https://doi.org/10.5392/JKCA.2019.19.01.108

인공지능 기술기반의 통합보안관제 서비스모델 개발방안

Development of Integrated Security Control Service Model based on Artificial Intelligence Technology

오영택, 조인준
배재대학교대학원 사이버보안과

Young-Tack Oh(speedisk@daum.net), In-June Jo(injune@pcu.ac.kr)

요약

본 논문에서는 인공지능기술을 통합보안관제 기술에 효율적으로 적용하는 방안을 제안하였다. 즉, 통합보안관제시스템에 수집된 빅 데이터를 기반으로 머신러닝 학습을 인공지능에 적용하여 사이버공격을 탐지하도록 하고 적절한 대응을 한다. 기술의 발달에 따라서 늘어나는 보안장비와 보안 프로그램들로부터 쌓이는 수많은 대용량의 로그들을 사람이 일일이 분석하기에는 한계에 부딪히고 있다. 분석방법 또한 한 가지 로그가 아닌 여러 가지 이기종간의 보안장비의 로그까지 서로 상관분석을 해야 하기 때문에 더욱 더 통합보안관제에 적용되어서 신속한 분석이 이루어져야 하겠다. 이런 행위를 분석하고 대응하는 과정들이 효과적인 학습방법을 통해서 점진적으로 진화를 거쳐 성숙해가는 인공지능기반 통합보안관제 서비스모델을 새롭게 제안하였다. 제안된 모델에서 예상되는 핵심적인 문제점들에 대한 해결방안을 모색하였다. 그리고 정상 행위 기반의 학습모델을 개발하여 식별되지 않는 비 정상행위 위협에 대응력을 강화하는 학습방법을 도출하였다. 또한, 제안된 보안 서비스모델을 통하여 보안담당자들의 분석과 대응을 효율적으로 지원할 수 있는 보안관제에 대한 향후 연구방향을 제시하였다.

■ 중심어 : | 인공지능 | 머신러닝 | 통합보안관제 | 보안관제 | 서비스모델 |

Abstract

In this paper, we propose a method to apply artificial intelligence technology efficiently to integrated security control technology. In other words, by applying machine learning learning to artificial intelligence based on big data collected in integrated security control system, cyber attacks are detected and appropriately responded. As technology develops, many large capacity Is limited to analyzing individual logs. The analysis method should also be applied to the integrated security control more quickly because it needs to correlate the logs of various heterogeneous security devices rather than one log. We have newly proposed an integrated security service model based on artificial intelligence, which analyzes and responds to these behaviors gradually evolves and matures through effective learning methods. We sought a solution to the key problems expected in the proposed model. And we developed a learning method based on normal behavior based learning model to strengthen the response ability against unidentified abnormal behavior threat. In addition, future research directions for security management that can efficiently support analysis and correspondence of security personnel through proposed security service model are suggested.

■ keyword : | Artificial Intelligence | Machine Learning | Integrated Security Control | Security Control | Service Model |

접수일자 : 2018년 11월 01일
수정일자 : 2018년 11월 21일
심사완료일 : 2018년 11월 21일
교신저자 : 오영택, e-mail : speedisk@daum.net

Ⅰ. 서 론

1. 연구의 배경 및 목적

“2018 RSA 컨퍼런스”에서 사이버 공격의 정교성 증대와 더불어 공격범위 확대를 쟁점으로 삼았다. 또한, 공격기술의 많은 발전이 있음에도 불구하고 현재의 기술만으로 알려지지 않은 공격에 적절한 대응이 불가능함을 지적하였다. 이런 문제 해결을 위한 대안으로 비즈니스 중심의 보안접근방식으로 위험을 관리할 것을 주장하였다. "Together is Power"를 표방하며 전 세계 시큐리티 전문가 및 기업들이 힘을 모아야 현재 직면한 사이버 위협에 대응할 수 있을 것이라고 내다보았다. 이는 인공지능 그 자체를 공격하려는 시도와 같이 “사람이 절대 알아 볼 수 없는 차이를 데이터에 섞음으로써, 인공지능을 우회하고, 교란시키는 해커들이 등장” 하고 있는 사이버위협의 변화에 대해서 대응이 필요하다고 말하고 있다. 이러한 문제점은 단순히 사이버 보안뿐만 아니라, 다양한 응용분야에서 발견되고 있는 문제라고 볼 수 있다.

이처럼 사이버 위협은 기술적으로 지속적인 발전이 이루어지고 있다. 더불어 사이버 범죄, 테러와 같은 위협도 조직화 고도화됨과 더불어 복잡하고 다양한 형태로 진화하고 있다. 최근의 사이버 위협에 대한 현재의 기술적 연구개발 추이를 살펴보면, 인공지능 기반, 머신러닝 기반의 분석을 통한 효율적, 능동적, 선제적 대응방안 모색 등의 분야로 나누어 살펴볼 수 있다.

