SOAR 오케스트레이션 기반 제로트러스트 성숙도 진단 자동화 프레임워크

서정우[1], 서진우[1], 공나영[1], 송민희[1], 박기웅[2]
[1]세종대학교 정보보호학과 학부생
[2]세종대학교 정보보호학과 교수
seojw329@naver.com, jinu2956@sju.ac.kr, username040@sju.ac.kr,
23011716@sju.ac.kr, woongbak@sejong.ac.kr

SOAR-Based Zero Trust Maturity Automated Assessment Framework

Jeong-Woo Seo[1], Jin-Woo Seo[1], Na-Young Kong[1], Minhee Song[1], Ki-Woong Park[2]
[1,2]Dept. of Computer and information Security, Sejong University

요 약

본 논문은 기존 제로트러스트 성숙도 진단의 한계를 해결하기 위해 SOAR(Security Orchestration, Automation and Response) 오케스트레이션 기반 자동화 프레임워크를 제안한다. 제안 프레임워크는 데이터 입력, SOAR 오케스트레이션, 성숙도 진단, 결과 출력의 4개 모듈로 구성되며, 오픈소스 보안 도구 API 자동 호출을 통해 실제 운영 환경의 증적 데이터를 수집하고 성숙도 등급을 진단한다. 또한 조직 환경을 고려한 목표 단계 설정과 단계별 개선 방안을 제안하여 조직의 제로트러스트 단계적 도입을 실질적으로 지원한다.

1. 서론

디지털 전환과 클라우드 환경의 확산으로 기업 내외부 경계가 무너지면서 전통적인 경계 기반 보안 모델의 한계가 명확해지고 있다. 내부자 공격, 계정 탈취, 권한 오남용 위협이 증가함에 따라 "Never Trust, Always Verify" 원칙에 기반한 제로트러스트 보안 모델이 차세대 패러다임으로 주목받고 있다.

국내에서는 KISA가 2024년 제로트러스트 가이드라인 2.0을 발간하여 6개 핵심 필러에 대한 체크리스트 항목 및 4단계 성숙도 모델을 제시하였다[1]. 그러나 현행 성숙도 진단은 보안 전문가의 수동 체크리스트 작성과 인터뷰에 의존하여, 많은 공수 소모, 판정 일관성 부족, 기업별 환경 미반영이라는 구조적 한계를 가진다[2]. 이로 인해 기업은 현재 보안 수준을 객관적으로 파악하기 어렵고, 반복적인 상시 진단이 사실상 불가능한 실정이다.

본 논문에서는 이러한 한계를 극복하기 위해 SOAR(Security Orchestration, Automation and Response) 오케스트레이션을 기반으로 기업 환경 정보 수집부터 성숙도 점수 산출, 개선 로드맵 제공까지의 과정을 자동화하는 프레임워크를 제안한다.

2. 관련 연구

2.1. 제로트러스트 성숙도 진단 연구

제로트러스트 아키텍처의 도입 수준을 평가하기 위한 성숙도 모델 연구가 국내외에서 진행되어왔다. NIST SP 800-207은 제로트러스트의 국제 표준으로 최소 권한 원칙과 지속적 검증을 핵심으로 제시하였으며[3], CISA ZTMM 2.0은 5개 영역에 걸쳐 4단계 성숙도 프레임워크를 구체화하였다[4]. 국내에서는 KISA가 이를 기반으로 6개 핵심 영역과 4단계 성숙도 모델을 제시한 가이드라인 2.0을 발간하였다[1].

그러나 이러한 표준은 개념 정립과 도입 전략 제시에 초점이 맞춰져 있어, 체크리스트 항목을 실제 데이터로부터 측정 가능한 형태로 변환하거나 자동화된 진단 파이프라인을 구현한 연구는 미흡하다[2].

2.2 SOAR 기술 및 활용

SOAR는 이기종 보안 도구를 통합 오케스트레이션하여 반복적 보안 작업을 자동화하는 플랫폼으로, Playbook 기반 워크플로우와 REST API 연동을 통해 보안 운영의 일관성과 효율성을 높인다[5]. 기존 연구들은 주로 악성코드 분석, 취약점 스캐닝 등 침

해 대응 시나리오에 SOAR를 적용하는 데 집중하였으며[6][7], 성숙도 진단이나 컴플라이언스 평가 영역에의 활용은 매우 제한적이다.

본 연구는 SOAR의 오케스트레이션 역량을 제로트러스트 성숙도 진단에 적용함으로써 이러한 간극을 채우고자 한다.

3. 제안하는 프레임워크

3.1. 전체 시스템 구조

본 연구에서 제안하는 프레임워크는 (그림 1)과 같이 데이터 입력 모듈, SOAR 오케스트레이션 모듈, 성숙도 진단 모듈, 결과 출력 모듈의 4개 모듈로 구성된다.

