정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

사이버 보안관제 체계 문제점과 머신러닝 적용 기술 현황

정 일 옥*, 조 창 섭**, 지 재 원***

요 약

IT 기술이 발전함에 따라 사이버 공격은 더욱더 지능화 대량화 되고 있다. 이로 인해 기존의 전통적인 보안 접근만으로는 모든 위협을 탐지하고 분석, 대응하기에는 한계에 이르렀다. 이를 해결하고자 사이버 보안관제에 머신러닝 기술을 적용하고자 하는 연구 및 사례가 증가하고 있다. 이에 본 논문에서는 기존 보안관제 체계 및 문제점에 대해서 알아보고, 이를 해결하고자 적용된 머신러닝 기술 현황에 대해 조사하였다. 그리고 해당 기술이 보안관제에 성공적으로 적용되기 위해 고려해야 할 관리적 측면과 기술적 측면을 제안한다.

Ⅰ. 서 론

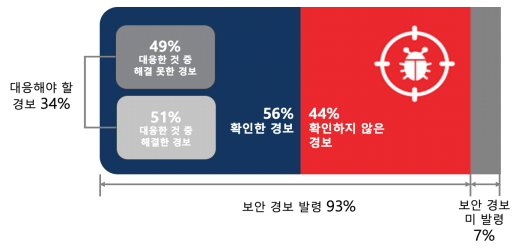
새로운 ICT 환경에서 사이버위협은 복합적인 공격기술을 사용한 신·변종 위협의 증가와 함께 고도화되고 있으며, 국내외에서 다양한 위협사례를 발생시키고 있다[1]. 국내의 경우 지형적인 요인으로 북한 해커에 의한 정보탈취 공격과 암호화폐 채굴을 위한 정보탈취 공격, 평창올림픽 해킹사고[2] 등 사이버위협이 지속적으로 발생하고 있으며, 해외에서도 제조, 의료, 교통 등 다양한 분야에서 ICT 기술과 융합발전하면서 사이버 공격의 사례가 전 분야에서 발생하고 있다. 특히, 최근에는 공급망 공격(Supply-Chain Attacks)으로 분류되는 솔라윈즈(SolarWinds) 해킹 사건[3]과 5일간 송유관 가동 중단을 일으킨 해커그룹에 의한 랜섬웨어(ransomware) 공격[4]은 사이버 위협이 점점 심각해지고 있음을 말하고 있다.

이러한 사이버보안 위협이 증가함에 따라 보안관제 분야에서도 보안역량의 한계에 직면하고 있다. 전 세계적으로 사이버보안 인력 부족[6] 등으로 인해 기관과 기업들은 점점 증가하는 사이버위협에 효율적으로 대처하는데 어려움을 겪고 있으며, 이러한 상황에서 머신러닝, 딥러닝 등의 발전에 따른 인공지능을 이용하여 이러한 부분을 해결할 것으로 기대하고 있다[7].

국내 또한, 주요 부처에서 운영하고 있는 전산장비 수가 매년 증가하고 있으나, 운영인력과 투자는 이러한 속도를 못 따라가고 있다. 주요 부처들이 사이버안전센터 통합보안관제시스템에 빅데이터를 구축 완료하여 대량의 로그가 수집되고, 전체 사이버 위협 탐지가 증가하고 있으나 관제 직원의 대응 처리에 한계를 느끼고 있다.

[그림 1]에서 보는 바와 같이 시스코(2019)[9]에 따르면 사이버보안 침입 경보의 44%는 조사되지 않고, 조사된 56% 알람 중 대응조치가 필요한 것은 34%로 파악되나, 이 중 조치되는 비율을 51%이고, 나머지 49%는 미해결 상태로 남겨져 있다고 한다.

