Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 8 pp. 607-614, 2023

https://doi.org/10.5762/KAIS.2023.24.8.607
ISSN 1975-4701 / eISSN 2288-4688

보안운영센터(SOC)의 효율성 향상을 위한 관제 지원 인텔리전스 설계 및 구현

김진원[1], 이용준[1*], 이상도[2]
[1]극동대학교 일반대학원 인공지능보안학과, [2]육군사관학교

Design and implementation of control support intelligence for the enhancement of efficiency in the Security Operations Center (SOC)

Jin-Won Kim[1], Yong-Joon Lee[1*], Sang-Do Lee[2]
[1]Department of Artificial Intelligence Security, Graduate School, Far East University
[2]Korea Military Academy

요 약 최근 다양하고 복잡한 인공지능 기반 사이버 공격에 대응하기 위해 보다 체계적인 보안 통제 정책이 적용되고 있다. 공격 유형이 점점 고도화되는 가운데 여전히 SIEM(보안 정보 및 이벤트 대응)과 같은 탐지 솔루션을 사용하여 악의적인 행동을 탐지하고 있으며, 많은 보안 전문가들이 보안 운영 센터(SOC)를 기반으로 관제 작업을 수행하고 있다. 본 논문에서는 SOC에서 인공지능 기반의 관제 업무 지원시스템을 설계하고 구현하였다. 제안된 시스템은 SOC에서 보안관제 업무를 수행하는 주요 과정인 티켓에 초점을 맞춰 인공지능이 티켓의 위험도에 따라 직접적인 업무를 처리하거나 지원할 수 있도록 하고 그 결과 관제요원이 처리해야 할 업무량의 감소가 기대된다.

Abstract To counter recent diverse and sophisticated AI-based cyberattacks, more systematic security control policies are being applied. Attack types are becoming increasingly advanced, but malicious activities are still being detected using solutions such as security information and event management (SIEM). Many security experts are performing control tasks based on a security operations center (SOC). This paper describes the design and implementation of an AI-based monitoring support system in an SOC. The proposed system focuses on tickets, which are used in the primary process of performing security operations tasks in the SOC. They enable AI to handle or assist with tasks directly according to the risk level of the tickets. As a result, a reduction in the workload for operations personnel is anticipated.

Keywords : SOC, Security Monitoring, AI, Classification, Similarity

1. 서론

보안운영센터(Security Operations Center, SOC)에서 일어나는 보안관제 업무의 효율성을 높이기 위한 연구로 특히 인공지능 기술을 활용하여 관제 요원의 업무 부담을 줄이는 기술적 방법을 연구한다. IT와 사이버 보안 기술의 발달은 사회를 안정적이고 편리하게 하지만 정부, 공공기관, 기업을 대상으로 한 해킹사고와 위협 수준은 계속해서 증가하고 있다. 이 때문에 기관과 기업은 지속적인 사이버 위협에 부담이 늘어가고만 있으며 이에 대비하기 위해 사이버상에서 일어나는 침해사고 대응을 위해 보안관제 업무를 보다 강화하고 있다[1]. 데이터와 자산을 보호하기 위해 새로운 위협에 대응하고자 보안관제 업무를 보다 신속하고 편리하게 지원하고자 등장한

*Corresponding Author : Yong-Joon Lee(Far East University)
email: bigman2u@naver.com
Received July 7, 2023 Revised August 7, 2023
Accepted August 10, 2023 Published August 31, 2023

것이 보안운영센터이므로 이는 조직의 전체 IT 인프라를 연중무휴 24시간 모니터링한다. 사이버 보안 이벤트를 실시간으로 감지하고 최대한 빠르고 효과적으로 해결하는 사내 또는 아웃소싱 IT 보안 전문가(관제요원)의 보안 관제 업무를 수행하기 위한 모니터링 시스템이다. SOC에서는 모든 사이버보안 기술 및 운영을 통합하고 조정하여 조직의 위협 감지, 대응 및 예방 능력을 개선한다. SOC는 조직의 사이버 보안기술을 선택, 운영, 유지관리하고 위협 데이터를 지속적으로 분석하여 조직의 보안 준비 태세를 개선하는 방법을 찾는다. 대량의 로그 데이터 중에서 실제 위험을 포함한 로그를 판별하는 것은 난해하고 어려우며 복잡한 작업이다[2]. 또한 SOC 운영진의 주관적 판단에 의존하기 때문이다. 즉 판단의 일관성의 유지는 더욱 어렵다[3]. 따라서 관제 시스템에 적용하여 효율적인 보안관제 업무를 보조할 수 있는 인공지능 기반의 분류, 오류탐지, 이상 행위 감지가 가능한 시스템의 필요성이 대두되고 있다[4]. 업무 부담을 가중하는 요인들로부터 이러한 문제에 대응할 수 있는 연구를 통해 보안관제 업무의 효율성을 높일 방법을 찾기 위해 AI 기반의 시스템을 적용하는 기술적 설계 및 구현을 연구한다. 이 연구에서 보안관제 업무의 효율성을 높이기 위해 인공지능 기술을 활용하는 방안을 제시한다. 본 논문은 보안운영센터에서의 보안관제 업무의 효율성 향상을 위해 인공지능 기술을 활용하여 기존 위협 인텔리전스의 한계점을 보완하여 향상된 관제 지원 인텔리전스를 목표로 한 관제 지원 시스템의 설계와 구현에 대해 다룬다.

