AI 기반 IT-OT 융합 환경의 통합 보안 위협 분석에 관한 연구

송현석, 이준영*
한전KDN(주) 전력ICT기술원 전력보안기술부
{hyunseok.song.17, ljy.953386}@kdn.com

A Study on Integrated Security Threat Analysis in AI-Based IT-OT Convergence Environments

Hyun-Seok Song, Jun-Young Lee
KEPCO-KDN. Power ICT Technology Institute, Power Security R&D Team

요 약

IT(Information Technology)와 OT(Operational Technology)의 융합이 가속화됨에 따라 산업 제어 시스템(ICS) 및 스마트팩토리의 운영 효율성은 크게 향상되었으나, 복합적 사이버 위협이 증가하였다. 본 논문은 에이전트리스 방식으로 IT·OT 환경의 정형·비정형 데이터를 통합 수집하고, AI 기반 다차원 상관분석 모델을 통해 이벤트 간 연관성을 실시간 분석하여 융합형 공격을 조기에 탐지·경보하는 시스템을 제안한다. 시스템은 SSH·NetFlow 기반 데이터 수집부, 상관계수 기반 데이터 분석부, 학습·검증·배포를 지원하는 AI 모델 관리부, Hadoop/HiveQL 기반 분산 확장형 데이터베이스로 구성된다.

Ⅰ. 서 론

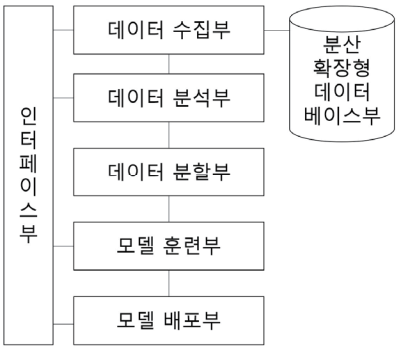
4차 산업혁명으로 IT와 OT의 경계가 사라지면서 제조·에너지·교통 분야에서 운영 효율성이 증대되었으나, IT 계정 탈취가 OT 제어 인프라로 전이되는 융합형 공격이 증가하였다.[1][2] 2022년 전 세계 OT 전문가 중 다수가 침해 경험을 보고했으며, ICS 시스템의 상당수에서 악성코드가 탐지되는 등 실질적 위협이 현실화되었다. 기존 보안관제 시스템은 IT 또는 OT 단일 영역에만 집중하여 복합 공격 탐지에 한계를 보인다. 본 연구는 이러한 문제를 해결하기 위해 AI 기반 통합 상관분석 시스템을 설계·구현하고, 그 구조와 핵심 기술을 분석한다.

Ⅱ. 본론

기존 SIEM(Security Information and Event Management) 연구는 단일 로그 유형의 상관분석에 초점을 두었다.[4] IT-OT 융합 보안 연구는 ICS 보안 가이드라인(NIST SP 800-82, IEC 62443) 및 융합 환경 위협 분석을 제안하였으나,[3] 실시간 다차원 상관분석을 통한 융합형 공격 탐지 기술은 부족하다. 최근 설명 가능한 상관분석 기반 이상탐지 연구가 제안되었으나, OT 환경 안정성을 저해하지 않는 에이전트리스 데이터 수집과 대규모 분산 아키텍처 적용 요구가 증가하고 있다.[5]

2.1 전체 구조

제안된 시스템은 [그림 1]과 같이 데이터 수집부, 데이터 분석부, AI 모델 관리부, 분산 확장형 데이터베이스부, 인터페이스부로 구성된다. Purdue 모델(Level 0-5) 전 계층에서 데이터를 수집하여 통합 분석한다.



[그림 1] IT-OT 통합 보안 이벤트 상관 분석 시스템 구성도

2.2 시스템 요약

구성 요소	주요 기능	기대 효과
데이터 수집부	• 에이전트리스 수집 • 정형·비정형 데이터 자동 정규화	OT 환경 안전성 유지 다양한 로그 연속 수집
데이터 분석부	• AI 기반 다차원 상관계수 계산 • 논리·시간적 인과관계 추론	융합형 공격 패턴 실시간 식별 복합 위협 탐지 강화
AI 모델 관리부	• 학습/검증/테스트 데이터 분할 • 머신러닝·딥러닝 모델 훈련·배포	지속 학습·업데이트 탐지 정확도 개선
분산 데이터베이스	• Hadoop/HiveQL 기반 저장 • Auto-scaling, 백업, 복제	대규모 이벤트 처리 고가용성·확장성 보장
인터페이스부	• REST API, 표준 프로토콜 연동 • 경보 및 분석 결과 상위 시스템 전달	외부 SIEM/SOAR 연계 통합 대시보드 구축

[표 1] 시스템의 구성 요소별 주요 기능과 기대효과

2.3 데이터 수집부

IT 인프라(서버, 네트워크 장비 등)와 OT 설비(PLC, SCADA 등)로부터 로그, 네트워크 트래픽, 성능 정보, 운전 데이터 등 다양한 형태의 데이터를 실시간으로 수집한다. 특히, 운영 안정성이 최우선인 OT 환경에 미치는 영향을 최소화하기 위해 별도의 에이전트 설치가 필요 없는 비에이전트(Agentless) 방식을 채택한다. SSH, NetFlow 등 표준 프로토콜을 활용하여 원격으로 안전하게 데이터를 수집하며, 수집된 이기종 데이터를 AI 모델이 학습 가능한 형태로 가공하고 표준화하는 자동 정규화 기능을 수행한다.