이와 더불어 글로벌 기업들의 위협정보 공유와 협력체계 강화가 중요한 시점이다[2]. 이런 이유로 사이버 위협들에 대해 인공지능 기반의 보안성 강화가 시급히 이루어져야 할 필요가 있다. 이러한 위협에 대응한 인공지능 기반의 보안성 강화의 핵심요소는 양질의 많은 위협정보 수집 및 분석을 들 수 있다. 이를 위해 관련 기업들의 협력기반을 확대하고, 이를 토대로 수집된 양질의 위협정보들을 인공지능 기반으로 분석·대응할 필요가 있다. 머신러닝을 활용한 인공지능 기술을 통해 자동화 할 필요가 있다. 이를 통해서, 급증하는 사이버 공격에 대응하고, 인공지능 기반의 보안관제 체계를 수립해야한다. 즉, 사람과 기계의 분업화를 통해 효율성을 강화해야하고 인공지능기술 기반의 통합보안관제와 같은 보안기술적용이 필요한 시점이다.

2. 연구의 내용 및 범위

국내·외 사이버공격은 해킹의 자동화로 무차별적인 공격 그리고 사이버 전면전 위험고조 등으로 나날이 지능화·고도화 되고 있다. 침해 이벤트 또한 기하급수적으로 증가하고 있고, 최근의 해킹 기법의 변화를 보면 제로데이 공격과 랜섬웨어와 같은 은닉기법을 비롯해 모바일 공격까지 증가하고 있다. 소셜 네트워크의 해킹으로 계정탈취와 개인정보유출 등의 공격도 증가하고 있는 추세이다[1]. 이런 다양한 공격에 대응하기 위해서 각 나라는 사이버 전사와 같은 보안전문 인력을 보유하고 있으나, 한정된 인력과 시스템의 한계로 인해 적기 대응하기에는 미흡한 실정이다.

이렇게 기하급수적으로 증가하는 추세에 있는 보안 이벤트를 보안담당자들이 모두 대응하기에는 한계에 부딪히고 있다. 본 논문에서는 이러한 복합적인 문제에 대한 하나의 해결책으로 인공지능 기반의 통합보안관제시스템을 효과적으로 구현하기 위한 통합보안관제 모델을 제안하였다. 본 논문의 내용을 살펴보면 다음과 같다.

제 Ⅱ 장에서는 통합보안관제 체계의 프로세스와 통합보안관제 현황과 문제점을 살펴보았다. 제 Ⅲ 장에서는 차세대 지능형 보안체계를 구축하여 잠재적인 위협탐지 및 선제적 대응을 통하여 지속적으로 변화하는 서비스 환경과 지능화되는 공격을 정리하였다. 제 Ⅳ장은 인공지능을 통한 통합보안관제 기법을 검증하기 위한 알고리즘의 이론적배경과 실험 및 평가에 대해 기술하였다. 제 Ⅴ장은 본 연구의 결론으로 연구의 결과를 정리하고 향후 보안분야에 추가적으로 연구가 필요한 부분을 기술하였다.

Ⅱ. 머신러닝기반의 인공지능 통합보안관의 필요성 및 활용방안

1. 통합보안관제 체계

일반적으로 통합보안관제 업무는 업무 성격에 따라 크게 3가지로 구분된다. 첫째, 보안 장비, 시스템의 장애를 파악하고 이력을 점검하며 보안 규제 준수 여부를 살펴보는 일련의 활동을 포함하는 '운영 및 관리' 업무이다. 각종 보안 장비가 기업의 IT 환경에 맞게 제대로 작동되고 있는지, 정책이 올바르게 설정되어 있는지, 각종 보안 장비를 수시로 관리하고 적절하게 운용 할 수 있는 능력이 요구된다. 방화벽, IDS, IPS, UTM, WAF, DDoS 대응 장비 등 여러 보안 장비에 대한 지식과 사용 경험, 최신 보안 규제에 대한 지식이 뒷받침되어야 함은 물론이다.

둘째, 공격자의 행위를 빠르게 탐지하고 우선적으로 해결해야 할 이슈, 위협 요소, 사고를 빠르게 판별해 대응하는 '탐지/분석/대응' 업무이다. 오늘날 공격이 지능화되고 다양화되고 있는 만큼, 네트워크 전반에 걸친 모든 정보의 흐름을 보다 빠르고 정확하게 인지해 다양한 위협을 확인하고 이에 대처할 수 있는 능력이 요구된다. 침해사고 발생, 악성코드/링크를 포함한 이메일 수신, 내부 정보 유출, 기업을 대상으로 한 디도스 공격 감행 여부 파악 등이 이에 해당된다.

