https://doi.org/10.5392/JKCA.2021.21.01.531

인공지능기반 보안관제 구축 및 대응 방안

Artificial Intelligence-based Security Control Construction and Countermeasures

홍준혁, 이병엽
배재대학교 사이버보안학과

Jun-Hyeok Hong(ehong78@naver.com), Byoung Yup Lee(bylee@pcu.ac.kr)

요약

사이버 상의 공격과 범죄가 기하급수적으로 증가와 해킹 공격들이 지능화, 고도화되면서 해킹 공격방법 및 루트가 복자하고 예측 불가능하게 진화하고 있어 실시간으로 범죄 발생을 예측, 예방과 대규모의 지능적인 해킹 공격에 대한 선제적 대응력 강화하기 위해 스스로 학습해 이상 징후를 감시 및 공격을 차단하여 대응하는 인공지능을 활용한 차세대 보안 시스템 구축을 통한 인공지능기반 보안관제 플랫폼 개발 방안을 제시하고자 한다. 인공지능기반 보안관제 플랫폼은 데이터 수집, 데이터 분석, 차세대 보안체계 운영, 보안체계 관리 등의 기반으로 개발되어야 한다. 빅데이터 기반과 관제시스템, 외부위협정보를 통한 데이터 수집 단계, 수집된 데이터를 전처리 후 정형화시켜 딥러닝 기반 알고리즘을 통해 정·오탐 선별과 이상행위 분석 등을 수행하는 데이터 분석 단계, 분석된 데이터로 통해 예방·관제·대응·분석과 유기적 순환구조의 보안체계를 운영하여 신규위협에 대한 처리범위 및 속도향상을 높이고 정상기반과 비정상행위 식별 등을 강화시키는 차세대 보안체계 운영, 그리고 보안위협 대응 체계 관리, 유해IP 관리, 탐지정책 관리, 보안업무 법제도 관리이다. 이를 통해 방대한 데이터를 통합적으로 분석하고 빠른 시간에 선제적으로 대처가 될 수 있도록 방안을 모색하고자 한다.

■ 중심어 : | 인공지능 | 플랫폼 | 빅데이터 | 딥러닝 | 보안체계 | 알고리즘 |

Abstract

As cyber attacks and crimes increase exponentially and hacking attacks become more intelligent and advanced, hacking attack methods and routes are evolving unpredictably and in real time. In order to reinforce the enemy's responsiveness, this study aims to propose a method for developing an artificial intelligence-based security control platform by building a next-generation security system using artificial intelligence to respond by self-learning, monitoring abnormal signs and blocking attacks.The artificial intelligence-based security control platform should be developed as the basis for data collection, data analysis, next-generation security system operation, and security system management. Big data base and control system, data collection step through external threat information, data analysis step of pre-processing and formalizing the collected data to perform positive/false detection and abnormal behavior analysis through deep learning-based algorithm, and analyzed data Through the operation of a security system of prevention, control, response, analysis, and organic circulation structure, the next generation security system to increase the scope and speed of handling new threats and to reinforce the identification of normal and abnormal behaviors, and management of the security threat response system, Harmful IP management, detection policy management, security business legal system management. Through this, we are trying to find a way to comprehensively analyze vast amounts of data and to respond preemptively in a short time.

■ keyword : | Artificial Intelligence | Platform | Big Data | Deep Learning | Security System | Algorithm |

접수일자 : 2020년 10월 20일
수정일자 : 2020년 11월 17일
심사완료일 : 2020년 11월 17일
교신저자 : 이병엽, e-mail : bylee@pcu.ac.kr

I. 서 론

사이버 위협은 지능화·조직화된 형태로 진화하고 있고, 보안 환경이 전례 없이 빠른 속도로 변화함에 따라 보안 전문가들의 고민은 더욱 깊어지고, 머신러닝과 인공지능 기술을 활용한 보안 솔루션이 요구되고 있다. 정교한 공격방법으로 인프라와 조직의 허점을 파고드는 공격자들이 점점 늘어나면서 천천히 시간을 들여 모든 정보를 살펴 시키거나 회사 시스템을 무력화 시키는 등 기업과 기관의 경영활동에 적지 않은 파장을 불러일으키고 있다. 또한 4세대(LTE) 이동통신보다 최대 20배 빠른 속도, 10배 많은 loT 장비의 연결, 10배 짧은 Low-Latency 서비스를 제공하기 위해 5G세대 이동통신이 세계최초로 상용화되면서 5G서비스의 개방성, 확장성, 유연성을 제공하기 위해 채택한 분산화 코어 네트워크 구조와 software 기반 아키텍처 기술적 변화는 새로운 공격 접근경로와 논리적인 보안 가시성과 복잡성 이슈가 되고 있고, 5G, loT, AI, 클라우드, 빅데이터 등 정보통신기술(ICT)의 발전으로 시작된 4차 산업혁명은 기술과 산업의 융합을 통해 DT(Digital Transformation) 시대의 시작을 알리며, 사람과 사람은 물론 사람과 사물간의 유기적인 결합을 통한 새로운 가치창조가 가능한 초연결사회(Hyper-connected society)로 이끌고 있다[1]. 산업전반의 디지털 전환이 가속화됨에 따라 business 민첩성과 IT인프라 구축 및 운영비용의 효율화를 목적으로 Cloud에 대한 관심이 급증되고 있다. 국내·외 클라우드 시장은 Cloud 관련 규제가 완화됨에 따라 공공·금융·민간 분야의 클라우드 서비스를 도입되고 있다. 그리고 중요 기반시설(에너지, 금융, 교통 등)을 타깃과 지능화, 조직화된 범죄 양태로 진화하고 유·무선 인프라의 고도화, 스마트기기 보급 확대 등 초 연결사회 도래로 사이버 상의 공격과 범죄가 기하급수적으로 증가와 전 해커들이 나날이 지능화, 고도화하면서 해킹 공격방법 및 루트가 복잡하고 예측 불가능하게 진화하고 있어서 머신러닝과 인공지능 기술을 활용하여 사이버공격의 발생환경, 유형, 빈도 등을 분석해서 실시간으로 범죄 발생을 예측, 예방과 대규모의 지능적인 해킹 공격에 대한 선제적 대응력 강화 및 기존 보안인력의 업무효율성 위해 방대한 보안 빅데이터를 스스로 학습해 모든 보안이상 징후를 감시 및 공격을 차단하여 대응하는 차세대 보안관제 체계 연구와 딥러닝 기반의 핵심 알고리즘 관련 문헌 연구를 통해 인공지능기반 보안관제 플랫폼 개발 방안을 제시하고자 한다.