이 논문의 1장은 서론으로 연구 배경을 다룬다. 2장에서는 관제 SOC의 관제 업무 및 티켓 처리 내용을 다룬다. 이벤트 관리를 위한 SIEM(Security Information and Event Management) 시스템의 개요와 관제 시스템에서 발생하는 Offense 이벤트에 대해 설명한다. 또한, SIEM 기반의 관제 시스템과 SOC의 개요와 역할을 기술한다. 3장에서는 제안하고자 하는 관제 지원 인텔리전스를 설계 및 구현한다. 4장에서는 구현된 결과를 토대로 성능을 평가한다. 5장은 결론으로 연구 결과와 향후 연구를 기술한다.

2. SOC의 티켓 기반 관제 업무

2.1 SIEM과 Offense events

SIEM은 보안 위협을 파악하기 위해 여러 출처로부터 수집된 로그와 이벤트를 분석한다. 이 과정에서 Offense

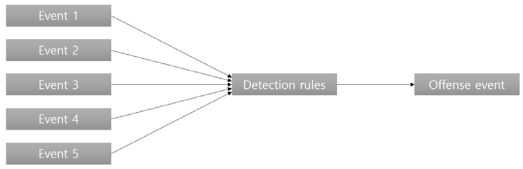

Fig. 1. Offense events

이벤트가 발생한다. Fig. 1과 같이, Offense 이벤트는 여러 이벤트가 특정 조건에 따라서 한 집합으로 묶여서 관리되는 것을 의미한다. 이를 통해 이벤트의 중복을 방지하고, 보안 위협을 더 효율적으로 관리할 수 있다. SIEM 기반 관제 환경에서의 Offense 이벤트는 네트워크 내에서 발생한 보안 위협이나 비정상적인 활동에 대한 통합된 정보나 경고를 의미한다[5]. Offense 이벤트는 시스템이나 네트워크에서 수집된 다양한 로그 데이터와 보안 이벤트를 통합하여 분석한 결과를 토대로 생성되며, 해당 이벤트의 심각도, 관련된 소스와 대상, 발생 시각 등의 정보를 포함하고 있다[6]. SIEM 시스템은 수집된 로그 데이터와 이벤트를 분석하여 비정상적인 활동이나 보안 위협을 감지하고, 이에 대응하는 Offense 이벤트를 생성한다. 생성된 Offense 이벤트는 보안 팀에 알림을 보내서 해당 이벤트를 조사하고 필요한 조치가 수행될 수 있도록 돕는다.

SIEM에서 이벤트가 발생되는 단계는 탐지 단계에서 많은 이벤트들이 오탐(False Positive), 미탐(False Negative)의 문제를 해결하는 데 어려움이 있다. 오탐은 실제로는 문제가 없지만, 문제가 있다고 판단하는 경우를, 미탐은 실제로는 문제가 있지만, 문제가 없다고 판단하는 경우를 의미한다. 이 두 가지 문제는 서로 Trade-off 관계에 있어서, 하나를 해결하기 위해서는 다른 하나가 악화될 수 있다. 이러한 Trade-off 관계는 결과적으로 SIEM 기반의 관제시스템에서 시그니처 탐지 룰을 지정하는 것에 있어서 반드시 어느 한쪽을 일부 포기하여야 한다는 문제점을 가지고 있다. 따라서 제안하고자 하는 관제 지원 인텔리전스는 강력한 탐지 룰을 위해 발생하는 오탐을 관제 분석 및 처리 단계에서 줄이는 것이 목표이다.