컨설팅전문기업인 캡제미니(2019)[7] 보고서에 따르면 다양한 분야에서 기업들이 사이버보안의 효율성을 개선하기 위해 인공지능 기술을 채택하고 있으며, 사이버 위협의 탐지, 예측, 대응 등 다양한 보안 영역에 광범위하게 예산과 시간을 투자하고 있다고 한다. 특히,



〔그림 1〕 CISCO(2019) 위협경보처리 현황

* 고려대학교 정보보호대학원 (박사과정, okkida@korea.ac.kr)
** 숭실대학교 IT정책경영학과 (박사, aisoc@naver.com)
*** 한남대학교 컴퓨터공학과 (석사, iversace@naver.com)

탐지 영역에서 인공지능 활용도가 51%로 다른 예측(34%)이나 복구(18%)보다 높게 나타남을 알 수 있으며, 예측이나 복구 분야도 점진적으로 증가할 것을 예상하고 있다. 특히, 그 외에도 사이버 보안 분야에서의 인공지능 적용은 보안업무 종사자의 일상적 반복적 과업을 줄이고 좀 더 고도화되고 전문적인 업무에 집중할 수 있도록 할 것이라 기대한다[8], 즉 24시간 365일 보안관제 업무 방식으로 발생하는 담당자의 피로도와 관제요원 역량에 따른 정·오탐 식별 및 위협분석 대한 편차 문제를 머신러닝 도입으로 일관성 있게 개선할 수 있을 거라 기대한다.

Ⅱ. 관련 연구

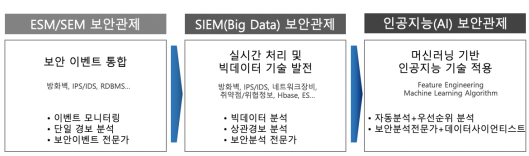
2.1. 기존 보안관제 현황 및 문제점

2.1.1. 보안관제 현황

보안관제센터란 사이버공격과 내부정보 유출을 체계적으로 대응하기 위해 구성된 인력과 프로세스, 기술의 집합이며(Alissa Torres, 2015)[10], 조직은 공격으로부터 생존하기 위해 잠재적인 위협을 인식하고 사고를 일찍 감지하며 신속하게 대응하기 위해 기술을 이용하여 조직의 정보 도메인을 모니터링하여 공격을 예방, 탐지 및 대응하는 보안 전문가가 운영하는 사이버 정보 센터로 정의하고 있다(Teresa Meek, 2017)[11].

보안관제센터를 구성하는 요소는 보안관제센터 내부에서 보안관제 및 관련 업무를 수행하는 전문조직(people), 보안관제센터에서의 업무의 흐름을 결정하는 프로세스(process), 보안관제를 위해 필요한 시스템으로 구성된 기술(technology)로 나뉘어 있다(Alissa Torres, 2015).

보안관제 기술은 [그림 2]에서 보는 바와 같이 초기 단위 보안 장비별 이벤트를 모니터링하며, 단일 경보분석, 보안이벤트에 대한 통합을닝목적으로 하는 ESM/SEM 보안관제를 수행하였다. 인터넷의 확장으로 단순 보안이벤트가 아닌 로그와 이벤트에 대해 빅데이터 분석과 상관경보 분석을 수행하는 보안분석 전문가가 필요하였으며, 실시간 처리 및 빅데이터 분석을 목적으로 하는 빅데이터 기반의 SIEM 보안관제를 수행하였다. 그 후 다양한 위협 정보와 자동분석과 우선순위 분석을 수행하는 보안 분석가와 데이터사이언티스트가 필요한 머신러닝 기술 적용을 목적으로 하는 인공지능 보안관제 수행으로 발전하고 있다.



