating and solving the problem of overlapping detection of AI and SIEM into a unified breach response process(procedure).

■ keyword : | Integrated Security Control | Artificial Intelligence | (Un)Supervised Learning | SIEM |

접수일자 : 2021년 07월 06일
수정일자 : 2021년 09월 13일
심사완료일 : 2021년 09월 13일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

1. 연구의 배경 및 목적

현 시대는 초고속 인터넷, 모바일 4, 5세대 등 통신기술의 발전과 인터넷 연결이 가능한 통신 단말(컴퓨터, 스마트폰, 태블릿PC, 자율주행 자동차 등)의 유형 증가에 따라 대량의 사이버위협이 시도되고 있으며, 사이버공격 기술 또한 나날이 진화, 고도화되고 있다[1].

한국인터넷진흥원(KISA)의 2020년 하반기 사이버위협 악성코드 은닉사이트 탐지 동향 보고서에 따르면 악성코드 유포지 탐지 및 대응 현황은 2020년 상반기 대비 26%(326건→412건) 증가, 2019년 하반기 대비 70%(243건→412건) 증가 된 추이를 [그림 1]을 통하여 확인이 가능하다[2].

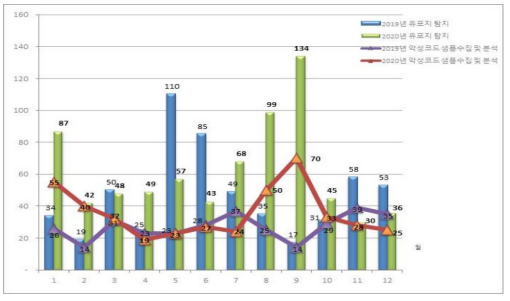

그림 1. 2020년 악성코드 탐지·대응 동향

이러한 고도화, 지능화 그리고 대량화되고 있는 사이버공격에 대응하기 위해 공공·민간을 구분하지 않고 많은 학교, 연구기관, 공공기관, 민간기업에서 최적의 사이버공격 대응기술에 대해 연구가 진행되고 있다. “2021 e-GISEC(e-Government Information Security Solution Fair, 전자정부 정보보호 솔루션 페어)”이라는 공공·민간 최대의 정보보호 컨퍼런스를 통해서도 빅데이터, 클라우드, 인공지능 등 차세대 기술 기반 정보보안 세미나와 솔루션이 주류를 이루고 있는 것을 볼 수 있으며, 이러한 대응기술 중에서도 “인공지능”과 관련된 세션 수가 총 세션 20여개 중 7개로 30%가 넘는 많은 비중을 차지하고 있었다.

결과적으로 끊임없이 고도화, 다양화되고 있는 사이버공격 기술에 선제적이고 효과적인 대응을 위해, 그리고 대량의 위협 이벤트를 분석하여 대응하기 위해서는 인공지능(머신러닝) 기술에 기반 한 대응이 유용 하다는 것을 해당 컨퍼런스를 통해서도 알 수 있다.

이러한 추세가 의미하는 것은 통합보안관제 솔루션(Security Information & Event Management)의 진화를 요구하고 있다는 것이다. 즉, SIEM에 인공지능 기술을 추가 적용하여 보안관제의 고도화 및 자동화가 가능한 능동적인 대응 솔루션이 필요함을 나타낸 것으로 볼 수 있다[3].

2. 연구의 내용 및 범위

본 논문에서는 빅데이터로그 기반 SIEM을 진화시켜, 당면한 사이버보안관제의 문제점 개선 방안을 제안하였다. 기본 구상은 최근의 추세를 반영, 인공지능기술을 보안관제 영역에 도입하여 SIEM 기반 보안관제의 난제들을 기술적으로 극복하고, 기존 보안관제와 인공지능 보안관제간의 긴밀한 연계를 통해 보다 개선된 통합보안관제 체계의 절차적 통합 방안을 제시하였다. 논문의 구성으로 제 II장에서는 관련 연구로서 기존 통합보안관제 체계의 현황과 문제점, 그리고 인공지능 기반 보안관제 체계의 필요성에 대하여 서술하였다. 제 III장에서는 인공지능 기술인 지도학습(Supervised Learning)과 비지도학습(Unsupervised Learning) 알고리즘을 보안관제에 심층 적용하고, 이를 통해 기존 보안관제 문제점의 구체적인 해결 방안을 제시하였다. 제 IV장은 앞 장에서 제시된 인공지능 보안관제와 기존 보안관제의 개별적 동작에 의한 보안관제 한계를 정리하고, 이를 개선하기 위한 보안관제 프로세스 통합 절차 방안을 제안하였다. 그리고 제 V장은 본 연구의 결론으로 연구의 결과를 정리하고 향후 인공지능 보안관제가 나아가야할 연구 방향에 대하여 기술하였다.