2.2 SOC의 관제 업무

SOC에서는 보안관제 업무를 처리하고 수행하는 라이프 사이클은 모두 티켓(Ticket)이라는 개념으로 접근한다. 이 티켓은 생성, 진행, 소멸의 단계로 구성되어 있으

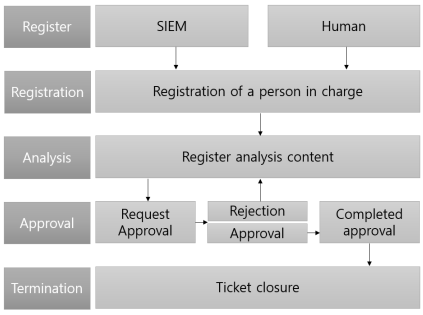

Fig. 2. Security Monitoring Process

며 담당자를 지정하고, 담당자가 분석을 시행하며 분석된 내용은 관리자를 통해 결재를 요청할 수 있다. 즉 티켓은 보안관제 업무에 있어서 개별 업무 단위로 볼 수 있다. 티켓 처리는 관제 업무의 핵심 요소 중 하나로, 보안 사고 수준의 위협 행위에 대한 접수, 분석, 해결, 그리고 보고를 포함하는 프로세스를 말한다. 보안 위협, 시스템 오류, 사용자 문제 등 다양한 이슈가 발생할 때마다 이는 티켓으로 생성되고 관리된다. Fig. 2와 같이 티켓 처리 과정은 먼저 티켓의 생성으로 시작된다. 티켓은 다양한 방법으로 생성될 수 있으며 이는 보안 시스템이나 네트워크 모니터링 도구에서 자동으로 생성되는 경우, 또는 사용자가 문제를 보고하는 경우 등을 포함한다. 생성된 티켓은 일반적으로 특정 형식을 따르며, 문제의 세부사항, 발생 시간, 관련 시스템, 중요도 등의 정보를 포함한다. 티켓이 할당되면, 해당 팀, 각 요원은 문제를 분석하고 해결하기 시작한다. 이 과정에는 문제의 원인을 파악하고, 적절한 해결 방안을 찾고 필요한 조치를 실행하는 것이 포함된다[7]. 복잡한 문제의 경우에는 추가적인 요원에게 도움을 요청할 수 있다. 문제가 해결되면 티켓 시스템에 기록되며 이를 통해 관제팀은 문제 해결 과정을 추적하고 관리할 수 있다.

2.3 위협 인텔리전스의 한계점

SOC에서는 보안관제 업무를 처리하기 위해 위협 인텔리전스를 참고 판단하여 활용한다. Fig. 3과 같이 위협 인텔리전스(Threat Intelligence)는 보안 위협에 대한 정보를 수집, 공유하는 시스템을 말한다. 이는 다양한 소스로부터 위협 정보를 수집하고, 이를 조직 내부 또는 외부와 공유하여 보안 대응을 돕는다. 위협 인텔리전스의 목표는 보안 위협을 이해하고, 이에 대비하며, 이를 방어하는 것이다. 위협 인텔리전스는 공격자의 동향, 행동 패턴, 사용하는 도구 등에 대한 정보를 수집하고 분석하여 보안 위협에 대응하는데 필요한 정보를 제공하며 이를 통해 조직은 자신들을 대상으로 하는 현재 또는 미래의 위협을 이해하고, 이에 대응하는 전략을 수립할 수 있다. 현재의 위협 인텔리전스는 정보의 표준화가 부족하고, 공유되는 정보의 질이 일정하지 않다는 문제가 있다.

Fig. 3. Threat Intelligence

위협 인텔리전스 공유는 다양한 소스에서 얻은 보안 위협 정보를 각기 다른 기관, 조직, 그리고 개인들과 공유하는 것을 말한다. 이러한 공유는 보안 위협에 대한 보다 넓고 깊은 이해를 가능하게 하고 효과적인 보안 대응을 위한 전략과 행동을 설계하는 데 도움을 준다. 그러나, 현재의 위협 인텔리전스 공유 환경에는 여러 가지 한계점이 존재한다. 주요한 한계점들로는, 위협 인텔리전스 공유는 정보의 품질과 신뢰성에 크게 의존한다. 이는 정보의 정확성, 완전성, 그리고 최신성을 포함한다. 하지만, 현재의 공유 환경에서는 이러한 요건을 만족하는 정보를 얻는 것이 어렵다. 이는 공유되는 정보의 출처와 질에 대한 불확실성, 그리고 이를 확인하고 검증하는데 필요한 자원의 부족 때문이다.

정보를 공유하는 것은 종종 보안과 프라이버시에 대한 문제를 일으킨다. 이는 특히 공유되는 정보가 민감하거나 기밀성이 높은 경우에 그렇다. 많은 조직은 자신들이 가진 정보를 공유하는 것을 주저하게 된다. 이는 위협 인텔리전스 공유의 효과를 저하시킨다. 따라서 제안하고자 하는 관제 지원 인텔리전스는 동일한 탐지정책(Detection rule)을 전제로, SOC에서 종료된 관제 티켓 정보를 수집하고 이 정보 자체를 공유하는 것이 아닌, 인공지능을 활용하여 분석 대상의 분석 결과(위험도, 오탐, 분석내용 추천, 이상 행위)만을 반환하여 기존 공유정보에 대한 위협 인텔리전스의 한계점을 보완한다.