〔그림 2〕 보안관제 기술의 변화

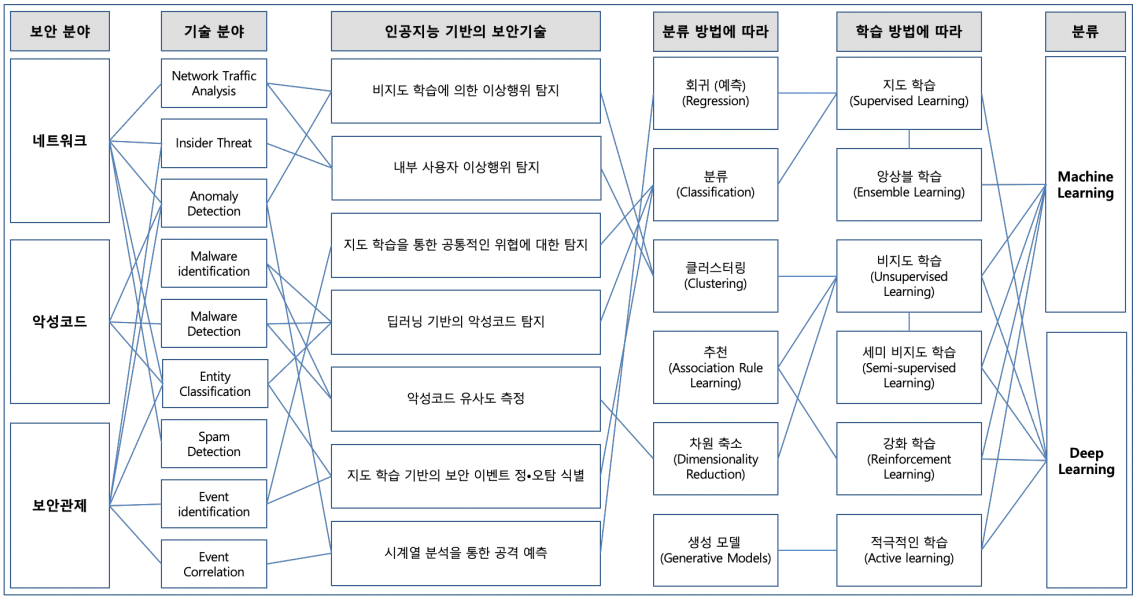
2.1.2. 보안관제 문제점

지금까지 보안관제는 IT 기술의 발전과 발맞춰 끊임없이 발전하는 모습을 보여 왔다. 그러나 도약을 거듭해온 보안관제시스템과 보안관제 시장에는 여전히 풀어야 할 과제가 있다.

가. 과·오탐 및 미탐

기존의 보안관제시스템은 침입탐지시스템, 웹 어플리케이션 방화벽 등 시그니쳐 기반의 탐지이벤트를 받아 상관분석이라는 절차를 통해 탐지 이벤트를 줄이고 있으나, 과탐과 오탐은 여전히 높은 것이 현실이다. 앞에서 언급한 것과 같이 CISCO의 통계 자료에 따르면 전체 경보이벤트 중 36%가 오탐(False Positive, False Alarm)이며, 44%가 조사되지 못하는 이벤트이다. 이는 탐지된 이벤트의 수가 너무 많아 모두 분석하지 못하는 부분으로 과탐(Over Alarm)이라고 한다. 이러한 오탐과 과탐은 빅데이터 기반의 보안관제에서도 마찬가지이며, 오탐과 과탐에는 중복된 경보를 포함한다. 중복된 경보는 지금 처리된 것과 이전에 처리된 것이 똑같은 것을 의미하는데, 통계조사 기관 Security Magazine(2016.12)[12]에서 발표한 자료에 따르면 보안 분석가가 분석할 내용의 30%는 중복된 경보라고 하였다. 이러한 중복 경보는 보안관제센터에 범람하고 있고 관제요원의 업무 수행을 방해하는 백 로그를 생성하는 주요 요인 중 하나일 가능성이 높다(Garry Fatakhov and Yair Stern, 2016)[12].

일명 쓰레기 데이터(garbage data)에 의한 정·오탐 판별 건수가 늘면서 경보를 처리할 관제인력의 부족과 함께 과·오탐 문제는 보안관제의 효율성을 감소시키는 요소로 자리 잡게 되었다.