셋째, 사고가 발생하는 것을 막고, 발생하는 경우에는 기민하게 대응해 피해를 최소화하기 위한 예방 업무이다. 알려진 공격은 물론 알려지지 않은 위협에도 기민하게 대응할 수 있도록 서버, 애플리케이션, 네트워크, SW 취약점을 점검하고, 유해 IP와 악성 URL 등 최신 위협 정보를 업데이트 한다. 또한, 임직원을 대상으로 한 모의 훈련을 실시하는 등 고도화된 위협에 대한 방어력을 높이고 임직원의 정보보안 인식을 제고하는 부분도 중요하다.

통합보안관제 업무는 대응 프로세스에 따라 구분될 수도 있다. 일반적으로, ▷이기종의 보안 장비에서 나오는 다양한 보안 데이터를 수집하는 '정보 수집 단계', ▷경보 발생에 따른 침해사고 및 해킹 패턴을 분석하고 다양한 장비에서 생성된 보안 데이터와 내·외부에서 수집된 최신 보안 위협 정보를 상관 분석하는 '모니터링/분석 단계', ▷공격으로 판단되는 이벤트에 대한 원인 및 대응책을 마련해 대응하는 '대응/조치' 단계, ▷침해사고 처리 및 장애 처리 결과를 정리하고 이를 관련 부서에 전달하는 '보고 단계'의 4단계로 나눠진다. 보안관제 서비스는 고객의 특성을 고려한 서비스 제공 형태에 따라 크게 3가지 유형으로 제공되고 있다. ▷관제센터에서 고객사의 보안 시스템을 원격으로 운영, 관리하는 형태로 비용효율성이 뛰어난 '원격관제', ▷보안관제 인력이 고객사에 상주하여 서비스를 제공하여 침해/장애 발생 시 즉각적인 조치가 가능한 '파견관제', 그리고 ▷기본적으로 원격에서 관제하되 침해 사고나 장애가 발생할 시에는 인력을 파견하여 빠르게 조치를 취하는 '혼합형 관제'로 구분되고 있다.

2. 인공지능 통합보안관제 체계

인공지능 기반 통합보안관제 설계 시 보안관제 노하우가 적용된 현황분석을 통해 최적의 학습데이터(Feature)가 정의되어야한다. 기 운영 보안관제시스템(SIEM)의 부하를 최소화하기 위한 방안과 최적의 인공지능 성능을 보장하는 설계를 통해 사고처리 예측과 비정상행위 탐지를 제공해야한다[1]. 이를 위해서 첫째로 보안분석 전문가가 투입되어 네트워크망 영역별 보안장비 구성현황과 DDos, IPS, TMS, F/W, 웹방화벽, 백신등과 망구성 현황을 파악한다. 또한, 보안관제 이벤트와 장비별 차단정책, 탐지정책의 보안정책 현황과 보안규칙 연동현황을 확인하여 공격 유형별로 분류가 필요하다. 이때 Web로그 및 시스템 로그까지 수집해서 향후 연관분석에 용이할 수 있어야 한다. 다양한 DDos 공격대응 시나리오, 웹해킹 공격대응 시나리오, 악성코드 공격대응 시나리오와 같은 침해대응 시나리오까지 분석을 해야 한다.

둘째로 보안관제시스템의 내장 인터페이스를 이용하여 실시간 이벤트를 수집하여 해킹에 대해서 공격유형별로 분류한다. 그리고 정탐과 오탐처리 내역으로 나누어서 경보이벤트에 대하여 정책분석을 해야 한다.

셋째로 정탐률 향상 프로세스 설계를 통하여 오탐률을 최소화 할 수 있는 프로세스를 수립해야한다. 마지막 네 번째로는 지도학습을 통한 이벤트 사고처리 예측 구현이 되고, 비지도 학습으로 비정상행위 탐지가 구현되어야 한다. 실제 구현 시에는 보안 분석전문가를 투입하여 보안장비, 보안정책 및 보안관제시스템의 보안

인프라 현황분석과 이벤트 처리현황 및 침해대응 시나리오의 보안관제 현황분석을 통하여 인공지능의 학습 데이터의 필드정의 및 추출을 하여야 한다.