II. 관련 연구

본 장에서는 관련 연구로서 기존의 SIEM에 기반한 통합보안관제 체계의 현황과 문제점 그리고 인공지능 기술 기반의 보안관제 필요성에 관련된 내용을 요약하였다.

1. 기존 통합보안관제 체계의 현황과 문제점

초기의 보안관제는 방화벽, IDS, IPS, WAF 등 개별 보안장비의 로그를 직접 조회하여 대응하였다. 이러한 보안관제는 여러 이기종 장비에서 발생하는 로그들을 종합적으로 수집하고, 검색 등을 통해서 관제가 가능한 통합보안관리(ESM, Enterprise Security Management)의 형태로 진화하였다. 최근에는 여러가지 다양한 종류의 장비 로그와 이벤트들을 수집·저장함에 따라 대량의 방대한 데이터가 쌓이게되고 이를 빅데이터 분석기술을 활용하여 상관분석을 할 수 있는 SIEM기반의 보안관제가 주류를 이루고 있다는 것을 [그림 2]을 통해 볼 수 있다[4].

그림 2. 보안관제 기술 변화

그러나 각 장비에서 기하급수적으로 증가하고 있는 로그와 보안 이벤트의 분석과 그리고 웹사이트 해킹, 랜섬웨어 감염, 개인정보 유출, 모바일을 이용한 소셜 네트워크 계정 탈취시도 등 다양한 유형의 사이버공격 측면을 고려할 경우 기존의 SIEM은 다음과 같은 문제점들을 지니고 있다.

첫째, 빅데이터로그분석의 기술이 미포함된 솔루션이라면, 침해사고로 이어질 수 있는 위협시도에 대한 상관분석이 어려운 문제점을 들 수 있다. 또한 보안 부서의 부족한 인력으로는 적게는 수십만건에서 많게는 수십억건 이상 발생하는 보안이벤트를 누수 없이 모두 분석한다는 것은 사실상 불가능한 것이 현실이다[5]. 둘째, 사이버위협에 대응하는 전문 보안인력의 기술수준 편차로 인해 해커(크래커)의 사이버공격이 정상적인 행위로 판단(미탐) 된다거나, 정상적인 행위가 사이버위협시도로 판단(오탐)이 될 가능성이 존재 한다. 이와 같은 내용은 [그림 3]의 통계자료를 통하여 확인이 가능하다[6]. 셋째, 지능화 등 복잡도가 점점 높아지고 있는 APT(Advanced Persistent Threat)와 같은 사이버공격은 현재의 패턴, 시그니쳐 등 문자열 일치로 탐지하기에는 한계가 있다. 또한 이들의 분석은 많은 시간을 필요로 한다[7].

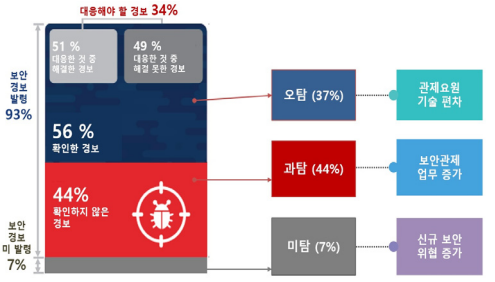

그림 3. 위협탐지 누수(미탐·오탐)

이와 같은 기존의 SIEM이 갖고 있는 문제점들 때문에 고도화 된 사이버공격의 탐지와 심층적 분석을 위해서는 보다 발전된 대응기술의 개발 및 실용화가 절실한 상황이다[8].