〔그림 3〕 보안 분야별 인공지능 적용기술 분류

나. 전문인력 확보의 어려움

현재의 탐지 체계는 사람에 의존하고 있기 때문에 과·오탐을 해결하기 위한 방법 중 인력을 확충하여 해결할 수 있으나 현실적으로 예산문제, 인력 확보 문제로 쉽지 않은 실정이다.

인력 부족 현상은 단순히 숫자적인 문제가 아니라 사회적으로 풀어야 할 이슈이기도 하다. 복잡해진 보안 위협에 대응하기 위해 24시간 365일 보안 인력을 운영한다는 것은 보안관제의 필요성을 나타내기도 하지만 사회적으로 워라벨(Work and Life Balance) 이슈와 함께 부담이 되는 것 또한 사실이다. 게다가 지속적으로 변화하는 IT 환경이나 이를 이용한 위협의 형태는 관련 지식에 대한 꾸준한 습득 없이 대응하기 어렵다.

2.2. 보안 분야별 인공지능 적용기술 분류

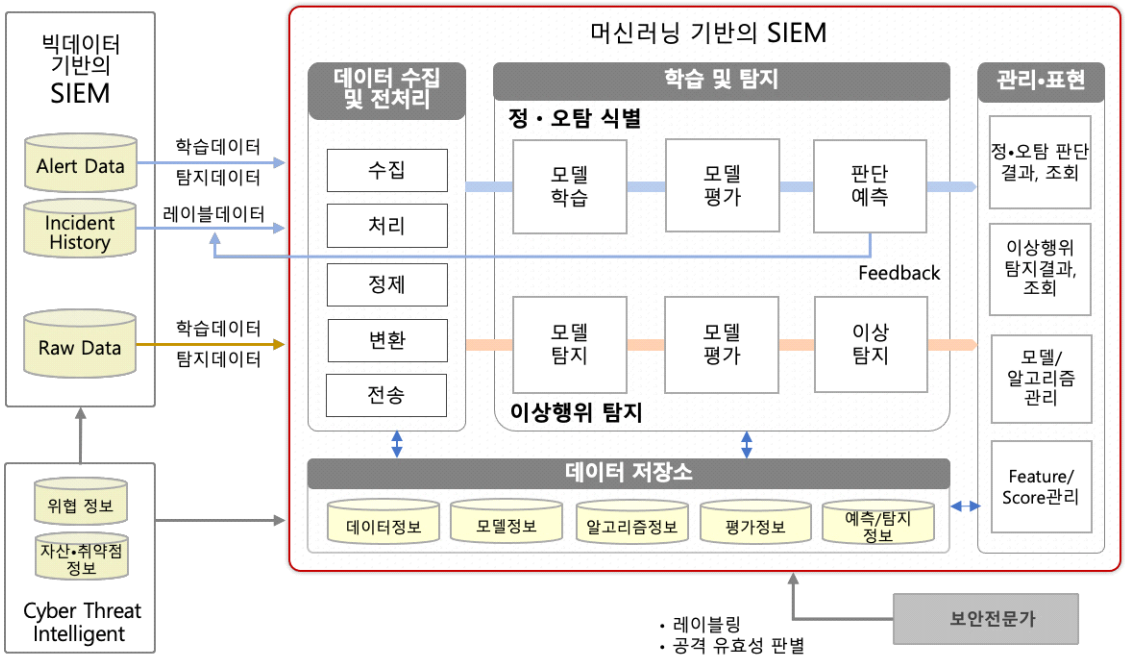
사이버 보안에서 인공지능 기술을 적용하는 분야는 관점에 따라 여러 가지로 구분할 수 있다. 첫 번째는 사이버 보안의 단계별 프로세스에 의해 구분할 수 있으며, 이는 보통 Gartenr의 PPDR 모델[13]에 따른 다섯 가지 범주(Prediction, Prevention, Detection, Response, Monitoring)로 나눌 수 있다. 두 번째는 기술 계층에 따라 분석하거나 모니터링 하는 계층으로 구분하는 것이다. 이는 Network, End-Point, Application, 사용자, 프로세스 등으로 나눌 수 있다. 세 번째는 마켓 상황에 따라 Anti Fraud & identity Management, Mobile Security, Predictive intelligence, Behavioral Analytics/Anomaly Detection, APP Security 등으로 나눌 수 있다. 지금까지 다양한 관점의 분류에 대해서 본 논문에서는 다음과 같이 적용 분야, 기술 분야, 분류 방법, 학습 방법에 따라 인공지능 기반의 보안기술을 [그림 3]과 같이 분류해 보았다.