표 1. 인공지능 통합보안관제 체계 목표

구분	목표
사용자 환경	• Model 추천 및 상세한 설명기능 • GUI기반 사용자 화면(Navigation)
스마트 플랫폼	• 모델계보관리를 통한 학습능력강화 • 지도, 비지도, 강화 등 다양한 학습 방식 • 공격 특성에 최적화한 알고리즘
고성능 플랫폼	• 자원활용 극대화를 위한 분산 및 병렬처리 • 대용량의 데이터 처리를 위한 분산 파일 체계 • 고속 분석을 위한 In-memory 검색
확장형 플랫폼	• 연계서비스를 위한 표준 API 지원 • 정교한 공격 사전예측, 위험도 별 탐지 및 대응연계를 위한 위험지표 도출

인공지능 통합보안관제 플랫폼의 기능적인 측면으로 본다면 인공지능 프로세스 정형화를 통한 체계적인 학습관리가 이루어진다. GUI기반 모델링, 자동 모델링 기능 구현을 통한 비 전문가 및 전문가 사용 편리성이 제공되어야한다. 또한, 머신러닝 알고리즘, 전처리 라이브러리 제공을 통한 공격 유형별 다양한 모델링 기능까지 고려되어야 한다.

플랫폼 응용 측면 사례로는 마케팅, 유통판매 및 장애예측, 예방정비 등 범용 플랫폼이 주종을 이루며 보안 플랫폼 사례는 없었다. 하지만 Craft ai 와 같은 기업들에서 클라우드 기반 AI-as-a-service 서비스 제공을 통하여 범용적인 서비스를 제공하고 있다.

적응형 보안체계(Adaptive Security 핵심 기능으로는 예측하기 위한 보안수준유지, 공격사전예측, 위험평가분석이 지원되어야한다. 지속적인 모니터링 및 사전 공격대응이 필요하고 외부 사이버 위협정보의 수집 및 활용이 필요하다. 예방으로는 시스템 보안수준 강화와 공격우회 유도, 사고예방이 지원되어야한다. 사이버대피소, 클라우드형 허니팟 운영과 서비스 중요도별 보안수준의 차등화가 필요하다. 탐지에서는 사고탐지, 위협확인 및 우선순위관리, 침해식별 및 격리를 위해 알려진 위협탐지 효율화 및 알려지지 않은 위협까지 탐지해야한다. 마지막 대응으로는 침해대응 정밀분석 보안정책생성 및 수정보안정책 자동화를 통해 신규정책 생성 및 정책 최적화와 고도의 정확한 알려진 위협탐지의 정합성이 확보되어야 한다. 이처럼 인공지능 통합보안관제를 위한 플랫폼은 다음과 같다.

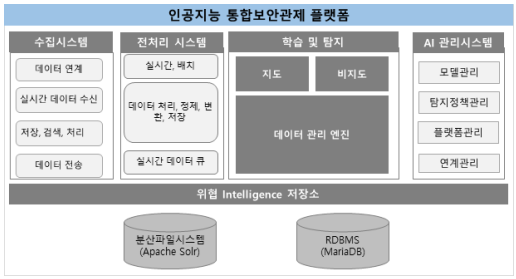

그림 1. 인공지능 통합보안관제 플랫폼

또한, 인공지능 통합보안관제 플랫폼 구축 시에는 알려진 공격, 이상행위 탐지, 신규 공격기술 탐지 대응능력 강화 및 축적을 고려해야한다. 비 전문가 및 전문가를 위한 사용자 환경을 제공하여 손쉬운 사용성을 제공해야한다. 그리고 기능 및 효과가 검증된 플랫폼의 적용으로 탁월한 학습관리 및 확장성이 확보되어야 한다.

3. 인공지능 데이터 수집방안

학습데이터 및 예측데이터를 생성하기 위해서 통합보안관제시스템으로부터 원본로그와 이력데이터 등을 수집한다. 원본로그를 기계가 학습하기 쉬운 형태로 변형하는 과정으로 분석가의 노하우에 의한 특성값 추출이 필요하다. 특성값 추출에 의해 머신러닝의 정확도 및 신뢰도가 높아지기 때문에 매우 중요한 단계이다. 이를 위해서 수집시스템 별 학습 및 탐지 데이터에 대한 용량정보를 사전에 확보하고 탐지데이터, 학습데이터에 대한 데이터 흐름 및 데이터 수집 시 이슈사항에 대하여 사전에 고려하여 수집하여야 한다. 학습데이터 및 예측데이터를 생성하기 위해 인공지능 수집기를 통해 보안관제시스템(SIEM)으로부터 원본로그와 이력데이터를 수집한다.

인공지능 수집기에 의한 표준화된 인터페이스를 제공하여 추후 외부 데이터로딩이 필요할 경우 수집기의 추가 구현에 대비하고 인공지능 수신기가 소켓통신하여 실시간 원본로그를 전달한다[2]. 데이터수집으로 원

본로그가 있는 시스템에 부담을 주지 않고 실시간으로 빠르게 수집하고 연계 할 수 있다. 그래서 에이전트 설치나 별도 개발 없이 보안관제시스템(SIEM)에 영향을 주지 않는 최선의 방안으로 수집해야 한다.