3. 관제 지원 인텔리전스 설계 및 구현

3.1 인공지능 모델 선정

모든 시스템은 SOC에서 종료된 티켓을 통해 추출된 피처를 바탕으로 인공지능 모델은 티켓의 위험도 분류와 모델의 추천 내용를 측정하는 데 사용되는 여러 기존 분석 내용들을 학습한다. 이를 통해, 유사한 티켓을 식별하

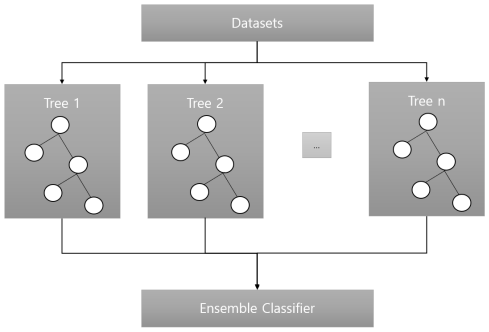

Fig. 4. XGBoost Classifier model

고 같은 카테고리의 티켓들의 처리 결과를 비교하는 등 다양한 분석이 가능하다. 결과 해석 단계에서는 이 인공지능 모델을 사용하여 측정된 유사도 결과를 해석하고 이해한다. 이 과정을 통해 관제 티켓의 유사성을 보다 정확하게 파악하고 분석할 수 있다. 이런 방식으로 SOC에서 제안 추천을 할 수 있다. 선택된 인공지능 알고리즘을 통해 Offense 이벤트를 고위험도와 저위험도로 분류하는 모델을 훈련하였다. 훈련 과정에서는 검증 데이터를 활용해 모델의 성능을 지속적으로 평가하였고, 과적합을 방지하기 위한 조치를 취하였다. 인공지능 기반의 관제 지원 인텔리전스를 개발하기 위해 XGBoost(Extreme Gradient Boosting) 모델을 사용하였다. Fig. 4와 같이 향상된 머신러닝 알고리즘으로 각기 약한 예측력을 가진 다수의 결정트리(weak learner)를 앙상블하는 방식으로 작동한다. 이 알고리즘은 각 결정트리의 예측 오차를 최소화하는 방향으로 반복적으로 새로운 트리를 추가함으로써, 복잡한 데이터 패턴을 높은 정확도로 예측한다. 이 과정에서 과적합 방지를 위한 정규화 항을 포함하여, 손실 함수를 최적화한다. 결정트리의 구조를 최적화하는 과정에서 XGBoost는 트리 분기점에서의 피처 중요도를 계산하고 이를 이용해 피처 선택을 수행한다. 이는 각 피처가 모델의 예측 성능에 얼마나 기여하는지 평가하며 이를 통해 중요한 피처를 식별하고 불필요한 피처를 제거한다. XGBoost는 병렬 처리를 통해 동시에 여러 트리를 구축하여 대용량 데이터셋에 대한 학습 시간을 크게 단축시킬 수 있다. 이 모델은 또한 누락된 값이나 다른 특이값을 자체적으로 처리할 수 있는 기능을 가지고 있어, 데이터 전처리 과정이 간소화된다. XGBoost는 그 성능을 더욱 향상시키기 위해 모델의 하이퍼파라미터를 최적화할 수 있다. 이러한 조정을 통해, XGBoost는 다양한 문제에 유연하게 적용할 수 있으며 높은 예측 성능을 보인다. XGBoost 모델은 Gradient Boosting 알고리즘을 확장한 모델로, 높은 예측 성능과 함께 병렬 처리 능력이 있어 대용량 데이터 처리에 적합하다. 이러한 이유로 XGBoost 모델은 고성능 모델을 필요로 하는 보안 관제 업무에서 유용하다.

모델 훈련에 앞서, 생성된 데이터를 학습 데이터와 테스트 데이터로 분리한다. 일반적으로 전체 데이터의 약 85%를 학습 데이터로, 나머지 15%를 테스트 데이터로 사용한다. XGBoost 모델의 훈련은 모두 지도 학습 방법을 사용한다. 지도 학습은 입력 데이터와 해당 레이블을 통해 모델이 학습하게 된다. 이 경우, 입력 데이터는 각 이벤트의 특성이며, 레이블은 이벤트의 위험도 및 정/오탐 분류, 판단된 위험도, 이상 행위 정보 등이다.

모델 구조와 하이퍼파라미터를 정의한 후 학습 데이터를 사용하여 모델을 훈련시킨다. 이 과정에서 모델은 최적의 분류 규칙을 학습한다. 마지막으로 테스트 데이터를 사용하여 모델의 성능을 평가한다. 이를 통해 모델의 일반화 성능을 확인한다. XGBoost 모델은 학습 과정에서 Gradient Boosting 알고리즘을 사용하여 오차를 최소화하는 방향으로 순차적으로 학습된다.