Ⅲ. 머신러닝 기반의 보안관제 적용기술

이번에는 일반적인 머신러닝 기반의 보안관제 플랫폼 아키텍처에 대해 알아보고 보안관제에 적용된 머신러닝 기술 중 지도학습에 의한 정·오탐 식별, 비지도 학습에 의한 이상행위 탐지에 대해 알아보도록 한다.

3.1. 머신러닝 기반의 보안관제 플랫폼

머신러닝 기반의 보안관제 플랫폼은 데이터 수집, 데이터 전처리, 학습 및 탐지, 관리 및 표현, 데이터 저장 부분으로 구성될 수 있다.



〔그림 4〕 머신러닝 기반의 보안관제 플랫폼

3.1.1. 데이터 수집

보안관제 분야에서의 수집대상은 환경에 따라 다르지만, 보통 정·오탐 식별의 경우 IPS, WAF, SIEM 경보 등 보안관제 요원이 직접 보고 판단할 수 있는 보안이벤트로 구성되며, 이상행위와 같은 비지도 학습은 FW, WEB log, Netflow, 시스템 로그 등으로 관제요원이 그동안 침해사고 분석 등으로 사용된 데이터를 사용한다. 특히, 보안관제에서의 수집시스템은 빅데이터 기반의 보안관제시스템을 수집 연계대상의 기본으로 선택되는 경우가 많지만, 필수적인 것은 아니다.

3.1.2. 데이터 전처리

데이터 전처리는 학습에 대한 품질 및 성능을 향상시키기 위해 수집된 데이터를 샘플링, 변환, 정제를 위해 유형을 정의하고 유사도 분석 등 다양한 단계를 적용한다. 이때, 수집된 데이터에서 결과를 예측할 수 있는 특징을 추출하는데 이때의 특징을 피처라고 하며, 이 과정을 피처 추출, 피처 선택 등이라 부른다. 이때 머신러닝을 통해 탐지하고 하는 결과를 명확히 하고, 보안전문가 또는 데이터사이언티스트를 통해 관련 피처를 추출하게 된다.

3.1.3. 학습 및 탐지

학습 및 탐지에서는 정·오탐 식별과 이상행위 탐지 등 목표로 하는 모델을 생성하는 단계이다. 이을 위해 전처리된 학습 데이터를 입력받아 학습 모듈과 탐지 모듈을 이용하여 선택된 머신러닝 및 딥러닝 등의 알고리즘을 적용하여 모델을 생성한다. 이때 만들어지는 모델은 머신러닝의 전형적인 평가지표 혼돈 행렬(Confusion Matrix) 을 이용하여 평가하거나, 보안전문가에 의해 보안관제센터에서 실증을 한다.

3.1.4. 관리 및 표현

머신러닝 탐지 결과를 도식화하여 보여주는 곳으로 머신러닝 탐지/예측결과, 보안위협의 통계용 정보로 표현하는 대시보드 기능과 각 탐지모델에서 나타난 결과와 분석정보를 표현하는 기능으로 구성된다.

3.1.5. 데이터 저장

데이터저장은 분산저장 파일시스템 저장소 형태와 RDBMS 형태 등 목적에 따라 구성할 수 있으며, 수집된 데이터, 전처리된 데이터, 학습 및 예측된 데이터 등 관련 머신러닝 기반의 시스템이 운영되면서 생성된 모든 데이터를 저장하는 시스템이다.