II. 인공지능기반 보안관제 플랫폼 개발 방안

본 논문에서 제안하는 인공지능기반 보안관제 플랫폼은 공공기관 또는 민간기업 사이버안전센터에서 운영하고 있는 보안관제 프로세스에서 인공지능을 활용하여 각 단계별(수집→분석→대응→관리) [그림 1] 특징과 절차 등을 보완하고 딥러닝 기반의 알고리즘을 통한 분석기술과 새로운 대응 보안 기술을 통해 기존에 보안관제 전문 인력이 수동으로 직접 수행하였던 업무 내용들을 인공지능기반 보안시스템에서 자동화하여 알려진 공격과 알려지지 않은 사이버 공격에 대해 보다 효율적이고 정확한 침해사고 대응이 가능하도록 하기 위한 개발 방안이다.

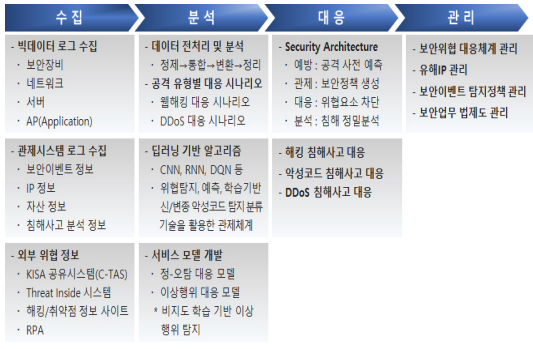

그림 1. 인공지능기반 보안관제 플랫폼

1. 데이터 수집

데이터 수집은 빅데이터(SIEM) 기반과 관제시스템 그리고 외부위협정보를 통해서 수집하는데 그 중 **첫 번째**, 빅데이터 시스템에서 보안장비·서버· 네트워크·AP 등 정보시스템 유형에 따른 다양한 형식의 로그가 발생하므로 장비별로 분류하고 각 장비별 로그 유형으로 선별하여 다양한 수집방법을 통해 생성된 로그의 데이터

를 정제시켜 정형된 로그와 비정형 로그로 분류한다. 그리고 수집된 로그정보를 Json 형태의 Binary 파일로 분산 저장하고 병렬처리가 가능하게 한 후 Lucene 기반 검색엔진으로 빠른 인덱싱과 실시간 처리, 분산· 대용량 저장하여 인공지능 학습에 활용 가능한 데이터로 분류한다. 그리고 분류된 로그는 [그림 2]과 같이 "정보시스템Log"→"중계서버Proxy 또는 수집Agent"→"Collector" 저장 후 Collector에 설정 값을 통해 *Sink를 정해주고 이를 통해 저장된 정형화된 많은 양의 Log 데이터를 효율적으로 수집이 가능하다[2].

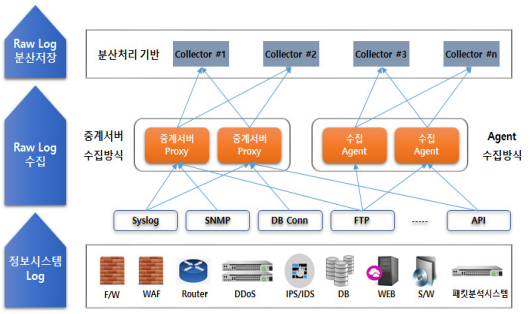

그림 2. 데이터 수집 흐름도

두 번째는 관제시스템을 통한 데이터 수집이다. 빅데이터에서 수집된 로그를 통한 이벤트 로그 및 경보정보를 관제시스템으로 전달되며 보안정책에 의해 Web Hacking과 DDoS, 웜/ 바이러스 등으로 분류된다. 보안관제 전문분석 요원은 출발지/목적지IP, 출발지/목적지Port, 페이로드, 시스템 정보 등의 정보와 Rule & Signature 정책에 의해 공격여부를 판단하고 정탐이면 공격자IP 또는 Signature를 차단한다. 그리고 관제시스템에는 탐지정책과 위협IP, 국가별IP 정보 등의 데이터를 관리하고 있다. 또한 다년간에 운영하면서 발생한 정·오탐 이벤트 정보와 이벤트를 처리하면서 수집 처리된 다양한 정보들에 대한 로그 수집이 가능하다. **세 번째**는 외부 위협정보 수집 시스템을 통한 데이터 수집이다. 외부 위협정보 공유는 각종 사이버 공격에 범국가 차원의 역량을 집결하여 체계적으로 대응하기 위해 관계부처 합동으로 종합대책이 필요하다. 이를 위해 한국인터넷진흥원 공유시스템(C-TAS, Cyber Threat Analysis & Sharing)이 있고 민간업체 중 위협 인텔리전스 서비스인 Threat Inside시스템은 실시간 공격 정보뿐만 아니라 이와 관련된 APT그룹을 추적하고 분석한 위협 인텔리전스 리포트와 분석데이터를 활용하면 네트워크 보안 장비나 SIEM, EDR 등에 최신 위협 feed를 반영하여 탐지력을 강화하거나 보안관제에서 발생하는 위협을 추적하고 분석하는 등 보안 강화를 위해 필요한 시스템 보안과 위협대응, 관리 업무 등을 이용할 수 있다. 그밖에 신규 취약점 정보(CVE, CWE), 해킹사이트(Zone-h 등), 신규 위협정보, 대응규칙 등을 OpenAPI 연계시스템을 구축하여 위협정보를 수집이 가능하다. **네 번째**는 RPA(Robotic Process Automation, 로보틱 프로세스 자동화)를 활용한 데이터 수집이다. RPA는 사람이 PC나 모바일 기기에서 수행하는 정형화되고 반복적인 일을 사람 대신 수행하는 소프트웨어이다. RPA는 반복적인 거래나 업무를 규칙-기반(rule-based)으로 프로그래밍 하여 자동화하는 기초 프로세스 자동화, 축적된 데이터와 머신러닝 기술을 활용하여 RPA 솔루션의 정확도 및 기능향상이 가능한 고급 프로세스 자동화, 빅데이터 분석과 예측 분석(predictive analytics)을 활용하여 복잡한 의사결정을 내릴 수 있는 인지 자동화가 가능하도록 하여야 한다.