2.4 데이터 분석부

시스템의 핵심 두뇌 역할을 수행한다. 정규화된 데이터를 바탕으로 AI 기반 다차원 상관 분석을 수행하여 서로 다른 이벤트 간의 연관도와 위협 패턴을 식별한다. IT 이벤트(e_i)와 OT 이벤트(e_j) 간의 상관계수(p_{ij})는 공분산과 표준편차를 이용하여 계산되며, 이를 통해 논리적, 시간적 인과관계를 추론한다.

$$\rho_{ij} = \frac{Cov(e_i, e_j)}{\sigma_{e_i}\,\sigma_{e_j}}$$

또한, 정상 행위 패턴을 학습한 모델을 기반으로 이상 징후를 탐지하고, 위협의 심각도를 평가하여 위협 점수(Threat Score)를 산출한다. 이 점수가 사전에 정의된 임계치를 초과할 경우, 관리자에게 즉시 경보를 전달하는 조기 경보 기능을 수행한다.

위협 점수 수식은 CVSS의 기본 점수 계산 방식과 유사하게 여러 평가 항목을 정규화 및 가중 합산한 뒤 비선형 보정 단계를 추가하여 점수를 산출하도록 하였다.

평가 요소	설명	점수/가중치
영향 범위(IS)	• IT 단일 영역 • IT-OT 융합 영역 • OT 제어 시스템 직접 영향	1-3 / 4-6 / 7-10
공격 복잡도(AC)	• 단일 이벤트 공격 • 다단계 연계 공격 • 지속형 APT 공격	1-3 / 4-6 / 7-10
자산 중요도(AsC)	• 일반 IT 자산 • 핵심 인프라 자산 • 안전 제어 시스템	1-3 / 4-7 / 8-10
신뢰도 (CL)	• 높은 신뢰도(>90%) • 중간 신뢰도(70-9%) • 낮은 신뢰도(<70%)	1.0 / 0.8 / 0.6
상관분석 강도 계수 (CF)	• 이벤트 간 상관계수 절댓값 평균 + 1	0.5-2.0

[표 2] 위협 심각도 점수 산출

위협 점수 계산식 :

$$TS = \frac{(IS + AC + AsC) \times CL}{3} \times CF$$

알림 단계	TS 범위	알림 수준
Low Alert	• TS < 3.0	정보성
Medium Alert	• 3.0 ≤ TS < 6.0	주의
High Alert	• 6.0 ≤ TS < 8.0	위험
Critical Alert	• TS ≥ 8.0	긴급

[표 3] 위협 알림 수준 임계치

2.5 AI 모델 관리부

데이터 분할부는 분석된 데이터를 AI 모델 구축에 필요한 학습용, 검증용, 테스트용 데이터로 분할한다. 모델 훈련부는 이 데이터를 활용하여 침입 탐지, 이상 탐지, 위협 예측 등 목적에 맞는 머신러닝 및 딥러닝 모델을 훈련시킨다. 학습이 완료된 모델은 모델 배포부를 통해 실제 운영 환경에 배포되어 실시간 위협 감지 및 분석에 활용된다. 이 과정은 지속적인 피드백을 통해 모델의 성능을 개선하는 순환 구조를 가진다.

2.6 분산 데이터베이스 및 인터페이스

대규모 산업 환경에서 발생하는 방대한 양의 데이터를 효율적으로 처리하기 위해 Hadoop/HiveQL 기반의 분산 확산형 데이터베이스를 사용한다. 이는 데이터 양과 네트워크 규모 증가에 따라 유연하게 자동 확장(Auto-scaling)이 가능하다. 인터페이스부는 표준 API를 통해 외부 위협 관리 시스템과의 연동을 지원하여 분석 결과 및 경보를 상위 시스템으로 전달하는 역할을 한다.

Ⅲ. 결론

본 시스템은 이기종 데이터의 통합 수집, AI 기반의 자동 정규화 및 다차원 상관 분석, 그리고 확장 가능한 아키텍처를 통해 기존 보안 시스템의 한계를 극복하고, 지능적인 융합형 위협에 효과적으로 대응할 수 있는 방안을 제시한다. 특히 NIST SP 800-82와 IEC 62443 표준을 준수하면서도 실제 산업 현장의 요구사항을 반영한 실용적인 접근법을 채택하고 있다. 이를 통해 산업 현장의 시스템 안정성과 가용성을 보장하고, 나아가 안전한 디지털 전환을 뒷받침하는 핵심적인 보안 인프라로 기능할 수 있을 것이다.

향후 연구로는 탐지된 위협에 대한 대응 시나리오를 자동화하는 SOAR(Security Orchestration, Automation and Response) 기술과의 연계, 그리고 설명 가능한 AI(XAI)를 적용하여 분석 결과의 신뢰도를 높이는 방안에 대한 심도 있는 고찰이 필요할 것이다. 또한 MITRE ATT&CK for ICS 프레임워크와의 연동을 통한 위협 인텔리전스 강화 및 양자 내성 암호화 기술 적용을 통한 차세대 보안 위협에 대비한 연구도 중요한 과제가 될 것이다.

참 고 문 헌

[1] Maleh, Y., et al., "IT/OT convergence and cyber security," Computer Fraud & Security, 2021.

[2] Bhamare, D., et al., "Cybersecurity for industrial control systems: A survey," Computers & Security, Vol. 89, 2020.

[3] Stouffer, K., Falco, J., & Scarfone, K., "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Rev. 2, 2015.

[4] Wu, Q., Ferebee, D., Lin, Y., & Dasgupta, D., "Monitoring security events using integrated Correlation-based techniques," ACM International Conference Proceeding Series, 2009.

[5] Birihanu, E., & Lendák, I., "Explainable correlation-based anomaly detection for Industrial Control Systems," Frontiers in Artificial Intelligence, 2025.