3.2. 지도학습에 의한 정·오탐 식별

지도 학습에 의한 정·오탐 식별에서 가장 중요한 것은 학습 데이터이며, 관제요원의 노하우를 동반한 다량의 정확한 학습데이터가 필요하다. 정·오탐 식별의 수집대상은 SIEM의 경보이벤트, 침입탐지/방지시스템(IDS/IPS), 웹방화벽(WAF)의 침입탐지 이벤트이다. 사용되는 알고리즘으로는 결정트리의 계열의 알고리즘(Random Forest 등), Boosting 관련 알고리즘, 신경망 알고리즘을 사용한다. 또한, 앙상블, 스태킹 등을 이용하여 다양한 알고리즘 중에서 최적의 스코어를 선택하는 기법을 포함하기도 한다.

3.3. 비지도 학습에 의한 이상행위 탐지

다음은 비지도 학습에 의한 이상행위 탐지이다. 이상행위 탐지에는 레이블 된 학습 데이터가 필요하지는 않지만, 시간 기반의 사용자에 의한 학습데이터 또는 악의적 사용자에 의한 학습데이터 등에 대한 정의는 필요하다. 이상행위 탐지의 수집대상은 FW 등의 보안로그, 웹로그 등 어플리케이션 로그와 네트워크 Netflow 등이 될 수 있다. 알고리즘으로는 클러스터링 계열의 알고리즘이나 이상탐지 관련 알고리즘으로 AutoEncoder, CNN, RNN, Isolation Forest, Outlier Detection 등을 사용한다. 또한, 지도학습과 같이 앙상블, 스태킹 등을 이용하여 다양한 알고리즘 가운데 최적의 스코어를 선택하는 기법을 포함한다.

또한, 최근에는 이상행위 탐지에서 비지도 학습뿐만 아니라 지도 학습과 병행하여 사용하는 사례도 제안되고 있어 머신러닝의 학습 방법으로 어떤 모델을 제한하거나 할 필요는 없다.

Ⅳ. 기술 도입 시 고려사항 및 발전 기술

최근 보안관제 분야에 머신러닝 기반의 보안기술이 적용되는 사례가 증가하고 있으나, 아직은 초기 단계라 몇 가지 부분에서는 만족할 만한 성과를 거두기도 하지만, 전체적으로 개선해야 할 여지가 많다. 이에 몇 가지 고려사항과 향후 적용되어야 할 기술에 대해 관리적 측면과 기술적 측면으로 나누어 알아보도록 한다.

4.1. 관리적 측면

4.1.1. 연계 표준화

머신러닝 기반의 기술은 기존의 SIEM 등과 같은 빅데이터 기반의 시스템이나 보안관제 프로세스와 연계되어 운영됨에 따라 기존 정보보호시스템과의 연계가 중요하다. 때문에 보안관제 분야에서 머신러닝 기술을 적용할 때 기존의 보안관제 관련 시스템에 기능이 추가되거나 별도의 시스템으로 구축 연계되어 구현이 된다. 이에 따라 기존 보안시스템 및 보안정보를 포함한 여타 시스템과 원활하게 연계될 수 있도록 데이터 표현 규격을 표준화 할 필요가 있다. 미국의 경우 국토안보부에서 발표한 사이버위협 표현 규격(STIX/TAXII)를 통해 사이버위협에 일관된 분석 및 연계를 가능하도록 제도화 하고 있다.

이에 다양한 기업에서 머신러닝을 포함한 통합솔루션 체계를 구현할 때 SIEM, AI, CTI 등이 연계된 경우가 많다. 이를 통해 SIEM 등 빅데이터 기반의 보안시스템에서 수집, 분석된 경보 이벤트에 머신러닝을 통해 예측된 위협 이벤트와 위협 인텔리전스를 통해 분석된 위협정보를 연계하여 정확성을 향상시킨다.