2. 인공지능 기반 통합보안관제 체계의 필요성

기존의 SIEM 기반 통합보안관제 체계에 내재된 문제점으로 누수 없는 보안 이벤트의 대응 미흡, 보안 인력들의 기술 수준 편차로 인한 오판단 그리고 지속적이고, 지능화된 복잡도가 높은 사이버공격의 탐지 및 분석이 어려움을 들었다. 이러한 문제들을 해결하기 위한 방안으로 자동화·고도화가 가능한 인공지능 보안기술을 들 수 있다[9]. 즉, 인공지능 기술을 보안관제에 도입한다면, 사이버공격을 탐지하고, 분석하고, 대응하는 절차 및 방법 등이 자동화 및 고도화 되어 전통적인 통합보안관제의 문제점들을 해결할 수 있다. 그리고 기존의 보안관제에서 필연적으로 내재된 위험을 낮출 수 있고, 인력과 시간 배분도 가능하게 되어 인력자원을 더 의미있고 중요한 부분에 많이 투입할 수 있게 될 것이다.

결과적으로 수없이 많이 발생하는 보안 이벤트를 사람이 아닌 인공지능 보안관제솔루션에서 처리가 가능하다면 누수 없는 이벤트의 처리와 사람의 기술 수준 편차로 인한 잘못된 대응이 감소 될 것이고, 인공지능

보안관제솔루션이 처리한 보안이벤트 만큼의 절감된 인력자원과 시간을 좀 더 심층 분석이 필요한 복합적 사이버공격의 대응에 사용할 수 있게 될 것이다.

Ⅲ. 기존 보안관제의 문제점 해결을 위한 인공지능 기술의 심층 적용

본 장에서는 인공지능 기술을 보안에 응용한 다른 문헌 연구 사례와는 달리, 실제 보안관제 현장에서 나타나고 있는 애로사항을 중점으로 기존 보안관제의 탐지·대응 문제점 해결 방안을 제시하였다.

1. 인공지능 지도학습 알고리즘의 보안관제 적용을 통한 보안 이벤트 위협 판단 자동화

본 절에서는 인공지능 지도학습 알고리즘의 보안관제 적용을 통해 수많은 사이버공격 보안이벤트의 정·오탐 판단(예측)을 자동화 함으로써 기존 보안관제의 문제점 해결방안을 제시하였다.

사이버공격을 탐지·대응하는 현장(사이버 보안관제센터)에서 가장 많이 탐지되는 종류의 위협시도는 패턴일치로 분류 되는 보안 이벤트이다. 이는 문자열과 바이너리 패턴 즉, 시그니처 기반의 탐지가 가능한 침입방지시스템(Intrusion Prevention System), 웹방화벽(Web Application Firewall) 등 보안장비가 발생시키는 로그, 경보를 통해 위협을 탐지하는 것이다. 이런 장비를 이용한 탐지는 한 번의 공격시도 안에서도 패턴만 일치 한다면 여러 건의 보안이벤트가 발생될 수 있기 때문에 자동화 처리의 기능이 필수적이다. 이러한 대량의 보안이벤트를 효과적으로 처리하기 위한 지도학습 알고리즘의 보안관제 적용 방안은 다음과 같다. 인공지능 지도학습 알고리즘은 [그림 4]와 같이 여러 사례의 문제와 답을 미리 학습시켜 새로운 질문에 답을 내릴 수 있도록 하는 학습 모델이다.

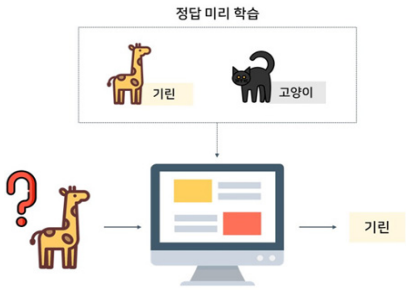

그림 4. 지도학습 알고리즘 원리

쉽게 설명해서 동물(기린, 고양이)에 대한 모양과 이름의 사례들을 학습 시켜, 새로운 동물의 질문에 대해 답을 내리게 하는 인공지능 기술이다. 이러한 지도학습은 CATBoost(범주형 문제처리), Stochastic Gradient Descent(확률적 경사 하강법) 등의 머신러닝 알고리즘을 사용하여 시그니처 기반 사이버공격 탐지 부분에 적용한다.