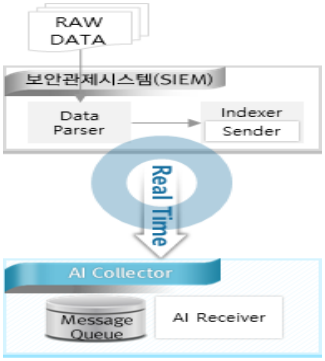

그림 2. 학습대상 데이터관리 수집/연계 방안

이를 통하여 보안관제시스템(SIEM)에 내장되어있는 인터페이스를 이용하여 로그를 보내는 시스템과 인공지능 수신기가 소켓통신을 통해 실시간 이벤트를 수신한다. 로그를 보내는 시스템은 CPU의 점유율이 높은 로그파싱이 이루어진 후에 이벤트를 전송하기 때문에 쿼리방식이나 파일 엑세스 방식 대비 레거시 부하 최소화 할 수 있다.

4. 인공지능 데이터 전처리 방안

데이터의 수신, 정제, 변환의 고속 처리를 위한 데이터 복제 및 분산 처리방안으로는 단계별 저장을 통한 전처리 데이터 완결성 보장되어야한다. 또한, 스키마 종속성이 없는 유연한 모델로 데이터 타입에 높은 자유도 부여하여야 한다.

데이터 전처리 요건으로 크게 세 가지가 있다.

첫 번째로 데이터의 처리에서는 수집시스템에 적재된 데이터를 선택하여 추출하고 분석가 요구사항에 따라 샘플링 기능이 구현되어서 분산 인메모리 저장소에 검색조건(데이터명, 날짜, 시스템명 등)을 통해 데이터를 선별하고, 표집데이터를 임시 저장한 뒤 사용자 인터페이스를 통해 탐색적 분석 지원을 할 수 있어야 한다.

두 번째로 데이터 정제과정을 위한 고속 처리를 위하여 사용자가 선택한 필드의 정제가 가능해야한다. 또한, 인메모리 방식의 분산처리 아키텍처를 통한 대규모 데이터 분산병렬 기능으로 구현되어야 데이터 압축을 통한 성능 향상을 기대할수 있다. 직관적인 필드 선택을 통해 정제하며 정제 정책을 DB와 XML 파일로 관리하여야 효율성을 높일 수 있다

세 번째로는 데이터의 변환으로 사용자가 정의한 변환정책의 유연한 적용이 가능해야한다. 탐지를 위한 고속 전송 및 완결성 보장되어야 태깅, 기본수치화, 정밀수치화 기능을 모듈화하며 변환정책에 따른 행동간 워크플로 지원까지 가능할 수 있다. 이를 통하여 인메모리 기반의 마이크로 배치작업을 통해 변환하며 전송 시 병목을 예방코자 큐(Queue) 가 사용되어야 한다.

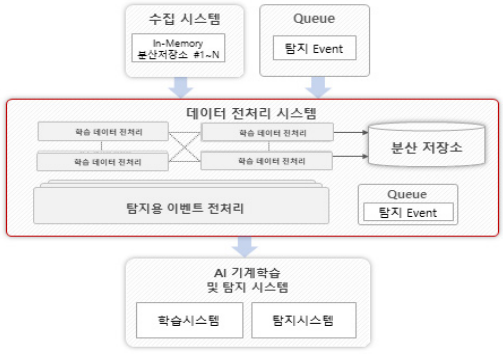

그림 3. 데이터 전처리 구성도

데이터의 전환 시에는 사전분석 및 철저한 검증을 통해서 수행되어야 한다. 필요에 따라서는 분석가의 심도 있는 검증이 동반되어야 한다.

5. 인공지능 데이터의 머신러닝 및 탐지체계

공격유형별 시나리오 기반의 학습데이터와 침해사고 대응 이력을 학습데이터로 생성한다[3]. 그리고 지도학습 (Supervised Learning) 알고리즘을 통해 이벤트 사고처리 분석가(관제인력)에 의한 피드백 프로세스를 통해 모델을 개선해 나아간다. 지도학습 과정과 공격유형별 시나리오 그리고 사용자 행위 분석 기반의 학습데이터를 생성한다.

이 학습데이터에 비지도학습(UnSupervised Learning) 알고리즘을 적용하고, 비정상행위 탐지 분석가(관제인력)에 의한 피드백(Feedback) 프로세스를 적용해서 모델 개선 및 공격 유형에 대한 예측이 가능하도록 한다. 이때, 행위기반학습(Active Learning) 아키텍처를 통하여 오탐을 줄이는 학습되어야 한다.