데이터 입력 모듈은 사전 설문조사를 통해 수집된 기업 환경 정보를 기반으로 구성된다. 각 체크리스트 항목은 증적 데이터의 특성에 따라 자동·반자동·수동 진단으로 사전 분류되며 설문조사를 통해 수집된 기업 환경 정보와 매핑되어 스프레드시트에 정리된다. 자동 진단이 가능한 항목은 스프레드시트를 JSON 형식으로 변환하여 SOAR 오케스트레이션 모듈로 전달되며 반자동 및 수동 진단 항목은 진단 담당자가 스프레드시트에 직접 입력한다.

SOAR 오케스트레이션 모듈은 진단 요청을 수신하여 각 보안 도구의 API를 자동으로 호출하고 증적 데이터를 수집하는 핵심 모듈이다. 상세 구조는 3.2절에서 기술한다.

성숙도 진단 모듈은 SOAR 오케스트레이션 모듈로부터 전달받은 증적 데이터를 KISA 제로트러스트 가이드라인 2.0 기준으로 검증하고 성숙도 점수를 산출한다. 각 체크리스트 항목을 True/False로 판정하고 영역별 가중 평균을 적용하여 기존, 초기, 향상, 최적화의 4단계 성숙도 등급을 결정한다.

결과 출력 모듈은 성숙도 진단 모듈에서 산출된 결과를 영역별 성숙도, 종합 성숙도, 목표 달성도, 개선 사항을 포함한 진단 결과 데이터를 리포트로 생성하고 웹 대시보드를 통해 시각화한다. 또한 실제 조직의 환경을 고려한 목표 단계 설정, 목표 달성을 위한 개선 과제 도출, 과제 이행을 위한 단계별 로드맵 수립을 지원함으로써 조직이 제로트러스트를 단계적으로 도입할 수 있도록 한다.

3.2. SOAR 오케스트레이션 모듈 구조

SOAR 오케스트레이션 모듈은 본 프레임워크의 핵심으로, 그림 1과 같이 영역별 진단 Playbook, 제어 엔진(Control Engine), 실행 엔진(Execution Engine)으로 구성된다.

3.2.1. 영역별 진단 Playbook

영역별 진단 Playbook은 SOAR 오케스트레이션 모듈의 실행 청사진으로, 진단 영역별로 설계된 워크플로우이다. 각 Playbook은 세 가지 구성 요소를 포함한다.

실행 조건은 해당 Playbook이 실행되는 조건을 의미한다. 진단 요청에 포함된 진단 영역 정보를 기반으로 어떤 Playbook을 실행할지 결정하며, 진단 범위와 환경 설정에 따라 실행 여부가 결정된다.

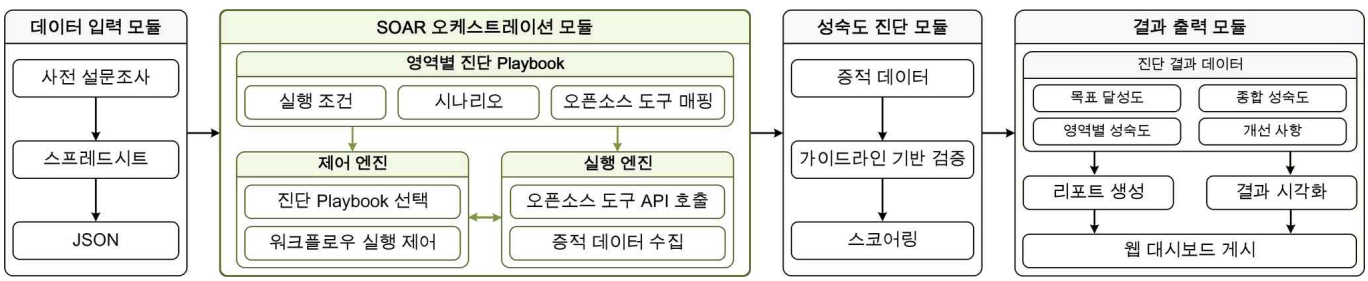
시나리오는 Playbook 내 작업의 실행 순서와 흐름을 의미한다. 인증 토큰 발급, API 호출, 증적 데이터 수집의 순서와 각 단계 간 의존 관계가 시나리오에 명시된다. 이를 통해 제어 엔진은 시나리오에 따라 일관된 워크플로우를 실행할 수 있다.

오픈소스 도구 매핑은 체크리스트 항목과 연동 보안 도구 간의 매핑 정보를 의미한다. 각 체크리스트 항목별로 호출할 보안 도구와 API 엔드포인트를 사전에 명시함으로써, 실행 엔진이 올바른 도구를 호출할 수 있도록 한다.

3.2.2. 제어 엔진(Control Engine)

제어 엔진은 진단 워크플로우의 흐름을 제어하는 엔진으로, 두 가지 핵심 기능을 수행한다.