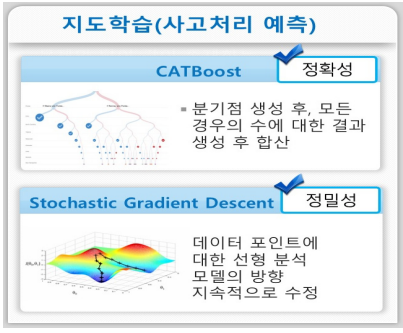

그림 5. 인공지능 지도학습 알고리즘

즉 5년 이상의 숙련된 보안관제 전문가가 처리한(검증된) 사이버공격 탐지·대응 결과(탐지문자열, 규칙, 분석내용, 처리결과 등)를 [그림 5]와 같이 지도학습 알고리즘을 통해 학습을 수행한다. 그리고 이러한 사례를 지속적으로 추가 학습 시킨다면, 시그니처 기반 보안이벤트를 스스로 분석하고 판단할 수 있는 위협 모델이 생성되고, 이를 통해 신뢰성이 보장된 자동화 처리 보안이벤트 대응이 가능하게 되는 것이다.

이렇게 인공지능 지도학습 알고리즘의 적용을 통해 개선 될 수 있는 주요사항은 3가지로 볼 수 있다. 첫째

수없이 많이 발생하는 보안이벤트에 대한 위협 여부 즉, 정·오탐 판단(예측) 자동화이며, 둘째 자동화 공격도구에 의한 기계적인 단순·반복 업무처리 해소(대부분 오탐)이고, 셋째 숙련되지 않는 초급 보안관제 인력의 판단 실수로 인한 장애, 침해사고 등의 방지 효과가 있다. 그러므로 인공지능 지도학습 기술의 통합보안관제 적용을 통해 인적·시간적 자원의 절감과 위협상황을 초래할 수 있는 요인을 사전에 제거할 수 있다.

2. 인공지능 비지도학습 알고리즘의 보안관제 적용을 통한 이상행위 위협 탐지

본 절에서는 인공지능 비지도학습 알고리즘의 보안관제 적용을 통해 기존의 보안관제체계에서 탐지하기 어려운 복합적 이상행위(Anomaly Action)등의 고도화된 사이버공격 탐지방안을 제시한다.

APT(지속적 지능형 위협) 등 진화하는 사이버공격은 문자열이나 패턴 등의 일치로 탐지하기에는 한계가 존재 한다. 일회성이 아닌 오랜기간 동안의 지속적인 공격이기 때문이다. APT 공격의 절차와 특성을 보면 ① 공격자는 취약성 정보수집을 위해 대상시스템에 여러 종류의 위협시도를 오랜 기간 수행하며, ②해당 행위를 통해 수집된 취약점을 기반으로 2차 공격을 실행 하여 계정 등을 탈취하고, ③획득한 권한을 통해 대상시스템에 접속하여 중요정보 수집 및 유출 시키고, ④급기야 해당 시스템 or PC를 분산서비스거부 공격(Distributed Denial of Service)의 좀비로도 사용될 수 있게 하는 순서로 진행 되는 복합적인 사이버공격이다. 이러한 복합적 위협상황의 탐지를 위한 인공지능 비지도학습 알고리즘 기반 보안관제 기술 구현방안은 다음과 같다.

인공지능 비지도학습 알고리즘은 지도학습과 접근방식이 다르다. 그림 6에서 보는 바와 같이 답의 제공 없이 여러 문제들을 입력하면 인공지능이 스스로 분류하고 판단하여 결과값을 도출하는 학습모델이다. 다시 말해서 여러 가지 동물들에 대한 입력값이 주어지면 군집화, 차원축소 등의 세부 알고리즘을 통해 데이터 특성을 스스로 파악하는 인공지능 기술이다.

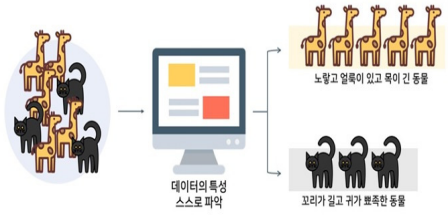

그림 6. 비지도학습 알고리즘 원리

이러한 비지도학습 기술은 Auto Encoder(중요도 높은 필수적인 필드 자동 계산), Angel Based Outlier Detection(데이터 상호간 분포를 통한 특이점 계산), Isolation Forest(기준점 정상 및 비정상치 탐지)와 같은 딥러닝(Deep Learn) 알고리즘을 사용하며, 이를 APT 공격과 같은 복합적 사이버위협 탐지 부분에 적용하는 것이다.