인공지능을 활용한 통합보안관제에서 탐지체계에는 기존 보안관제시스템(SIEM)과의 상호 연계모델을 이용하여 불필요한 리소스 낭비를 줄인다. 동일한 DB/UI를 사용해서 가용성을 증가시키고, 장애율을 감소 시킬 수 있다. 정탐률을 높이기 위한 방안으로 최적의 알고리즘 2개이상 결합하여 더 좋은 결과를 도출하기 위한 앙상블 기법을 적용해야한다. 또한, 알고리즘간의 호환성이나 성능적인 문제를 상호 보완하도록 한다. 이때 성능적인 문제점으로 단순히 여러 알고리즘을 같이 돌리기만 하는 것은 무의미하며 전문가의 충분한 고려와 테스트를 통해 최적을 알고리즘을 선정하여야 한다.

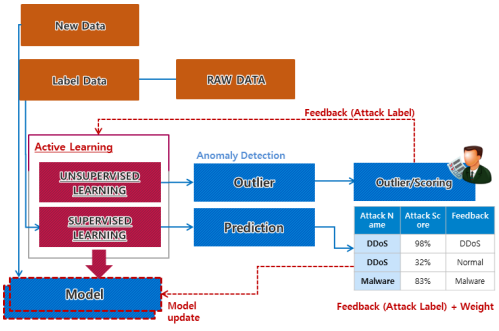

그림 4. 행위기반 학습(Active Learning) 구조

결과에 대한 오탐(False Positives)을 줄이기 위한 방안으로 피드백 반영 모델 및 초 매개변수 최적화 기술을 적용할 수 있다. 피드백 반영 모델은 예측된 결과에 대해 분석가(관제요원)의 추가 피드백을 통해 모델이 발전하고 정확도를 향상시키는 기술이다. 학습 데이터 특성값 선정에도 매개변수 최적화를 적용하여 격자탐색방법과 같이 매개변수의 개수가 많아져 그 차원이 높아지면 격자 탐색은 모든 경우의 수를 대입하는 것이 불가능해 진다[4]. 결국 후보집한이 한정됨을 예방해야 한다. 격자탐색은 중요하지 않은 매개변수와 중요한 매개변수를 동일하게 관측할 수 있도록 해서 정확도를 향상 시킬수 있도록 한다

학습에 대한 모델이 생성되면 점수를 통한 모델성능평가와 행렬을 통한 모델 성능평가 이루어진다. 이를 통해 최적화된 모델을 적용함으로써 오탐을 줄일 수 있다. 그래서 혼동행렬에 의한 정확도 수치와 성능에 대한 수치화를 통해 사용자는 최적의 모델을 선택하여 적용할 수 있다

Ⅲ. 인공지능 통합보안관제 서비스 모델 개발 방안

1. 서비스 모델 개요

인공지능이 적용된 통합보안관제체계를 위해서는 탐지 후 분석과 대응하는 보안체계에서 예측, 예방, 탐지, 대응하고 스스로 진화하는 체계 마련해야한다. 정상기반의 학습모델을 개발하여 비정상행위로 식별되지 않는 위협에 대응하는 능력 강화하도록 해야한다. 관리대상에 대한 사이버 위협의 오탐을 줄이고 선제적 대응하는 예방 체계 마련할 수 있도록 해야 한다.

2. 서비스 모델의 알고리즘 동향

미래형 인공지능 알고리즘을 적용하여 오탐률 최소화 및 탐지 성능 개선 알고리즘이 개발되고 있다. 알려지지 않은 위협정보 중에서 발생 빈도가 낮은 신규 위협 탐지를 위한 서비스 모델 개발을 위한 알고리즘들도 속속들이 개발되고 있다.

룰 베이스 모델은 처리 속도가 빠르고, 직관적인 알고리즘이지만, 룰에 정의되지 않은 공격은 탐지 불가하다. 이미 많이 알려진 머신러닝(Machine Learning)의 지도 학습 알고리즘은 답안을 선 제시하는 라벨리드 학습을 통해 새로운 이벤트에 대한 정상/비정상 자동 판별 과 탐지 커버리지 확대가 가능하다. 하지만, 실제 비정상(공격)데이터가 적은 단점과 대량의 데이터 태깅 문제를 야기할 수 있다

비지도 학습 알고리즘은 언라벨리드 학습을 통해 새로운 이벤트에 대한 유형 자동 분류가 가능하지만 지도 학습에 비해 오탐률이 높을 수도 있다

인공지능의 하이브리드 알고리즘은 지도 학습 모델로 정상 모델 탐지 후 비지도 학습을 활용해 이상 행동에 대한 유형 분류가 가능하다. 또한, 오탐률 최소화 및 학습 성능 개선해 낳아갈 수 있다.

신규 위협 탐지를 위하여 알려지지 않은 새로운 위협에 대한 대응은 가능하지만 학습기 선택 및 결합 방식이 매우 중요해서, 신규 위협탐지를 위해서는 충분한 테스트가 필요하다.

