AI 기반 로그 파싱과 풀 클론 가상머신 격리 환경을 활용한 ICS 보안 점검 시스템

오다희, 송현석, 이준영*
한전KDN 전력ICT기술원 전력보안기술부
{5_dahee_k, hyunseok.song.17, *ljy.953386}@kdn.com

ICS Security Audit System Using AI-based Log Parsing and Full Clone Virtual Machine Isolation

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

요 약

본 논문은 보안점검 환경에서의 독립성과 재현성 확보를 위해 풀 클론(Full clone) 기반 가상머신 복제·관리 시스템을 설계하고, 스냅샷 프로비넌스(provenance)와 AI 머신러닝 로그 자동 파싱, 위협 자동 탐지를 통합한 오케스트레이션(Orchestration)을 제안한다. 제안 시스템은 사전 정의 이미지, 라이브 마이그레이션, 스냅샷을 결합하여 점검용 가상머신(VM)을 신속하게 생성한다. 세션의 시작, 중간, 종료 시점의 스냅샷을 생성하고, 각 로그 배치에 해시값과 메타데이터를 부여하여 출처 기반의 데이터 수집 체계를 구현한다. 다기종 장비 로그는 머신러닝 기반의 파서를 통해 정규화하며, 위협 탐지는 시계열, 연관 분석, 그래프 기반 보안 위협 행위 맥락을 포착하고, 로그 배치에 부여된 해시값과 메타데이터를 사용하여 신뢰성을 보정한다. 점검 결과 송신 후 자동 폐기, 자원 반환까지 운영 자동화를 구현한다. 제안 시스템은 표준화된 베이스라인(사전 정의 이미지), 격리된 재현 환경(풀 클론), 증거 수집(스냅샷 프로비넌스)의 결합을 통해, 이기종 OT/IT 환경에서 재현 가능하고 확장 가능하며 운영자 친화적인 보안 점검을 제공한다.

Ⅰ. 서 론

최근 OT 및 IT 환경의 융합이 가속화되면서 산업제어시스템(ICS) 및 OT 인프라 보안에 대한 관심이 급증하고 있다. 또한 다양한 제조 및 공정 장비에서 생성되는 방대한 로그 데이터를 효과적으로 통합·분석하는 것이 보안 위협 대응의 핵심 과제로 대두되고 있다. 데이터 통합 분석 능력은 대응 속도 및 위협 식별 정확도와 직결된다. 반면 ICS 시스템의 특성상 실시간 연속 운영 및 안정성, 엄격한 규제 준수, 전통적인 폐쇄망 구조의 유지가 핵심적 과제로 남아있다. 클라우드 기반의 빅데이터 분석, AI 로그 파싱, 자동 위협 탐지 등 차세대 보안 기술은 IT·공공·금융 분야에서 성과를 내고 있으나, ICS의 경직된 네트워크 환경에서는 직접 적용이 쉽지 않다.

본 연구는 ICS 및 OT 환경의 본질적인 보안·운영 요구를 훼손하지 않으면서, 자동화, 확장성, 실시간 분석이라는 최신 보안 관리 니즈를 만족시키고자 한다. 특히, 운영망의 영향을 최소화하는 클라우드 Full Clone 복제 기반의 격리 점검 환경을 도입해, 로그 파싱 및 AI 위협 탐지 자동화 체계를 제안한다. 이 접근법은 최근 국제 산업 표준화 단체 및 실제 산업 현장에서도 하이브리드·엣지-클라우드 모델과 더불어 점진적으로 논의가 되기 시작했다는 점에서, 기술 및 정책성 실효성을 갖추었다.[2]