진단 Playbook 선택은 데이터 입력 모듈로부터 전달된 진단 요청을 파싱하여 진단 영역에 맞는 Playbook을 선택하고 워크플로우 인스턴스를 생성하는 기능이다. 진단 요청에는 진단 대상 식별자, 진



(그림 1) Proposed Framework

단 영역 범위, 가중치 설정 등의 정보가 포함되며, 이를 기반으로 해당되는 영역의 Playbook이 선택된다. 진단 영역이 확장될 경우, 새로운 Playbook을 추가하는 방식으로 유연하게 대응 한다.

워크플로우 실행 제어는 선택된 Playbook의 시나리오에 정의된 실행 순서를 기반으로 각 노드의 수행을 제어하고 노드 간 데이터 흐름을 관리하는 기능이다. 예를 들어 인증 토큰 발급 노드에서 생성된 결과값은 이후 API 호출 노드의 인증 헤더에 자동으로 전달되며, 각 노드는 이전 단계의 결과를 반영한 순차적 실행 구조를 형성한다. 이와 같은 구조를 통해 워크플로우 전반에 걸쳐 일관된 인증 컨텍스트가 유지된다.

3.2.3. 실행 엔진(Excution Engine)

오픈소스 도구 API 호출은 Playbook의 오픈소스 도구 매핑 정보를 참조하여 각 보안 도구의 REST API를 실제로 호출하는 기능이다. 각 API 호출 시 제어 엔진으로부터 전달 받은 인증 토큰이 Authorization 헤더에 자동으로 주입되어 연속적인 API 호출이 가능하다. 또한 독립적으로 실행 가능한 항목은 병렬로 처리하여 전체 진단 소요 시간을 단축하며, 네트워크 오류 발생 시 재시도 및 타임아웃 처리를 통해 안정적인 동작을 보장한다.

증적 데이터 수집은 각 보안 도구로부터 수신한 API 응답 데이터를 원형 그대로 수집하여 성숙도 진단 모듈로 전달하는 기능이다. 수집된 진단 결과 데이터는 성숙도 진단 모듈로 전달되며, 판정 결과에 대한 근거 추적과 향후 재판정 시 동일한 증적 데이터로 활용이 가능하다.

4. 결론 및 향후 연구

본 논문에서는 제로트러스트 가이드라인 2.0 기반 성숙도 진단의 한계를 해결하기 위해 SOAR 오케스트레이션을 활용한 자동화 프레임워크를 제안하였다. 기존 성숙도 평가는 수작업 중심으로 수행되어 평가자의 주관이 개입될 가능성이 높고, 동일 기준에 대한 반복 적용이 어려워 결과의 일관성이 저하되며, 실제 운영 환경 데이터를 충분히 반영하지 못하는 한계를 가진다.

제안하는 프레임워크는 Playbook 기반 워크플로우를 통해 진단 절차를 표준화하고, API 연계를 통해 다양한 보안 도구로부터 증적 데이터를 자동 수집하여 평가에 반영한다. 이를 통해 동일한 조건에서 일관된 진단 수행이 가능하며, 데이터 기반 판단을 통해 기존 수작업 중심 평가의 한계를 보완한다. 또한 자동·반자동·수동 진단 구조를 병행함으로써 현실적인 평가 환경과 확장성을 동시에 확보한다.

향후 연구에서는 진단 범위 확장과 함께 제안하는 프레임워크를 실제로 구현하고, 해당 프레임워크의 실현 가능성을 입증한다. 또한, 머신러닝 기반 분석 및 컴플라이언스 프레임워크 연계를 통해 실용성을 더욱 고도화한다.

Acknowlegement

[2]교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC) (Project No. ,10% IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431 30%)의 지원을 받아 수행된 연구임.

참고문헌

[1] 한국인터넷진흥원(KISA), "제로트러스트 가이드라인 2.0," 2024.

[2] Wendler, R., "The maturity of maturity model research: A systematic mapping study" Information and Software Technology, vol. 54, no. 12, pp. 1317-1339, 2012.

[3] NIST, "Zero Trust Architecture," Special Publication 800-207, 2020.

[4] CISA, "Zero Trust Maturity Model," Version 2.0, 2023.

[5] Gartner, "Market Guide for Security Orchestration, Automation and Response Solutions," 2023.

[6] Z. T. Sworna, M. Ali Babar, and A. Sreekumar, "IRP2API: Automated Mapping of Cyber Security Incident Response Plan to Security Tools' APIs," Proc. IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Taipa, Macao, 2023, pp. 546-557.

[7] 대한민국 등록특허, "제로트러스트 기반의 보안 모델 도입을 위한 보안 컨설팅 방법, 장치 및 컴퓨터-판독 가능 기록 매체," 특허번호 1020240124377 2024.