3. 서비스 모델 설계 원칙

학습 모델 설계 방향은 데이터의 수집부터 위험도평가와 모니터링 맵 까지 고려한 End to End 모델을 기준으로 설계되어야한다. 그리고, 알려진 공격 패턴과 정상 데이터 기준으로 학습 모델 설계를 기본으로 한다. 향후 조직적, 지능적인 신규 사이버 위협에 대응하는 지속 진화하는 학습모델로 설계해야한다[5].

학습 데이터 설계 원칙은 로그시스템의 저장된 정형화 데이터 시간과 일 단위 데이터를 병렬 처리 기반의 통합적 요청 및 수집해야한다. 실시간 데이터 와 배치 대용량 데이터 처리의 성능과 품질을 고려한 전처리 워크플로우로 구성되어야 한다.

기본적인 전처리 워크플로우는 인공지능 관리기능을 통해 전처리 라이브러리(일반화/ 군집화 등)로 구성한다. 그 외 기능은 수작업과 전처리 라이브러리 추가를 통하여 전처리 워크플로우를 완성해야 한다.

4. 서비스 모델 개발 방법

사이버 위협 유형과 상황에 따라 유연한 개발을 위한 MBD(Model-ID Based Development) 방법론 기반으로 개발되어야한다. 또한, 데이터 분석 노하우 및 인공지능 기술의 전문가의 직접적인 참여가 있어야한다. 그리고, 융통성을 가지고 서비스 모델의 상황에 따라 plug & play 할 수 있는 재 사용성이 제고되어야 한다. 또한, 소프트웨어의 유지보수성을 위해 공격 위협의 변화에 효과적으로 대응하기 위한 빠른 현지화(Localization) 전환을 고려하여야 한다.

개발을 위한 절차로는 학습/검증 데이터를 선별하여 수집하고 데이터의 특성값을 확정하여야 한다. 이때 선정된 알고리즘을 통해 학습/평가가 이루어진다. 그리고 서비스모델을 통한 검증 및 평가를 통해 강화 학습을 수행하고 마지막으로 테스트 배드를 통한 시뮬레이션 및 서비스 모델을 배포 한다.

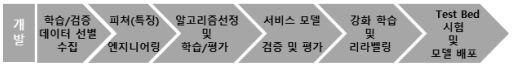

그림 5. 서비스모델 개발 절차

Ⅳ. 인공지능을 통한 통합보안관제 기법 검증

1. 알고리즘의 이론적 배경

머신러닝의 학습법 알고리즘에서 비 지도학습 러닝은 문제만 주고 정답은 수많은 데이터들로부터 스스로 학습해서 정답을 찾도록 하는 알고리즘 이다. 지도학습 러닝은 문제와 정답까지 주고, 이런 데이터를 가지고, 스스로 학습하는 알고리즘 이다. 좀 더 이해를 돕자면, 비 지도학습 러닝은 어떠한 데이터를 주었을 때 출력값에 대한 정보 없이 비슷한 데이터들을 군집화 하는 학습방법을 통해서 문제를 해결하는 알고리즘 이다.

지도학습 러닝은 어떠한 데이터를 줄때 출력 값도 함께 주는 방식으로, 이런 값들을 통해서 기계학습을 하는 알고리즘 이다. 주로 인식, 분류, 진단, 예측 등의 문제해결에 적합하고 비 지도학습 러닝에 비해 성능이 좋으나 좋은 결과를 위해서는 시간과 비용이 많이 든다는 단점이 있다.

앞서 말한 두 가지 학습 알고리즘을 통해서 인공지능이 강화된다. 또한, 행위기반(Active Learning)으로 SIEM과 같은 빅데이터 시스템을 통해서 실시간으로 수집되는 대용량의 보안 이벤트와 로그머신를 활용한다. 머신러닝을 적용하더라도 보안전문가와 인공지능의 결합을 통한 선순환 구조가 더해지면 정말 최적의 머신러닝 학습이 된다[6]. 그래서 오탐(False Positives)을 줄이고 정확도를 향상시켜 결국 보안에서 인공지능도 보다 높은 탐지율로 빠르게 대응 할 수 있다.

2. 서비스모델의 구현방안

비지도 학습(Unsupervised Learning)에 의한 네트워크 비정상 행위 탐지 기능 확인 할 수 있고, 네트워크 이상치 탐지(Network Anomaly Detection)와 유형별 경보 및 이상치 스코어, 위협정보, 시각화정보의 상세내역을 볼 수 있다.