Ⅱ. 본론

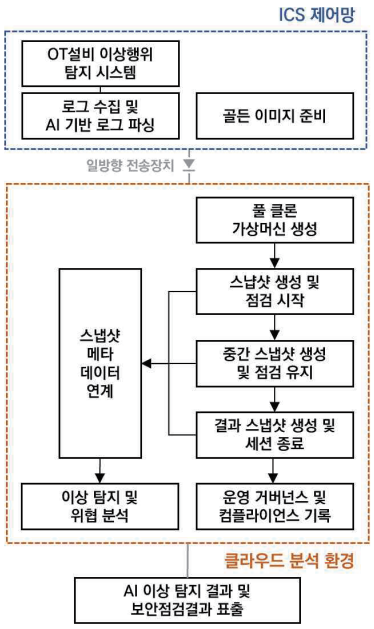
2.1 관련 연구 및 한계

ICS 보안 연구는 장기간 폐쇄망 환경, 실시간 통제, 규제 준수를 전제로 한 온프레미스 위주의 방식이 표준으로 자리 잡아왔다. 그러나 최근에는 글로벌 제조기업을 중심으로 제어 시스템의 실시간 처리는 엣지단에서 수행하고, 보안 점검·데이터 분석·모니터링 등은 클라우드에서 수행하는 하이브리드 모델을 점차 도입하고 있다. 특히 NIST SP 800-82, IEC 62443 등 국제 표준 문서에서도 운영망과 실시간 제어 계층을 물리적으로 분리한 상태에서 점검·분석·사전 검증 환경을 클라우드 또는 엣지로 이관하는 시나리오를 제시하고 있으며, 이를 위한 컴플라이언스 및 아키텍처 가이드라인을 제공하고 있다. 하지만 실제 적용 단계에서는 현장 환경의 다양성, 데이터 전송 및 보안 우려, 복제 환경 유지 비용 등 여러 현실적인 문제가 존재한다. 따라서 완전한 클라우드 전환이 아닌 운영과 무관한 복제 점검 환경의 클라우드 활용이 주요 전략으로 대두되고 있으며, 정책적 요구사항으로는 폐쇄망 본선과의 직·간접 연결 차단, 전용선 및 망분리 구조, 보안 게이트웨이 구축, 데이터 보호 및 암호화 전송 그리고 강력한 접근 통제 체계 마련 등을 필수 요건으로 상정하고 있다. 국내에서도 스마트팩토리 보안 가이드라인과 같은 정책적 대응이 병행되고 있다.[1][3]

2.2 시스템 아키텍처 및 구현

본 연구에서 제안하는 보안 점검 시스템의 핵심은 운영 중인 ICS환경의 이미지를 풀클론 방식으로 격리 환경에서 복제·운용하는 데 있다. 우선, 점검 및 복제에 필요한 운영체제와 보안 설정을 반영해 골든 이미지(Golden Image)를 구축한다. 폐쇄된 제어망에서 추출된 로그와 골든 이미지는 '일방향 전송장치(Data Diode)'를 통해 클라우드 분석 환경으로 안전하게 전송된다. 이 장치는 물리적 전송 경로를 단방향으로 제한하며, 운영망으로의 역방향 통신과 외부 공격 및 정보 누출을 효과적으로 차단한다. 외부 환경에서는 직접적인 접속 또는 데이터 역유출이 불가능하여, 제어시스템 로그, 이상행위 탐지 이벤트, 골든 이미지 등의 정보만을 안전하게 클라우드 분석 환경으로 송출할 수 있다.[2][4]

클라우드 분석 환경에서는 전달받은 골든 이미지를 기반으로 풀클론 VM을 생성하고, 수집된 로그와 현장 상태 정보를 해당 VM 내 점검 세션에 매핑한다. VM은 운영 환경과 논리적으로 완전히 분리된 하이퍼바이저 내에서 생성되며, VM 단위로 전용 네트워크·스토리지 리소스가 할당된다. 이로써 점검 및 위협 분석 과정이 원본 운영망과 데이터, 서비스에 실질적인 영향을 미치지 않고 수행될 수 있다. 점검 시작, 중간, 종료 시점에서 VM 상태 스냅샷을 생성하며, 각 스냅샷에는 고유 해시, 메타데이터(생성시간, 정책 정보 등)을 부여해 로그 및 이벤트와 연계한다. AI 이상 탐지 및 분석 엔진이 정규화된 로그, 스냅샷 데이터, 현장 이벤트를 종합적으로 분석하여 이상행위를 탐지한다. 이상행위 탐지 결과, 취약점 점검 리포트, 스냅샷 연계 데이터 등이 실시간 대시보드, 알림 시스템 등을 통해 사용자에게 직관적으로 전달된다. 필요한 경우 점검결과를 폐쇄망인 업무 환경으로 안전하게 보낼 수 있도록 일방향 데이터 송출 등 연계도 가능하다.[5]