2. 데이터 분석

2.1 데이터 전처리와 학습데이터 분석

데이터 전처리는 분석 및 처리에 적합한 형식으로 데이터를 조작하는 것으로 자료의 적합성과 가치에 따라 결과가 다르게 나온다. 전처리 기법에는 데이터 정제, 데이터 통합, 데이터 변환, 데이터 정리가 있으며 원본 로그 필드를 다양한 방법으로 연산하고 변환을 시켜 의미 있는 데이터로 변화하는 프로세스를 갖추어야 한다.

그 요건으로 [그림 3] 첫 번째 데이터 정제는 레코드 집합, table 또는 database에서 손상되거나 부정확한 레코드를 검색 및 수정(또는 제거)하고 데이터를 정제하고 변환 시에는 통일되고 정확한 값의 추출을 위해 필드를 정의하고 중복 필드 제거를 통한 학습 성능을 높여서 데이터 준비 단계에서 필요한 기능에 대해 구현 설계 및 개발과 학습데이터 최적화 준비와 데이터 정제로 노이즈 처리까지 되어야 한다. 두 번째 데이터 통합

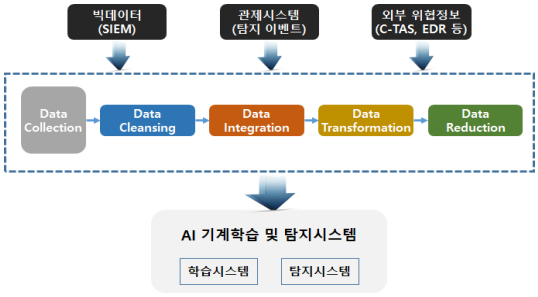

그림 3. 데이터 전처리 구성도

이다. 여러 소스의 데이터베이스나 데이터 파일을 결합하거나 서로 다른 데이터 세트가 호환이 가능하고 객체나 단위 좌표로 데이터를 통합하여 완전 자동화 또는 반자동화 시켜서 다수의 정제된 데이터로 표현되어야 한다. 세 번째 데이터 변환으로 하나의 형식 또는 구조에서 다른 형식이나 구조로 데이터를 변화하는 프로세스로 데이터 마이닝의 효율을 높이기 위한 변환 및 변형 작업이며 데이터에서 노이즈를 제거되고 새로운 속성을 추가되도록 데이터를 정규화(normalization) 또는 집단화(aggregation) 시켜 Z스코어로 바꾸거나 Log를 씌우거나, 평균값을 구해야 한다. 그러기 위해서는 데이터 변환 단계에서 유사필드나 중복필드를 처리해서 최적화된 학습을 제공해서 유사필드는 제거하고 중복필드는 그룹화 또는 종속 시켜서 학습데이터 최적화로 예측에 대한 성능 및 정확도를 향상 시킬 수 있어야한다. 마지막으로 데이터 정리는 일반적으로 데이터는 매우 커서 대용량 데이터에 대한 복잡한 데이터 분석은 실행하기 어렵거나 불가능한 경우가 많다[3]. 데이터 축소는 보통 용량 기준보다 작은 양의 데이터 표현 결과를 얻게 되더라도 원 데이터의 완결성을 유지해야 하며 데이터 분석 시 좀 더 효과적이고 원본 데이터와 거의 동일한 분석 결과를 얻어내어 동일한 분석 결과를 만들어야 한다.

2.2 지도학습 기반 알고리즘

현 사이버위협 방어체계 운영에서 인공지능 기반 보안체계로 진화하기 위해서는 모든 내·외부 보안위협으로부터 100% 안전하고 강력한 보안체계와 빠른 학습, 빠른 응답을 보장하는 초고속 인공지능 플랫폼 구축으로 위협환경에 스스로 적응하는 인공지능 기반 보안체계로 변화가 필요하다. 이미 알려진 보안 위협은 사람의 판단기준을 학습시켜 대응의 속도를 증가시키고 분석·대응 업무처리량을 향상시켜서 보안 효과성과 효율성을 극대화하고 위협이벤트를 자동분석 하게 함으로써 공격 대응률을 증가 시킬 수 있다. 또한 알려지지 않은 보안 위협은 정상상태를 학습시켜 이상상태를 탐지하여 분석·대응 능력을 향상시키고 지능화 공격 대응에 강화함으로써 신·변종 공격대응과 조기경보와 위협예방을 높일 수 있다. 지도학습은 컴퓨터에서 훈련데이터를 미리 준비하고 어떤 입력이 들어오면 올바른 답이 나오도록 컴퓨터를 학습시키는 방법이다. 기존의 침입탐지시스템(IDS)나 침입방지시스템(IPS), 방화벽 등 탐지 및 차단되는 패턴들에 대한 공격유형별 시나리오 기반의 학습데이터와 초동대응·분석 이력을 학습데이터로 생성하여 인공지능 알고리즘을 통해 침해대응 분석가에게 전달되면 새로운 모델을 생성할 수 있으며 이로 인해 사용자 행위 분석 기반의 학습데이터를 생성할 수 있다.