3.2 관제 지원 인텔리전스 설계

인공지능 기반 티켓 지원 시스템의 주요 목표는 보안 이벤트의 효과적인 분류 및 관리를 위해 AI를 활용하는 것이다. 시스템은 SOC 내에 위치하여 Offense 이벤트를 분류하고 위험도를 평가하는 데 필요한 학습 데이터를 수집하고 처리한다. 또한, 시스템은 중/고위험도를 나타내는 이벤트에 대해 처리결과를 토대로 분석 내용을 추천한다. 저 위험도의 이벤트에 대해서는 자동으로 티켓을 처리한다. 그리고 사용자의 이상 행위가 감지되면 대상자에게 자동으로 소명을 요청할 수 있어야 한다[8]. 이처럼 관제 지원 인텔리전스는 관제사에 의해 종료된 티켓을 대상으로 인공지능 기술을 활용하여 일정 주기마다 학습을 진행하고 Fig. 5의 흐름과 같이 티켓의 처리를 지원한다.

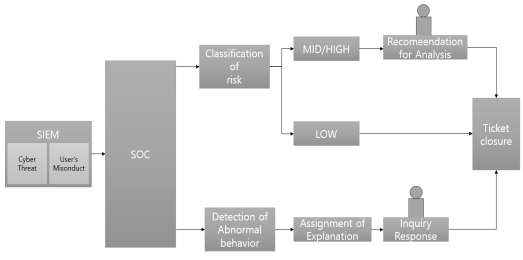

Fig. 5. System diagram

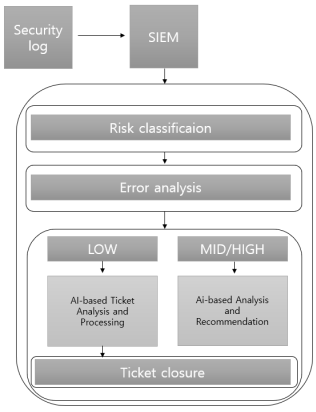

Fig. 6. Risk classification process

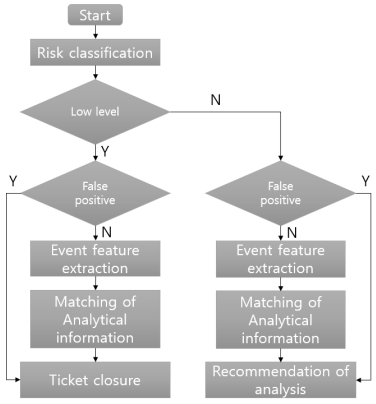

Fig. 7. False positive classification process

관제 티켓은 다양한 네트워크 장비로부터 생성되는 보안 로그를 기반으로 SIEM으로부터 Offense 이벤트가 발생하면 관제 지원 인텔리전스는 티켓의 분석을 위해 이를 우선 텍스트로 변환한다[9].

Fig. 6은 위의 과정을 더욱 상세하게 보여준다. 우선 관제 티켓의 위험도에 따라 분류된다. 이 분류는 인공지능 알고리즘에 의해 자동화되며 저위험도와 중/고위험도로 나뉘게 된다.

① 저위험도 티켓 : 이 경우에는 자동 분석이 수행된다. 인공지능 기반의 분석 도구를 활용하여 실시간으로 티켓을 분석하고 처리한다. 이런 방식으로 시스템은 다수의 저위험도 이슈를 효율적으로 처리할 수 있으며 이 과정을 거친 후에는 티켓이 종료된다.

② 중/고위험도 티켓 : 이 경우에는 분석 지원이 이루어진다. AI가 분석을 추천하여 사람이 이를 참조하여 결정을 내린다. 중요한 이슈에 대한 사람의 개입을 보장하면서도, AI가 제공하는 분석 내용 추천으로 신속한 의사결정을 지원한다.

시스템의 설계는 AI를 활용함으로써 대량의 로그 데이터를 신속하게 처리하고 보안 위협에 대응할 수 있다[10].

인공지능 기반의 관제 티켓 처리 시스템을 설계하고 Fig. 7과 같이 보안 로그 분석과 처리 과정을 자동화, 추천해주는 시스템의 상세한 작동 순서는 다음과 같다.

① 위험도 분류 : 이 단계에서 시스템은 보안 로그를 수집하고 이를 기반으로 관제 티켓을 생성한다. 그 다음으로 생성된 티켓을 인공지능 알고리즘을 사용하여 위험도에 따라 분류한다.

② 저위험도 분류 여부 판단 : 분류된 티켓이 저위험도인 경우, 오탐 여부를 판단한다.