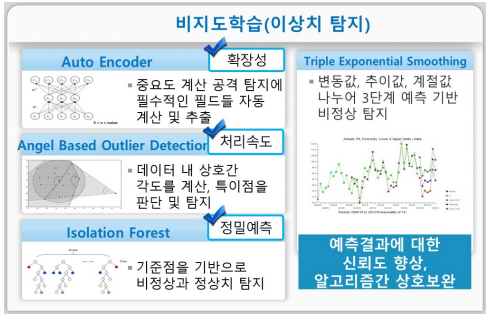

그림 7. 인공지능 비지도학습 알고리즘

APT와 같은 복합적 공격은 다수의 접근시도, 여러 가지 유형의 공격시도, 그리고 오랜 기간 지속적이라는 형태를 보여 준다. 이러한 특성을 탐지하기 위해서는 방화벽, 웹서버 등 접근시도와 데이터 전송량을 확인할 수 있는 장비의 로그들을 비지도학습 알고리즘으로 인공지능에 학습을 시킨다. 이렇게 비지도학습 알고리즘에 적용하면 [그림 7]과 같이 비슷한 유형의 행위들이 분류가 되는 것을 볼 수 있다. 그렇다면 군집된 분류중 많은 내용은 정상적인 행위일 가능성이 높고, 적은 내용중 비정상 행위 즉 우리가 탐지 하고자 하는 이상행위들을 확인할 수 있을 것이다. 이를 통해 APT와 같은 복합적 사이버공격들의 개별적 이상행위를 탐지할 수

있으며, 각 공격 행위를 차단하여 사이버킬체인(Cyber Kill Chain)의 효과를 볼수가 있다. 결과적으로 기존의 규칙 기반 단순 공격 탐지에서 감지할 수 없었던 지능화, 고도화 된 공격들을 탐지하고, 차단하여 차후에 발생 가능한 큰 위험상황을 예방할 수 있다.

이렇게 인공지능 비지도 학습 알고리즘의 적용을 통해 크게 다음과 같은 4가지, 즉 ①외부에서 내부시스템으로의 과도한 접근 ②비인가된 서비스로의 다수 접속 시도 ③한 대 또는 다수 시스템으로의 불필요 트래픽 발생 ④내부 PC 및 시스템에서 외부로의 많은 데이터 전송 등의 이상행위를 탐지·대응할 수가 있다.

이렇게 인공지능의 2가지 알고리즘 즉, 지도·비지도 학습 기술의 보안관제 적용으로 [표 1]과 같이 기존 보안관제의 문제점이 해결되고, 이를 통해 향후 발생 가능한 내재적, 잠재적 위험을 감소시킬 수 있다.

표 1. 기존 보안관제와 인공지능 보안관제 비교

구분	비교 내용
SIEM(기존) 보안관제	• 대량 발생 보안 이벤트의 모든 처리 어려움 • 시그니쳐 기반 단일 위협 탐지에 의존 • 사람의 보유 기술력에 따라 대응 수준 상이
인공지능 기반 보안관제	• 대량 발생 보안 이벤트 자동화 예측 처리 • APT와 같은 복합적 지속적 공격 대응 가능 • 사람의 기술력 편차로 인한 오대응 감소

Ⅳ. 사이버침해대응 절차 개선 방안 제안

본 장에서는 3장에서 제시된 인공지능 기술을 보안관제의 현장 적용·활용시 나타한 한계를 기술하고, 이를 해결하기 위해 기존 보안관제와 인공지능 기반 보안관제의 연계를 통한 침해대응 절차 개선 방안에 대하여 기술하였다.

1. 인공지능 보안관제 솔루션의 실제 보안관제 활용 한계

인공지능의 보안관제 적용을 통하여 인적·시간적 자원을 절감과 잠재적 위험을 예방할 수 있는 효과가 나타났다. 하지만 해당 기술을 보안관제 현장에 구축하여 적용한 결과 3가지 문제점이 확인 되었다. 첫째 기존의 보안관제와 인공지능 보안관제가 서로 개별로 동작한다는 것이다. 보안관제 운영자는 중복 이벤트가 발생하는 두 시스템의 탐지 결과를 모두 확인해야 하는 어려움이 발생하였다. 둘째 인공지능 보안관제의 탐지 이벤트가 [그림 8]에 보는 바와 같이 매우 많이 발생하여 운영자가 전체를 분석 하는 것은 시간적으로 불가능하였다. 셋째 인공지능 보안관제의 탐지 결과는 해당 위협에 대한 위험도 예측이기 때문에 보안관제 운영자가 재검증해야 하는 상황은 심리적으로 가장 큰 애로사항이다.