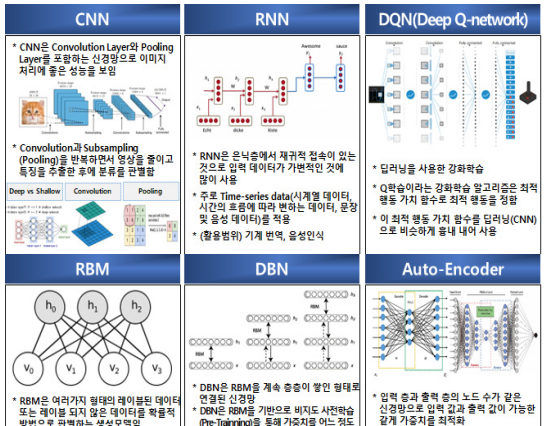

그림 4. 딥러닝에 사용되는 핵심 알고리즘

그리고 정확도를 높이기 위해 심층학습 적용이 필요한데 실 데이터를 Convolution Layer와 Pooling Layer를 포함하는 신경망으로 이미지 처리에 좋은 성능을 보이는 [그림 4] *CNN모델과 은닉층에서 재귀적 접속이 있는 것으로 입력 데이터가 가변적인 것에 많이

사용하는*RNN모델, DQN(Deep Q-Network)모델 등의 2-3개의 최적의 알고리즘 조합하고 가중치에 의한 결과를 병합하면 최적의 결과를 도출할 수 있다[4]. 또한 이런 알고리즘을 통해 비용감소와 기능 효용성을 제공하기 위한 보안기능 가상화 확산, 클라우드 기반의 위협 데이터 분석, 탐지 및 분석 체계를 위한 지속적 접근 노력, 단위 기술 중심의 악성코드 분석·대응을 인공지능 플랫폼 기반 침해사고 예측 및 공격자IP 추적, 악성코드 분석 결과 및 침해사고 연관정보들의 기계학습을 통한 신·변종 악성코드의 신속한 탐지·분류, 악성코드와 연관된 침해사고의 자동분석이 가능하다. 또한 알고리즘을 선정할 때 정교한 알고리즘을 선정하는데 더 많은 시간을 할애해야 한다. 그래야 초급자가 실행하는 데이터를 이해하는데 좋을 것이며 결과도 개선시킬 수 있다. 그리고 최고의 성능을 발휘하기 위해서는 세심한 튜닝과 광범위한 학습을 필요하다. 이에 따라 인공지능 통합관제체계 기반 위협탐지, 예측, 학습기반 신·변종 악성코드 탐지, 분류기술을 활용한 관제 체계 확보와 침해사고에 대한 신속한 판단 및 적극적인 대응을 위해 지능형 사이버공격인지와 추적기술 적용 그리고 관제기술, 관제체계, 대상시스템, 관제 업무범위 변화 등에 대한 전문적인 침해사고 대응인력과 조직 등의 필요 자원 및 운용기술과 정보보호 시스템 등의 구축되어야 한다.

2.3 정·오탐 및 이상행위 대응 서비스 모델 개발

사이버 위협이 날로 지능화됨에 따라 APT와 같이 지속적, 지능화된 공격에 대한 탐지와 예측의 한계로 미탐(False Negative)이 증가되고 있다. 보안관제 Process는 일반적으로 known 사이버 위협 탐지 및 대응에는 효과적이지만 unknown 위협을 탐지하기에는 역부족이다. 더구나 탐지, 대응, 분석, 운영 부분에서 대량으로 발생하는 이벤트를 처리할 보안관제 전문 인력이 부족하여 공격을 판단하고 차단을 수동으로 적용하기까지 효율성이 떨어진다. 이에 따라 SIEM과 관제시스템 의한 경보이벤트와 이벤트 처리내역을 학습하고 인지하여 인공지능 자동식별 탐지 모델에 적용하여 사이버침해 시도에 대한 자동 예측이 가능하도록 정·오탐 처리를 자동화 하는 것이다. 또한 Event에 대한 사고처리 예측, 침해사고 대응결과에 지속적인 학습 강화를 통해 오탐을 최소화 하는 것이다[5].

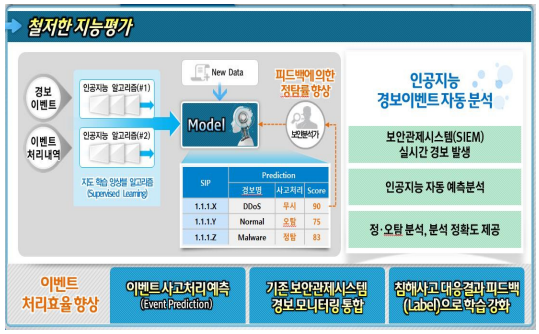

그림 5. 정·오탐 처리 자동화 서비스 모델

이렇게 [그림 5]와 같이 정·오탐 이벤트를 자동으로 선별하는 자동화 서비스 모델의 프로세서는 1) SIEM, 관제시스템 이벤트 추출, 2) 정·오탐 라벨링(식별), 3) 지도학습 알고리즘 적용, 4) 학습 데이터 피드백에 의한 보안관제 전문 인력 검증, 5) 자동화 서비스 모델강화, 6) IP 정보수집 및 유해 IP 식별, 7) 유해 IP검증 후 IP차단, 8) 유해 IP등록 및 결과검증 등에 대한 수행절차가 필요하다. 단, SIEM이나 관제시스템에서 급작스럽게 증가된 데이터에 효율적인 라벨링과 시그니처 분석 수행 작업이 필요하며, 공격 유형별 시그니처 최적화와 탐지 공격 유형 확장 모델을 추가로 개발하여 처리 범위를 확대해야 한다. 또한 IP정보에 대한 사전 정보 수집과 유해 IP에 주기적인 검증 작업이 필요하다.