4.1.2. 양질의 학습 데이터(Training Dataset) 수집 및 관리

머신러닝 기반의 시스템에서에서는 그 무엇보다 양질의 데이터 확보가 필수적이다. 기존의 보안장비에서 수집되는 보안, 침해사고, 악성코드 데이터를 수집하고 이를 머신러닝 기반으로 사용할 수 있는 데이터로 가공한다. 또한, 해당 데이터에는 목적에 따른 레이블이 필수적이다. 기존 빅데이터 기반의 SIEM 을 통해 수집된 데이터에 대해 침입여부에 대한 이력을 선제적으로 수집하고 관리될 필요가 있다. 특히, 비용부담 및

전문성 부족 등으로 데이터 수집이 어려움을 겪을 수 있기 때문에 데이터에 대한 가공 및 성능에 대한 꾸준한 관리체계가 필요하다.

4.1.3. 머신러닝 기반의 보안전문가 육성

머신러닝을 이용한 효율적인 보안적용을 위해서는 보안지식과 머신러닝 기술 지식을 함께 갖춘 인재가 필요하다. 현재, 보안 분야의 머신러닝 적용이 초기 단계인 만큼, 보안 분야 머신러닝 적용에 대한 학습데이터 생성 및 예측된 결과에 대한 해석에 필요한 전문가 집단이 매우 부족한 상태이다. 보안관제, 침해사고 분석, 악성코드 분석 등 분야별 머신러닝 적용에 대한 이해와 지식이 필요하며, 기존 보안전문가의 머신러닝 보안전문가로서의 역량 전환 및 신규 머신러닝 보안인력 육성을 위한 투자가 필요하다.

4.2. 기술적 측면

머신러닝 기반의 보안관제 기술이 보안관제 현장에서 잘 활용되기 위해서는 아직은 많은 연구가 필요하지만, 머신러닝에 대한 위협 대응과 설명 가능한 인공지능 기술이 추가 되어야 한다.

4.2.1. 적대적 머신러닝(Adversarial ML)에 대한 대응

머신러닝 기술이 발달하면서 기술의 활용범위가 지속적으로 확대되고 있으나, 이로 인해 발생할 수 있는 머신러닝에 대한 위협 또한 우려되고 있다.

대표적인 머신러닝에 대한 공격으로는 첫 번째, 머신러닝을 활용한 공격으로 공격자가 머신러닝을 활용하여 기존 공격방식을 고도화하거나 새로운 방식의 공격을 수행하는 방법이 있다. 두 번째, 머신러닝을 노리는 공격으로 공격자가 머신러닝을 교란시키는 목적으로 적대적 예시, 데이터 중독, 은닉음성 명령 등의 공격이 발생할 가능성이 있다.

따라서, 머신러닝을 보안 분야에 도입하고자 할 때 머신러닝 자체에 대한 보안위협 또한 고려하여 지속적인 모니터링 및 기술적 보완을 고려해야 한다. 이를 위해 현재 운영되고 있는 정보보호시스템의 보안 검토와 인증 제도를 머신러닝 기반의 보안기술에도 확대 적용하는 방안이 필요하다.

4.2.2. 설명 가능한 인공지능(XAI)

머신러닝, 딥러닝 등 인공지능 기술은 빅데이터와 복잡한 알고리즘 등을 기반으로 사용자에게 의사결정, 추천, 예측 등의 결과를 제공한다.

이에 일부 인공지능 기술은 알고리즘의 복잡성으로 블랙박스로 불리고, 도출된 최종 출력값의 근거, 도출 과정의 타당성은 알 수 없는 경향이 있다. 설명 가능한 인공지능은 사용자가 인공지능 기술 적용 과정과 결과를 이해하고 올바르게 해석하여 결과물이 도출되는 과정을 사용자가 이해하기 쉬운 방법으로 제시하는 것이다. 이를 위해 최근 LIME(Local Interpretable Mode-agnostic Explanations)이나 SHAP(Shapley Additive exPianations) 등을 이용하거나 통계적인 접근이나 시각화 등에 대한 연구가 활발하다. 미 DARPA는 2017년부터 XAI(Explainable AI) 프로젝트를 추진하여 사이버위협에 대한 능동적 대응 및 사용자 신뢰를 도모하고 있다.