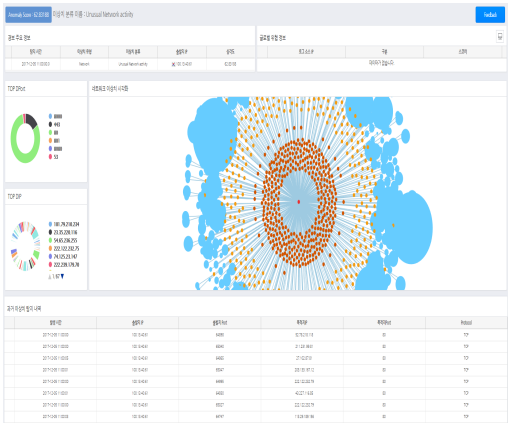

그림 6. 네트워크 이상치 탐지내역

지도 학습(Supervised Learning)에 의한 사고처리 예측과 기존 보안관제시스템 발생 경보에 대한 사고처리 예측심각도가 점수 형태로 보여진다.

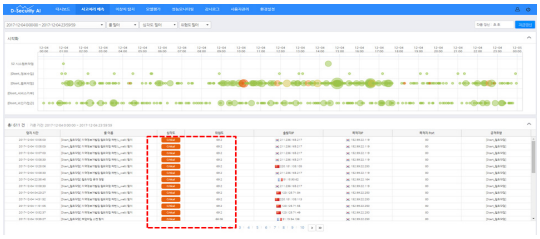

그림 7. 발생 경보, 사고처리예측, 예측률

V. 결 론

사이버공격이 자동화됨에 따라 기하급수적인 보안 이벤트들이 발생함에 따라 현재의 수작업 중심의 기술로 모두 대응이 불가능하다는 문제를 지닌다. 기존의 보안 분석 체계와 다르게 이들은 단순한 로그와 더불어 다양한 이기종의 장비로그들을 대상으로 서로 상호연관성 뿐만 아니라, 기존의 보안이벤트에 대한 대응 방법들도 포함되어 분석되어야 한다. 본 논문에서는 이러한 문제점에 대한 하나의 해결책으로 보안이벤트 처리에 인공지능 기술을 적용하여 효율적인 통합보안관제를 실현할 수 있는 방안을 새롭게 제안하였다.

이를 위해 기존 연구들과 다르게 본 논문에서 데이터의 수집처리부터 머신러닝기술을 도입하여 인공지능의 처리능력을 강화하는 학습방법을 제안하였다. 그리고 이를 통한 탐지체계를 새롭게 제시하였다. 이를 통해 향후 효율적인 인공지능 통합보안관제시스템 구축을 위한 서비스 모델을 개발하였다. 이 모델은 수집된 데이터에 보안 분석가의 노하우가 적용된 인공지능이 개발될 수 있도록 하였다.

인공지능을 활용한 통합보안관제에서는 무엇보다 데이터가 중요하며, 이러한 데이터는 내부 데이터뿐만 아니라 외부의 보안이슈까지도 함께 적용되어야 한다. 본 연구에서는 다양한 로그데이터의 정형화 방안에 대한 한계점이 있을 수 있다. 그래서 외부 정보공유시스템이 정형적인 데이터형식으로 다양한 통합보안관제서비스에 활용이 가능하도록 표준화 및 공유체계를 위한 표준적인 정보공유시스템의 연구가 지속되어야 할 것이다.

참 고 문 헌

[1] 김진홍, *공공기관의 아웃소싱 보안관제 수준 측정 지표에 관한 연구*, 숭실대학교 대학원 논문지, 2014.

[2] 정진영, *인공지능을 활용한 금융권 통합보안관제 자동화 방안*, 건국대학교 정보통신대학원, 석사학위논문, 2018.

[3] 김영인, *국방 인공지능(AI) 활용방안 연구*, (사)한국융합보보연구소 연구보고서, 2017.

[4] 최지우, *빅데이터 기반의 보안관제 방안에 대한 실증적 연구*, 공주대학교, 2015.

[5] 신기동, *효과적인 보안관제 방법론 정립*, 한국산

업기술대학교 대학원, 2014.
[6] 김규일, *보안관제 효율성 제고를 위한 실증적 분석 기반 보안이벤트 자동검증 방법*, 한국과학기술정보연구원, 2014.

저 자 소 개

오 영 택(Young-Tack Oh) 정회원

- 2013년 2월 : 한밭대학교 컴퓨터공학과(공학사)
- 2014년 7월 ~ 현재 : 이글루시큐리티(보안컨설턴트)
- 2017년 3월 ~ 현재 : 배재대학교 사이버보안과(공학석사)

<관심분야> : 정보보호, 인공지능, 보안컨설팅

조 인 준(Jong-Bok Kim) 정회원

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

<관심분야> : 정보보호, 컴퓨터네트워크보안, 전산조직응용