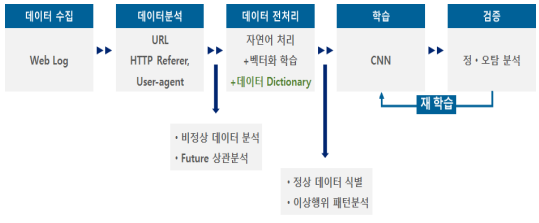

그림 6. 이상행위 처리 자동화 서비스 모델

[그림 6]는 정상 행위 기반 이상행위 대응은 다양한 서비스 도메인의 이상탐지 가능한 모델 생성이 필요하

다. 이상행위 기반 공격은 시그니처 기반의 보안장비에서 탐지하지 못하여 비지도 학습을 통해 지능화된 알고리즘으로 사용자의 변칙 활동 및 이상행위 탐지를 구현해서 비지도 학습 알고리즘을 활용하여 데이터를 수집 및 분류하고 이를 기반으로 정상행위 사용자와 이상행위 사용자를 구분함으로써 이상행위를 도출해낼 수 있다[6]. 이는 인공지능플랫폼의 알고리즘에 의해서 기존의 보안장비에서 탐지하지 못했던 이상행위를 탐지할 수 있어 데이터 분석에 투입되는 시간을 최대한으로 줄일 수 있다.

3. 차세대 보안관제 체계(Adaptive Security Architecture)

3.1 차세대 통합보안관제 운영 방안

인공지능 기반 침해사고 대응체계는 지속적이고 전반적인 모니터링이 수반되어야하며, 침해의 징후를 끊임없이 분석하는 것이 필요하다.

표 1. 보안관제 대응 업무 프로세스

구분	주요 내용
예방	• 서비스/시스템/보안정책 보안 대응 수준 유지 강화 • 신규 위협정보 수집체계 기반의 공격 사전예측 서비스 • 위험평가 분석 서비스 제공
관제	• 보안대응 시스템 보안 수준 강화 • 접근통제 강화를 통한 사고예방 기능 강화 • 신규 보안정책 생성 및 권한 정책 변경사항 반영
대응	• 정상기반 이상행위 탐지와 잠재적 위협 탐지 서비스 • 사이버 위협 우선순위 부여 및 대응 • 노출된 위협요소 격리 및 차단
분석	• 외부 위협 인텔리전스를 활용한 침해 정밀분석 서비스 • 보안 정책 적용 자동화와 긴급 보안 정책 Push 기능 제공

[표 1] 예방·관제·대응·분석 및 분석체계의 유기적 순환구조인 보안체계와 탐지되는 신규위협에 대해 인공지능의 선처리를 통해 처리범위 및 속도향상, 정상기반의 학습모델을 통해 비정상행위 식별로 알려지지 않은 신규위협 대응, 마지막으로 인공지능기술을 활용 분석 능력을 강화하고 최신위협 정보에 대해 수집하여야 한다[7].

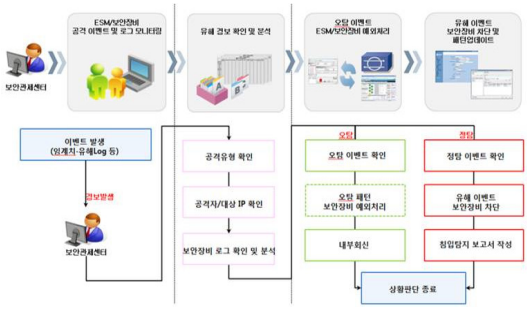

그림 7. 이벤트 대응 프로세스

[그림 7] 이벤트 대응 프로세스는 1) 관제시스템을 통한 실시간 경보 모니터링, 2) 출발지/목적지IP 정보와 공격유형, 탐지규칙 등을 통한 이벤트 상세 분석, 3) 페이로드(Payload)를 통한 정·오탐 분석, 4) 방화벽 또는 네트워크 장비를 통한 유해IP 차단, 5) 침입탐지 보고서 작성 후 사건은 종료된다[8].

3.2 해킹 침해사고 대응 방안

최근에 해커는 오랫동안 장기간에 걸쳐 지능적이고 지속적으로 목표 대상을 공격하는데 이러한 공격 기법을 APT(Advanced Persistent Threat)라고 한다. APT 공격은 침투, 잠입, 공격 프로세스로 진행된다. **1단계** 침투는 해커는 목표물에 연관된 정보를 조사하는데 악성 메일 제작해서 수신자가 메일을 열어볼 수 있도록 하기 위해 주제를 조사하는 것이다. 이를 통해 악성코드를 침투시키는 것이다. **2단계** 잠입은 목표시스템에 접근하는 것으로 목표물에 침투한 뒤 악성코드를 해커의 지시에 따라 추가 감염을 수행하여 새로운 유형의 악성코드를 계속 유입하는 것이다. **3단계** 공격은 해커가 원하는 정보를 탈취하기 위하여 백도어(Back door)를 설치하여 보안 관리자에게 들키지 않고 오랫동안 공격을 수행하는 것이다.

이러한 APT공격에 대응하기 위해 보안 전문가와 인공지능을 결합하여 선순환 구조의 [그림 8] Active Learning 기술로 빅데이터 시스템에서 발생하는 대용량의 보안 이벤트와 로그들 중 라벨링 되어 있지 않은 데이터를 학습에 보다 효율적인 데이터를 골라 보안 담당자에게 요청을 보내고 담당자는 그 요청에 따라 데이터를 라벨링 후 머신러닝에 적용한다면 전문가의 직

관력과 인공지능의 학습을 통해서 APT기법에 의한 해킹 공격에 대응이 가능할 것이다[9].