저위험도 오탐 판정이 아닌 경우, 이벤트의 특성을 추출하고 분석 정보를 매칭한다. 그 후 분석 내용을 기입하고 관제 티켓을 종료한다. 저위험도 오탐 판정인 경우, 분석 없이 관제 티켓을 바로 종료한다.

③ 중/고위험도 분류 여부 판단 : 분류된 티켓이 중/고위험도인 경우, 오탐 여부를 판단한다.

중/고위험도 오탐 판정이 아닌 경우, 이벤트의 특성을 추출하고 분석 정보를 매칭한다. 그 후 인공지능은 분석 결과를 바탕으로 분석 내용을 추천한다. 중/고위험도 오탐 판정인 경우, 인공지능은 직접적인 분석 없이 분석 내용을 추천한다.

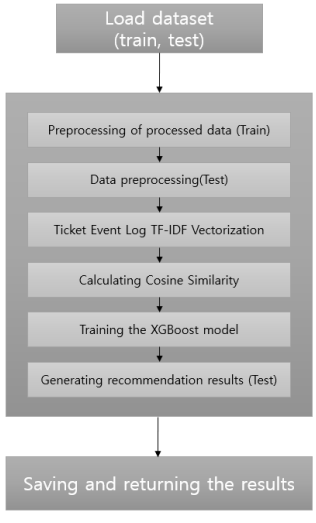

Fig. 8. Recommendation system process

이렇게 설계된 시스템은 관제 티켓의 처리를 최적화하고 보안 로그 분석 효율성을 크게 향상시킨다. 시스템은 대량의 데이터를 빠르게 처리하고 각 티켓의 위험도를 정확하게 판단한다. 적절한 처리 방안을 제시함으로써 보안 업무의 효율성이 증대된다.

종료된 티켓이 수신되면 SOC DB의 AI테이블에서 이를 저장한 후 탐지 룰 카테고리별로 분류된 카테고리에 따라 유사도를 측정한다. 그 후 인공지능 학습을 진행한다. Fig. 8과 같이 기술의 핵심은 문서 유사도 비교의 과정에 초점을 맞추고 있다[11]. 우선, 처리 결과에 대한 수집으로 시작하며 이후 탐지 룰 카테고리 안에서 모든 티켓의 처리 결과를 포함하여 학습을 진행한다. 학습이 시작하기에 앞서, 텍스트 전처리 과정을 통해 유효하지 않은 문자를 제거하고 텍스트를 정제한다. 이 단계에서는 종료된 관제 티켓의 데이터로부터 의미 있는 Feature(특징)를 추출한다. TF-IDF(Term Frequency-Inverse Document Frequency)의 방법을 사용하여 단어, 구, 문장 등의 피처를 추출한다. 피처 추출 후에는 유사도 측정이 이루어진다. 결과 해석 단계에서는 유사도 측정 결과를 해석한다. 이를 통해 종료된 관제 티켓의 유사성을 평가하고, 유사한 티켓을 식별하거나 비슷한 특징의 티켓의 처리 결과를 찾는 등의 활용이 가능하다. 관제 티켓 유사도 비교는 관제 티켓 카테고리 안에서부터 결과 해석까지의 여러 단계를 통해 이루어진다는 것을 확인할 수 있다. 이 과정을 통해 관제 티켓 유사성을 정확히 파악하고 분석하는 것이 가능하다.

3.3 관제 지원 인텔리전스 구현

위험도 분류는 관제사에 의해 분석 후 종료된 티켓을 토대로 학습한다. Fig. 9과 같이 티켓의 오펜스 이벤트 로그를 통해 해당 이벤트의 페이로드를 대상으로 티켓 ID별로 목록을 확인할 수 있으며 오른쪽에서 자세한 상세 로그와 각 위험도 레벨을 확인할 수 있다. 또한 전체 확인 시점의 분류 결과 통계를 확인할 수 있다.

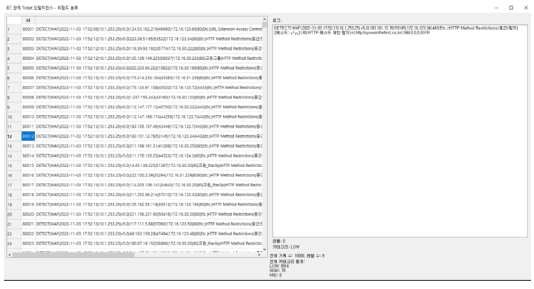

Fig. 9. Risk classification system

티켓의 오탐을 감지하기 위해 관제사에 의해 분석 후 종료된 티켓을 토대로 학습한다. Fig. 10과 같이 티켓의 오펜스 이벤트의 로그를 통해 해당 이벤트의 페이로드를 대상으로 티켓 ID별로 목록을 확인할 수 있다. 로그 창 하단에 분류가 'Y'로 표기된다면 관제 지원 인텔리전스에서 해당 티켓을 오탐으로 판단한 것이다.