<그림 1> ICS 보안 점검 시스템 동작 순서

모 듈	설 명
골든 이미지 및 풀 관리 모듈 (Golden Image & Pool Manager)	표준 보안 설정, OS 패치, 점검/에이전트의 사전 설치된 골든 이미지를 정기적으로 자동 갱신·서명 검증하여 VM 생성을 관리
풀 클론 VM 오케스트레이터 (Clone Orchestrator)	점검 시작 전에 운영 환경의 현재 상태를 기반으로 VM을 생성한다. 리소스 할당, 네트워크 격리, 스냅샷 스케줄, 폐기 등 전 과정 자동화
네트워크 격리 모듈 (Network Isolation)	일방향 전송장치, Vlan, 방화벽 규칙 등으로 통신 경로를 엄격히 제한
스냅샷 및 프로비넌스 관리 (Snapshot & Provenance Manger)	점검 세션 시작, 중간, 종료 등 체크포인트에서 스냅샷을 생성하며 운영 상태를 고정 저장, 각 스냅샷에는 고유 ID, 해시, 정책 버전, 자산 태그 등 메타데이터를 자동 첨부하고 시스템 로그와 맞춤형 OT 태그에 동기화
로그 파싱 엔진 (Log Parsing Engine)	최적화된 ML 파서로 이기종 로그를 정규화 및 구조화
위협 탐지 및 분석 모듈 (Threat Detection & Analysis)	정규화된 로그와 이상행위 탐지 시스템을 통해 AI엔진으로 이상행위/위협을 탐지하며, 모든 탐지 결과에 provenace(스냅샷 메타데이터)와 설명 가능 경로 자동 첨부
운영 거버넌스 및 규정 준수 (Governace/Compliance Layer)	점검, 데이터 송출, 접근 통제에 대해 국제 표준에 맞춘 컴플라이언스 정책을 적용, Audit로 로그와 정책 변경 이력을 자동 기록 및 관리
보안 결과 전송 모듈 (Secure Result Dispatcher)	분석 결과는 암호화 후 클라우드 또는 일방향 전송장치 경유 후 업무 환경으로 전송

<표 1> ICS 보안 점검 시스템 모듈

Ⅲ. 결론

본 논문은 폐쇄망 운영이 필수인 ICS 환경에서, 최근 산업계·학계에서 제한적으로 논의되는 클라우드 Full Clone 복제 기반 자동화 보안 점검 체계의 특징 및 한계를 분석하고 새로운 ICS 보안 점검 프레임워크를 제안하였다. 해당 프레임워크는 운영망과 완전히 격리된 점검 복제 환경에서 AI 기반 로그 파싱 및 위협 탐지 자동화를 수행하는 구조로서, ICS의 폐쇄망 운영 철학과 최신 산업 표준 및 규제 요구사항과도 부합하도록 제안하였다. 그러나 현재까지 제안 시스템은 실험 환경에서의 검증이나 현장 적용을 통한 성능 평가가 이루어지지 않았다. 따라서 성능, 확장성, 운영 안정성 및 실제 ICS 현장과의 호환성에 대한 엄격한 실증적 검증이 필요한 상황이다. 시뮬레이션, 산업 현장의 대규모 로그 데이터를 활용한 성능 평가, 그리고 국내외 표준과의 지속적 정합성 검증 및 컴플라이언스 준수 여부에 대한 중점적인 연구가 후속 과제로 남아 있다.

향후 연구는 다음과 같은 방향으로 추진될 예정이다. 첫째, ICS 점검 복제 환경의 실시간 가용성 유지 및 위협 탐지 정확도 검증을 위한 통합 테스트베드 구축 및 운영, 둘째, 파서 드리프트 감지와 자동 폴백, 보안 정책 거버넌스 체계의 효과성 평가, 마지막으로 본 시스템의 실무 적용을 위한 규제기관 및 산업계와의 협력 기반 마련과 검증 절차 표준화가 포함된다. 본 연구는 ICS 환경에 적합한 클라우드 Full Clone 점검 프레임워크의 가능성과 설계 원칙을 제시했으나, 이를 뒷받침할 충분한 실증 자료 확보와 검증이 요구되는 초기 연구 단계임을 명시한다. 특히 본 시스템의 검증을 위해서는 실증 테스트베드가 필수적이나, 가용성을 최우선으로 하는 ICS 제어시스템의 특성상 실제 환경에서의 검증에는 많은 제약이 존재한다. 제안 시스템이 실효성 있는 솔루션이 되기 위해서는 통제된 환경에서의 체계적인 실증 실험과 단계적 현장 검증이 필수적이며, 특히 ICS 환경의 핵심 요구사항인 가용성과 보안성을 동시에 만족하는 결과를 도출하는 것이 중요하다. 이를 통해 제안 프레임워크의 효과성과 산업계적용 가능성을 입증하는 후속 연구가 필요할 것이다.[4][6]

참 고 문 헌

[1] P. Ackerman, Industrial Cybersecurity, 3rd ed. Wiley, 2023.

[2] Ed Moyle and Joshua Franklin, Hybrid Cloud Security: Practical Architectural Approaches, Apress, 2024.

[3] C. J. Brooks and P. A. Craig Jr., Practical Industrial Cyber Security: ICS, Industry 4.0 & IIoT, Wiley, 2024.

[4] Matthew Portnoy, Virtualization Essentials, Updated Edition, Wiley, 2024.

[5] Kartik Gopalan, Applied Artificial Intelligence for Cybersecurity: Detect Threats and Protect Systems, Packt Publishing, 2023.

[6] Brian Smith, Enterprise Virtualization Essentials, Wiley, 2024.