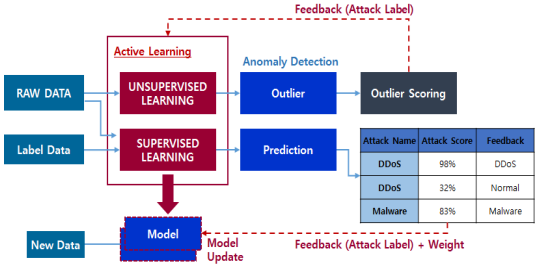

그림 8. Active Learning Architecture

3.3 악성코드 침해사고 대응 방안

악성코드는 제작자가 악의적인 목적으로 사용자에게 피해를 주기 위한 프로그램이다. 기존의 악성코드 차단은 네트워크 실시간 한계와 SSL 암호화 탐지가 불가능, Zero-Day 공격에 취약하고 시그니처, 휴리스틱, 샌드박스 등의 기술은 신종/변종 악성코드를 탐지하지 못했다. 그러나 인공지능 기반 End-Point 보안기술(바이러스→HIPS→Anti-Exploitation→Sandbox→EDR→SIEM)이 진화하면서 악성코드 위협의 수준을 정량화가 가능하였고, Stealth 엔진 기반 보안 기술로 탐지가 가능하였다.

표 2. 악성코드 침해사고 방지 기술

방지기술	설명
프로세스 패턴 탐지	• 라이브러리 로딩 시 파일검사 • 프로세스 모델링, 분류, 회귀
악성행동 분류	• 이상행동 악성여부 검사, 판단 • KNN, SVM, 베이지안 네트워크
익스플로잇 자동차단	• 코드 덮어쓰기, 랜 스크래핑 • 자체 판단기반 차단 수행
코드인젝션 실시간 방지	• 메모리 원격 할당, 매핑 차단 • 실시간 Over Flow 사전차단
Active Script 공격분석	• 악성 Power Shell 스크립트 분석 • 가상 실행 결과 악성여부 도출
VBA 매크로 공격 탐지	• File-Less기반 공격탐지/차단 • Office 문서 내 스크립트 분석
지능형 앱 리스크 관리	• 실행 가능한 APP리스트 관리 • APP 행위 시계열 분석
저장장치 자동 통제	• Driver 수준 DMA데이터 추적 • Cycle Stealing Word 단위 분석
신종 악성코드 탐지	• 행위기반 모델링/패턴화 수행 • 정상/악성행위 벡터 거리 측정
변종 악성코드 탐지	• 기존 시그니처 분석, 전이 학습 • Fine Tuning 기반 유사 코드 차단

악성행위를 탐지하기 위해서는 [표 2] *Precision, **Recall 기반의 분석기술이 필요하며, 악성코드 속성, 프로세스 행동 분석, IP주소 등 다양한 연관분석 정보를 바탕으로 학습을 수행하는 다차원 인공지능 기술을 사용해야 한다[10]. 이를 통해 수집된 데이터에 대한 분류 모델을 적용하고 위험도에 따른 확률적 예측이 가능한 알고리즘을 적용하여 판단-예측을 분리해서 프레임워크 구성 예측 모델을 이용한다면 침해 사고 예측과 위험도 분석 및 대응이 가능하다.

3.4 서비스거부 침해사고 대응 방안

DDoS 공격은 네트워크 또는 서버에 대량의 트래픽을 전송하여 운영 능력을 붕괴시키기 위한 것으로 이때 수백, 수천 또는 수백만의 좀비PC를 이용해서 공격한다. [그림 9]은 DDoS 공격 대응 절차는 **1단계)** 공격인지를 위한 체크포인트로 사건 발생 당시 공격인지 아닌지 명확한 판단이다. **2단계)** 공격유형 파악이다. 유입되는 트래픽(Incoming Traffic)에 대한 패킷을 수집하여 확보된 트래픽에 대해 분석하거나 시나리오 기반(Scenario Drawn)으로 DDoS 유형을 파악한다. **3단계)** 차단정책 적용에 의한 대응이다. 공격유형을 명확히 판단하여 DDoS 대응장비나 기타 보안장비에 차단정책을 설정하여 웹서비스의 가용성을 확보한다. **4단계)** 공격시점이 BPS, PPS, CPS 등의 양과 지속시간 등의 내용을 정확히 규명함으로써 추가 발생할 수 있는 공격에 대비하여 추가 정책을 세우고 공격에 활용되었던 좀비IP를 확보한다. 이렇게 단계별 DDoS 대응을 침해대응이 가능한 전문 인력이 실시간으로 패킷수집과 분석, 대응 그리고 사후처리 까지 모두 수행해왔다. 이러한 대응 절차와 유형별 공격 특징 및 정보 등을 인공지능 알고리즘에 학습시켜 시스템이 자동으로 대응을 한다면 보다 신속하고 정확한 대응으로 서버에 자원을 확보할 수 있다.