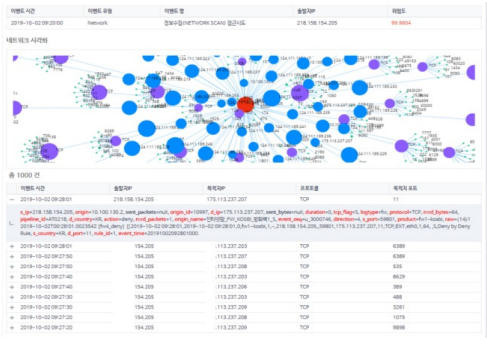

그림 8. 인공지능 보안관제 솔루션 탐지

이렇게 인공지능 기술의 보안관제의 일선 적용시 이론과 현실이 괴리되는 현상들이 나타났다. 하지만 이런 현장에서 도출된 어려움과 문제점들을 해결 한다면 기술적으로 한 단계 더 진보한 위협탐지를 할수 있다. 그리고 탐지결과의 신뢰성을 좀 더 향상시킬 수 있는 개선된 통합보안관제체계로 발전할 수 있을 것이다.

2. 인공지능 보안관제와 기존 보안관제 프로세스의 연계를 통한 개선된 사이버침해대응 절차 방안 제안

인공지능 보안관제 기술을 활용하는데 있어, 한계상황을 해결하기 위해서는 여러가지 방안이 있을 수 있다. 본 절에서는 하나의 방안으로 접근성이 가장 용이한 기존의 통합보안관제(SIEM 이용)와 인공지능 보안관제의 침해대응 절차(프로세스)를 통합하는 방안을 다음과 같이 제안하였다.

두 보안관제의 동작을 새롭게 일원화된 침해대응 프로세스로 통합한다. 이는 별개의 기능으로 동작하여 결과가 각각 출력 되었던 보안관제의 형태를 각 보안관제의 핵심기능에 근거하여 적절한 침해대응 절차의 위치에 새로이 배치하는 방안이다. 구체적으로 보면 기존의 '1.접수 〉 2.판단 〉 3.대응 〉 4.완료'인 4단계 침해대응 절차에 인공지능의 탐지결과를 반영하고, 최종 처리결과를 인공지능에 학습시키는 '1.접수 〉 (2.1 판단 〉 2.2 인공지능 예측값) 〉 3.대응 〉 (4.1 완료 〉 4.2 최종 처리 내용 인공지능 학습)'의 구조로 통합·개선하는 것이며, [그림 9]과 같이 직렬화 및 순환된 침해대응 프로세스 안에 기존 보안관제와 인공지능 기반 보안관제가 서로 최적의 위치에서 동작할 수 있는 새로운 탐지·대응 방안이 도출되는 것이다.

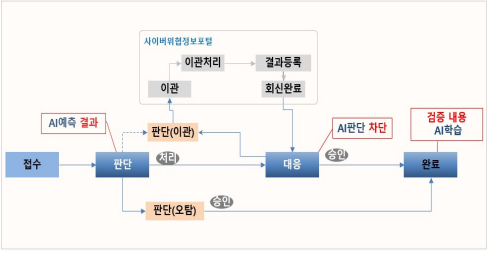

그림 9. 기존 보안관제와 인공지능 보안관제의 침해대응 절차 통합 흐름도

이러한 획기적인 보안관제 침해대응 프로세스 통합으로 첫째, 한 번의 보안이벤트 대응으로 관제 업무를 처리할 수 있다. 둘째, SIEM의 상관분석 기능을 활용하여 대량으로 발생되는 탐지 결과를 그룹핑 하여 대응할 수 있다. 셋째, 각 솔루션 간 처리 결과 값이 자동으로 서로에게 피드백 되어 탐지 위험도 예측 신뢰성이 지속적으로 향상 된다는 것이다. 즉, 인공지능 기술 기반 보안관제의 '위험도 예측' 학습이 자동화 된다는 것이다. 이것을 통해 정·오탐 판단의 신뢰성이 높아지고, 불필요한 탐지 이벤트가 감소되는 놀라운 효과를 볼 수 있다 [표 2]. 결과적으로 모든 것을 스스로 처리하고 학습하는 완전한 인공지능 보안관제는 아니지만, 사람의 일부 시스템 처리 프로세스 개입을 통해 점점 더 탁월한 성능을 발휘할 수 있는 솔루션으로 진화가 가능하게 되는 것이다.