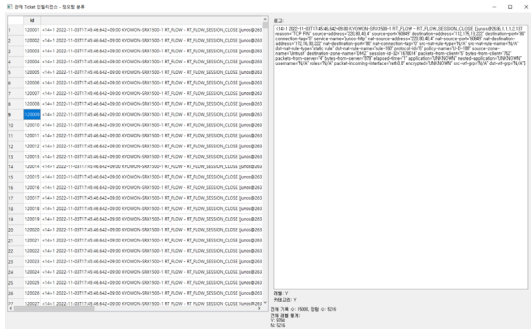

Fig. 10. False positive classification system

추천시스템은 종료된 티켓의 처리 결과를 토대로 분석 내용을 추천해준다. Fig. 11은 티켓의 ID 별로 해당 내용에 대해 세부적인 내용에 대해 우측 상단에서 추천 내용을 확인할 수 있다.

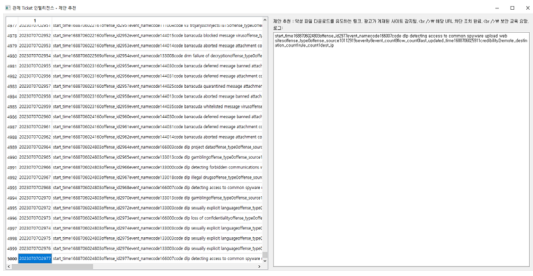

Fig. 11. Recommendation system

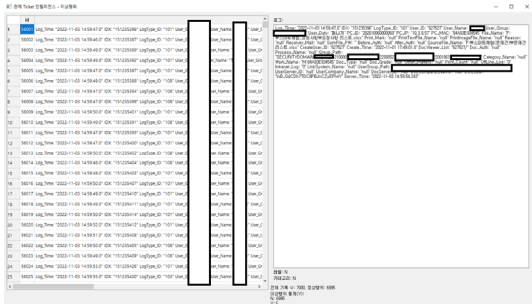

Fig. 12. Anomaly detection system

이상 행위 감지 시스템은 이전에 이상 행위로 판단하여 소명 요청에서 결재까지 프로세스가 완료된 티켓을 토대로 학습한다. Fig. 12와 같이 티켓의 ID 별로 이상 행위 여부의 확인이 가능하다. 이때 'Y'로 표기된다면 시스템이 이상 행위로 판단한 것이다.

4. 실험 평가

본 연구를 통해 개발된 관제 지원 인텔리전스를 실험하기 위한 실험 환경은 Table 1과 같이 CPU i7-12700K, RAM 64GB, Windows 10 Pro 운영체제를 이용하였다.

Table 1. Test environment

Item	Experiment environment
CPU	Intel(R) Core(TM) i7-12700K CPU @ 3.61GHz
RAM	64.0GB
System	64-bit operating system, x64-based processor
OS	Windows 10 Pro

실험에 사용된 데이터셋은 Table 2와 같다. 학습 데이터셋은 각 모듈을 평가하기 위해 다른 데이터셋을 활용하였다.

Table 2. Test Results of ticket based learning datasets

Items	results
Risk Classification Training Dataset	80,000
Risk Classification Test Dataset	10,000
False Positive Classification Training Dataset	120,000
False Positive Classification Test Dataset	15,000
Recommendation System Training Dataset	50,000
Recommendation System Test Dataset	5,000
Anomaly Behavior Training Dataset	56,000
Anomaly Behavior Test Dataset	7,000

학습을 모두 마친 후 테스트용 데이터셋을 활용하여 평가한 관제 지원 인텔리전스의 성능 결과는 Table 3과 같다.

Table 3. Performance test results

Test Items	Performance test results
Ticket risk classification	98%
Ticket false positive detection	≥ 100 times
Recommended analysis content of tickets	≥ 150 instances
Detection of abnormal user behavior	4 times out of 4

실험 결과, 위험도 분류 모듈은 98%, 오탐 분류 모듈은 100개 이상의 오탐이 올바르게 판단되었다. 추천 모듈은 150회 이상 올바른 추천 내용임을 확인하였다. 이상 행위 감지 모듈은 데이터셋에 지정된 4개 행위를 모두 발견하였다.

따라서 본 연구를 통해 개발된 관제 지원 인텔리전스의 성능은 관제 실무에 있어 유의미한 업무의 효율성 증대를 기대할 수 있었다. 또한 개별 티켓의 정보를 토대로 결과와 통계를 확인할 수 있는 것은 SOC에서의 편의성을 증대시킬 수 있다고 평가할 수 있다.