* Precision(정밀도) : 모델이 True라고 분류한 것 중에서 실제 True인 것의 비율, Precision = TP / TP + FP
** Recall(재현율) : 실제 True인 것 중에서 모델이 True라고 예측한 것의 비율, Recall = TP / TP + FN

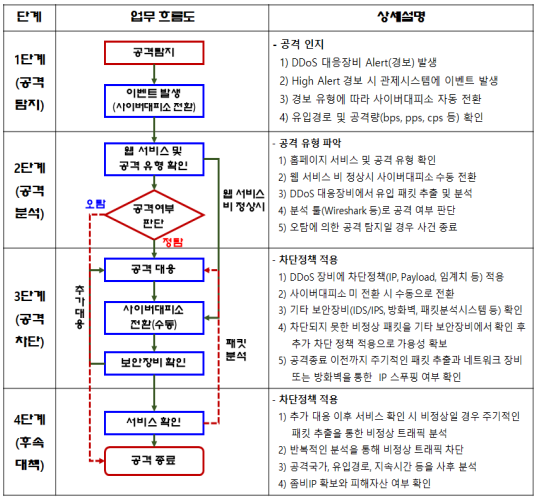

그림 9. DDoS 대응 절차

4. 보안관제 체계 관리 방안

4.1 보안위협 대응 체계 관리

인공지능 서비스 모델 고도화와 신규 보안 기술 대응 모델 연구를 통해 인공지능 적용 범위 확대와 정확도 향상과 지도, 비지도, 강화학습 및 탐지 알고리즘 모델과 보안기술 서비스 모델 관리해야한다. 또한 알려진 공격의 서비스모델에 대해 학습 탐지 성능 향상과 공격 유형 대응 범위를 넓히고 이상행위 대응 서비스모델은 비정상행위 식별모델을 확대하고 탐지모델을 개선해서 인공지능 플랫폼에 주기적으로 업데이트가 돼야 한다. 그리고 신규 보안기술에 대한 대응 모델은 공격 동향 수집과 분석, 데이터 생성 기법 고도화 데이터 처리 속도 향상, 모델 분석 자동화를 통해 지속적인 관리를 수행해야 한다.

4.2 유해 IP 관리

해커들이 유해IP를 재사용한 사례가 있다. 2011년 3월에 발생한 3.4 DDoS 공격 IP와 2009년 7월에 발생한 7.7 DDoS 공격에 사용되었던 IP가 같은 주소를 사용됐었다고 분석결과 보고된 바 있다. 그리고 악성코드 제작기법과 취약점 코드는 지속적으로 새로운 기법이 나오고 있지만 악성코드 공격에 사용되었던 명령 제어 서버(C&C)는 재사용된 것으로 나온다[11]. 이를 위해 유해IP 관리는 국내외 해외IP의 저장기간을 별도로 관리하지 않고 최소 1년을 보관 및 관리가 필요하며 기관에 특성에 따라 저장기관을 정해야 한다. 그리고 [그림 10] 유해IP를 찾는 방법에는 방화벽 로그를 분석하여 비정상IP 식별, 예를 들어 비정상 아웃바운드 통신, 5분간 대량 접속 유해IP, 일일 신규 접속 유해IP 등으로 찾을 수 있다.

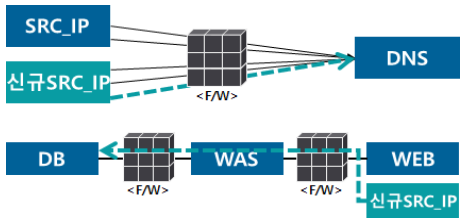

그림 10. DNS 접속 및 서버 간 통신 식별

4.3 보안이벤트 탐지정책 관리

지능화되는 사이버 보안 위협에 대응하기 위해서는 보안장비 벤더에서 제공하는 탐지패턴 뿐만 아니라 기업이나 기과의 특성을 고려하여 자체 생성하는 사용자 정의 패턴이 개발과 관리가 필요하다. 수많은 사이버 공격에 대응하기 위해서는 기존의 탐지규칙에 대한 개선을 통해서 오탐율 또는 미탐율을 줄여야 하며, 신규 취약점이나, Zero-day Attack이 발표될 경우 즉각적인 대응을 위해 여러 가지 공격기법 탐지를 위해 자체적으로 패턴을 생성하고 테스트 및 적용하여 운영해야 한다.

4.4 보안업무 법제도 관리

마지막으로 보안업무 법제도 관리는 2020년 데이터 3법(「개인정보보호법」,정보통신망법」,「신용정보법」)이 통과되었다. 4차 산업혁명 시대를 맞아 신산업 육성을 위해서는 데이터 이용을 활성화하여 인공지능(AI), Cloud, 사물인터넷(IoT)등 신기술을 활용한 데이터 이용이 필요하다. 이에 안전한 데이터 사용을 위한 사회적 규범 정립으로 데이터 이용에 관한 규제 혁신, 개인정보보호 협치(거버넌스) 체계의 2가지 문제를 해결해야 한다. 정보보호 분야는 공공분야 또는 민간분야에 인공지능 ALC 클라우드 기술의 서비스가 확대대고 있고 많은 양의 데이터를 수집, 보관, 분석 등으로 데이터

를 다루는 업무를 수행하고 있기 때문에 더욱더 사전에 규범 정립이 필요하다. 이를 위해 인공지능기반의 통합보안관제 업무에 대한 범제도와 관리자를 통한 연 1회 이상의 꾸준한 기준 및 절차에 대한 업데이트를 수행해야 한다.

Ⅲ. 기대효과

사이버보안 분야에 인공지능 기술을 적용하면 기존에 방어기술이 탐지하지 못하던 새로운 악성코드, Intelligent 위협이나 이상행위를 탐지해낼 수 있으며, 많은 양의 위협정보 속에서 정탐인 것을 걸러내고 Intelligence를 확보해 빠르게 대응이 가능하도록 지원해줄 수 있다. 반복되는 단순 업무, 수작업으로 처리하고 있는 일들을 인공지능 플랫폼이 대체한다면 업무효율성을 높을 수 있으며, 짧은 시간에 탐지, 분석, 대응, 상황전파까지 신속하게 업무를 함으로써 효과적인 대응이 될 수 있다고 생각한다. 보안전문 업체의 가장 중요한 과제는 사고 대응과 해결시간 단축, 경보의 정확성 최적화, 새로운 위협과 취약점 파악이다.