표 2. SIEM 및 인공지능 보안관제 침해대응 절차 통합 전·후

구분	비교 내용
통합 전	• 독립적 동작으로 인한 탐지 결과 중복 발생 • 각 보안관제 탐지 이벤트의 대량 생성 • 두 솔루션의 탐지 결과 모두 검증 필요
통합 후	• 대응 절차 일원화를 통해 중복 탐지 제거 및 1번의 검증으로 이벤트 처리 가능 • 지속적인 피드백을 통한 탐지 신뢰성 향상(불필요 탐지 제거) 및 자가 학습체계 구현

V. 결론 및 시사점

본 논문에서는 인공지능 기술 기반 보안관제를 통하여 기존 보안관제의 문제점들을 해소할 수 있는 방안과 통합보안관제 침해대응 절차 통합 방안을 제안하였다. 학술적으로는 기존 전통적인 보안관제의 개선을 위해 AI 보안관제의 심층 기술적용 및 기존 보안관제와 AI 보안관제 체계의 대응절차 통합으로 향상된 보안관제 방안을 제시하였으며, 비즈니스적으로는 해당 방안을 적용한 통합 인공지능보안관제솔루션의 개발 여지를 마련하였다. 하지만 본 논문의 실질적인 적용과 지속적으로 발전하는 사이버공격기술에 대응하기 위해서는 다음과 같은 핵심 고려사항의 전제조건과 향후 지속적인 연구가 필요하다. ①전방위적인 분석을 위한 로그 수집 유형의(분석 인자) 확장, ②오랜기간의 로그 원본을 저장하고 빠른 시간에 분석할 수 있는 빅데이터 저장·분석 기술, ③수많은 노하우가 담겨 있어 어느 곳에서나 활용 가능한 수준 높은 인공지능 보안관제 표준 위협모델, ④최종적으로 자동으로 학습되고 스스로 진화 되어 가는 인공지능 학습체계 등의 기술발전이다 [10].

논문을 마치며 이러한 선진 기술들의 지속적인 연구를 통하여 보다 안전한 사이버 세상을 만들어 가는 데 이바지되길 기대한다.

참 고 문 헌

[1] 국경완, 공병철, *인공지능을 활용한 보안기술 개발 동향*, 정보통신기획평가원, 2019.

[2] 한국인터넷진흥원, 악성코드_은닉사이트_탐지_동향_보고서(20년_하반기), 2020.
[3] 김기영, 김종현, "빅데이터 환경에서 통합 보안관제를 위한 이종 보안정보 이벤트 수집 및 공유기술 동향," 한국정보기술학회지, 제10권, 제3호, pp.23-30, 2012.
[4] https://www.igloosec.com
[5] 최동열, 안은영, "빅데이터를 이용한 자동 이슈 분석 시스템," 한국콘텐츠학회논문지, Vol.20, No.2, pp.240-247, 2020.
[6] Cisco 2018 Security Capabilities Benchmark Study, 2018.
[7] 유홍렬, 정성미, 권태경, "새롭게 진화하는 위협의 패러다임 - 지능형 지속 위협(APT)," 전자공학회지, Vol.41, No.4, pp.16-30, 2014.
[8] 김규일, 박학수, 최지연, 고상준, 송중석, "보안관제 효율성 제고를 위한 실증적 분석 기반 보안이벤트 자동검증 방법," 정보보호학회논문지, Vol.24, No.3, pp.507-522, 2014.
[9] 류권상, 최대선, "인공지능 보안 공격 및 대응 방안 연구 동향," 정보보호학회지, Vol.30, No.5, pp.93-99, 2020.
[10] 이세호, 조인준, "사이버보안 프레임워크 기반의 보안 오케스트레이션 서비스 모델 제안," 한국콘텐츠학회논문지, Vol.20, No.7, pp.618-628, 2020.

저 자 소 개

고 광 수(Kwang-Soo Ko) 정회원

- 2001년 2월 : 한밭대학교 전자계산학과 공학사
- 2013년 10월 ~ 현재 : 이글루시큐리티 정보보호, 사이버안전센터 PM
- 2021년 8월 : 배재대학교 사이버보안학과 공학석사

〈관심분야〉 : 정보보호, 침해분석, 보안관제, 빅데이터 로그분석, 인공지능

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 학사
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1991년 ~ 현재 : 컴퓨터시스템응용기술사
- 2006년 ~ 현재 : 정보시스템수석감리원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 컴퓨터시스템응용, 정보시스템감사