5. 결론

이 연구에서는 인공지능 기반 관제 업무지원 시스템의 설계 및 구현을 제시하였다. 이 시스템은 보안운영센터(SOC)의 효율성을 향상시키고, 보안담당자의 업무 부담을 줄이는 것을 목표로 하였다. 또한, 이 시스템은 공유가 가능한 위협 인텔리전스와 같이 보안운영센터의 외부에서 작동하도록 구성되어 있어 기업, 기관간 협의에 따라 각자의 보안운영센터 포털과 연동이 가능하도록 하는 것을 목표로 하였다. 데이터가 많이 수집할수록 성능이 향상되며 더 나아가 기존의 위협 인텔리전스 시스템과 달리 인공지능 기술을 활용하여 결과 판단을 보조하는 기능의 제공이 가능하다.

본 연구에서 구축된 시스템은 인공지능 기술이 보안 분야 중 특히 보안운영센터의 환경에서 어떻게 활용될 수 있는지에 대한 가능성을 보여주기 위해 SIEM에서 필연적으로 발생하는 많은 오탐(False positive)를 줄일 수 있도록 기존의 위협 인텔리전스 기능을 보완하여 인공지능 기술이 접목된 관제 지원 인텔리전스를 구현 및 설계하였다. 자동화된 처리의 기준이 되는 저위험도의 Offense 이벤트를 높은 정확도로 분류하였으며 오탐과 이상 행위를 감지하고 중/고위험도에 대해서는 기존 티

켓의 처리 결과를 토대로 추천까지 가능하였다. 앞으로의 연구에서는 AI 알고리즘의 세밀한 튜닝, 학습 데이터의 다양성 확보를 통해 시스템의 성능을 더욱 향상하는 방안을 모색할 계획이다. 이 연구가 SOC 환경에서의 인공지능 활용에 대한 새로운 통찰을 제공하고 보안 분야에서의 인공지능 기술 활용을 촉진하는 것에 도움이 될 수 있기를 바란다.

References

[1] An Jung Hyun, A Review of the Problems with AI-Based Security Control, *IITP*, 2021

[2] Eom Jin Guk, Proposal for a Breach Detection Method Using SIEM, *The Journal of The Institute of Internet, Broadcasting and Communication*, 2016

[3] Jeon Deuk Jo, Industrial Control System Security Control Model, *Journal of KII*, 2015

[4] Jang Sang Hyun, A Study on Factors Influencing the Introduction of Next-Generation AI-Based Security Control Systems Using AHP Technique, *Korean Society for IT Policy and Management*, 2022

[5] Lee Soo Young, A Study on the Use of Threat Data Intelligence for Advanced Security Control, *Master's Thesis, Dongguk University*, 2019

[6] Methodology for SOAR-based Internal Security Response Automation in SIEM Environment, M*aster's Thesis, Chung-Ang University*, 2022

[7] Kim Nam Gyun, Implementation of Security Information Management System for Real-time Abnormal Behavior Detection and Visualization, *Asia-Pacific Journal of Multimedia Services Convergent with Art, Humanities*, and Sociology, 2018

[8] Hwang Bo Hyeon Woo, Development of Anomaly Detection Algorithm Using Machine Learning, *The Journal of Society for e-Business Studies*, 2022

[9] Shin Ik Soo, Practical Feature Extraction Study for the Accuracy and Speed Improvement of Machine Learning-based IDS Security Event Classification Model, *Journal of The Korea Institute of Information Security & Cryptology*, 2018

[10] Lim Jong Hyuk, True/False Alarm Classification of IDPS Detection Data Based on Deep Learning, *Journal of Korea Information Security Society*, 2019

[11] Shin Sung Yoon, Text Classification Using LSTM-CNN, *The Journal of The Korean Institute of Communications and Information Sciences*, 2019

김 진 원(Jin-Won Kim) [정회원]

- 2021년 1월 ~ 현재 : ㈜코드원 기업부설 보안연구소 선임 연구원
- 2021년 2월 : 극동대학교 대학원 산업기술보안학과 (석사)
- 2021년 3월 ~ 현재 : 극동대학교 대학원 인공지능보안학과 (박사과정)

〈관심분야〉
정보보호, 보안관제, 인공지능보안

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 박사
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구위원
- 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
해킹보안, 국방보안, 인공지능보안

이 상 도(Sang-Do Lee) [정회원]

- 2005년 2월 : 성균관대 정보통신대학원 정보보호학과 (석사)
- 2018년 2월 : 숭실대 컴퓨터학과 (박사)
- 2021년 8월 ~ 현재 : 육군사관학교 컴퓨터과학과 조교수

〈관심분야〉
정보보호, 정보통신, 사이버전