이중에서 **첫 번째** 보안관제 전문 인력은 사고 대응과 해결시간 단축이 가장 우선시 된다. 수많은 이벤트 중 중요한 이벤트를 찾아내고 초동 분석을 통해 피해 시스템에 취약점 발견과 피해 여부를 파악하여 신속한 초동대응하고 침해사고 대응팀에 전파를 통해 보호 자산에 피해가 확산되지 않도록 하기 위해서는 많은 어려움이 발생하기 때문이다. **둘째** 경보의 정확성과 최적화이다. 오탐(False positive), 미탐(False Negative) 등 정확성 있는 탐지규칙을 확보하지 못하고 있는데다 자원 부족으로 위협을 인지하고 평가하는데 많은 어려움이 있어서 해결해야 할 중요 과제이다. **세 번째** 새로운 위협과 취약점 파악이다. 미래는 5G와 IoT 등 다양한 정보기기들의 사용으로 인해 수많은 사이버위협과 취약점이 나타날 것이다. 이러한 사이버 공격에 알아가고 대응하기 위해서는 많은 시간과 노력이 필요하기 때문이다. 이렇게 사이버보안 분야에 인공지능 기술을 적용한다면 보안전문 인력들이 중점적으로 인식하고 있는 문제점들을 해결할 수 있을 거라 생각한다.

Ⅳ. 결론

다양한 딥러닝 알고리즘의 최적화 조합과 머신러닝에 대한 기대에도 불구하고 다양한 방법과 아이디어가 제공되고 있지만 아직까지 통합보안 관제분야에 인공지능기반의 플랫폼 개발의 결과물이 나오질 않고 있으며 이렇다할만한 투자와 개발이 이뤄지지 않고 있다. 앞으로의 사이버침해는 고도화 되고 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 증가될 것으로 예상되며 이에 따라 기술에 발전의 속도만큼 사이버상의 보안 위협은 종료와 공격 방식이 빠르게 진화하고 있기 때문에 방대한 데이터를 통합적으로 분석하고 빠른 시간에 선제적으로 대처할 수 있는 인공지능기반의 통합관제 체계를 빠른 시일 내에 구축하고 운영돼야 한다.

본 논문을 연구하면서 국내에는 아직까지 보안 분야에 인공지능기반의 플랫폼을 적용한 사례나 시스템이 존재하지 않아 어떻게 운영되고 있는지? 과연 효과성과 효율성이 얼마나 높은지 정확한 데이터가 존재하지 않아 저 자신도 플랫폼 개발 방안 또는 서비스 모델을 만드는데 이론적인 지식을 통해 연구하고 개발 방안을 제시할 수밖에 없는 아쉬움이 남는다. 보안 분야에 인공지능을 접목시켰을 때 인공지능에 대한 부작용도 고려돼야 하고 보안 위협이 지능화되고 또 방대하게 늘어나는 만큼 기존 보안관제 운영 방식인 사람이 직접 보안위협 정보를 찾아내고 분석 또는 대응하는 수동적인 이벤트 처리 방식의 한계를 보완해서 인공지능을 활용하여 스스로 학습하고 처리 대응하는 심도 깊은 인공지능 플랫폼 활용 방안을 꾸준히 모색해야 한다고 생각한다.

참 고 문 헌

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

[2] 손기준, 조인호, 김찬우, 전채남, “Design and

Implementation of Hadoop-based Platform "Textom" for Processing Big-data," 한국콘텐츠학회 종합학술대회 논문집, pp.297-298, 2015.
[3] 이주열, *AI와 최신 딥러닝 기술 동향*, LG CNS AI빅데이터연구소, 2019.
[4] 오영택, "인공지능 기술기반의 통합보안관제 서비스모델 개발방안," 한국콘텐츠학회논문지, Vol.19, No.1, pp.113-114, 2019.
[5] http://www.igloosec.co.kr/BLOG_다가오는 인공지능 기반의 보안관제, 그 전에 준비해야 할 것은 [qs]?searchItem=&searchWord=&bbsCateId=17&gotoPage=2
[6] https://blog.lgcns.com/1221
[7] 정기문, 박학수, "침해위협 상관분석 기반의 보안관제 시스템 설계," 한국컴퓨터정보학회, 제19권, 제2호, pp.335-337, 2011
[8] http://www.igloosec.co.kr/BLOG_SIEM을 통한 경보 설정과 이벤트 대응
[9] 김규일, *보안관제 효율성 제고를 위한 실증적 분석 기반 보안이벤트 자동검증 방법*, 한국과학기술정보연구원, 2014.
[10] http://blog.skby.net/인공지능-기반-침해사고-공격-분석-방안/
[11] 이후기, 성종혁, 백동훈, 김종배, 김관용, "A Study on Estimation of Malicious IP Storage Cycle in Security Monitoring Base," Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, Vol.7, No.7, July 2017.

저 자 소 개

홍 준 혁(Jun-Hyeok Hong) 준회원

- 2010년 2월 : 한밭대학교 전자공학과 학사
- 2019년 3월 ~ 현재 : 배재대학교 사이버보안학과 석사과정
- 2012년 10월 ~ 현재 : 이글루시큐리티 대전관제팀 팀장

〈관심분야〉 : 정보보호, 인공지능, 정보보안 감사

이 병 엽(Byoung-Yup Lee) 종신회원

- 1991년 2월 : 한국과학기술원 전산학과(공학사)
- 1993년 2월 : 한국과학기술원 전산학과(공학석사)
- 1997년 2월 : 한국과학기술원 경영정보공학(공학박사)
- 1993년 1월 ~ 2003년 2월 : 대우정보시스템 차장
- 2003년 3월 ~ 2016년 2월 : 배재대학교 전자상거래학과 교수
- 2016년 3월 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 지능정보시스템, 데이터베이스, 정보보안