Ⅴ. 결 론

지금까지 본 논문에서 보안관제 분야에 적용된 머신러닝 기술과 이를 통해 구현된 시스템이 보안관제에 성공적으로 적용되기 위한 관리적 측면과 기술적 측면에 대해서 알아보았다. 머신러닝 기반의 보안관제 기술은 기존의 보안관제 문제점을 해결해 줄 수 있는 아주 매력적인 기술임에는 틀림없다. 하지만, 아무런 준비 없이 받아들이면, 기존의 문제를 해결하는 것이 아니라 더 악화 시킬 수 있음을 인지해야 한다.

이에 본 논문에서는 관리적으로 연계 표준화와 양질의 학습데이터 관리, 보안전문가 육성 등이 이루어져야 하며, 기술적으로는 적대적 머신러닝에 대한 대응과 설명 가능한 인공지능 구현의 필요성을 말하였다. 이를 통해 머신러닝 기반의 보안관제 기술이 끊임없이 공격하는 사이버 위협으로부터 우리를 지켜주는 하나의 해결책이 되었으면 한다.

참 고 문 헌

[1] “2021 국가정보보호백서”, KISA, 2021.5

[2] 러 해커, 평창올림픽 사이버공격 두달 전부터 수백곳 해킹 시도, https://www.yna.co.kr/view/AKR20

201021003900071, 2020, 10
[3] KISA, 솔라윈즈 제품 보안 업데이트 권고, 2021. 02
[4] 한국인터넷진흥원, 기반시설 등을 공격대상으로 하는 랜섬웨어 피해방지를 위한 보안 대책 권고, 2021.05
[5] 국가정보보호백서 2021, 전담조직을 신설하지 않는 이유, pp. 223
[6] 한국 IDC, Market Pulse 2018, 6
[7] Capgemini Research Institute(2019), 'Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security', 11 July 2019.
[8] Deloitte Review - Deborah golden, Ted Johnson, AI로 증강된 사이버보안-어떻게 인지기술이 보안 노동력 부족을 해결할 수 있는가.
[9] Cisco(2019), 2019 연례 사이버보안 보고서.
[10] Terres, Alissa, “Building a World-Class Security Operation Center:A Roadmap.” SANS, 2015
[11] Why Your Business Needs A Security Operation Center, https://www.forbes.com/sites/eycybersecurity/2017/05/09/why-your-business-needs-a-security-operations-center/?sh=34436fb742aa , 2019, 05
[12] Duplicate Alerts Draining Security Analysts' Time https://www.securitymagazine.com/articles/87601-duplicate-alerts-draining-security-analysts-time, 2016, 11
[13] Gartner, Using the Predict, Prevent, Detect, Respond Framework to Communicate Your Security Program Strategy, 2016, 4
[14] 조창섭, "사이버공격 탐지 성능 개선을 위한 머신러닝 기반 보안관제 시스템”, 숭실대학교 박사논문, 2019. 6

〈저자소개〉

정 일 옥 (Jung il ok)
2001년 2월 : 전남대학교 물리학과 졸업
2008년 8월 : 고려대학교 컴퓨터정보통신학과 석사
2011년 3월~현재 : 고려대학교 정보보호학과 박사과정
<관심분야> 보안관제, 머신러닝, 정보보호, 침해사고

조 창 섭 (Cho chang seob)
1992년 2월 : 동국대학교 전자계산학과 졸업
2019년 8월 : 숭실대학교 IT정책경영학과 공학박사
<관심분야> 보안관제, 머신러닝, 사이버보안

지 재 원 (Ji Jae won)
2010년 2월 : 한남대학교 컴퓨터공학과 졸업
2012년 2월 : 한남대학교 컴퓨터공학과 석사
<관심분야> 관제기술, 머신러닝, 사이버보안