Chapter
04

사이버 보안 오케스트레이션 및 자동 대응 기술

김태은_한국인터넷진흥원 책임연구원

I. 결과물 개요

개발목표시기	2024. 12.	기술성숙도 (TRL)	개발 전	개발 후
			4	6
결과물 형태	SW-System, SW-Platform	검증방법	자체검증, 시험인증	
Keywords	보안 관제, 인공지능, 빅데이터, 자동화, 위협 분석 Security Monitoring, Artificial Intelligence, Big data, Automation, Threat analysis			
외부기술요소	Open Source 사용, License 이용	권리성	특허, SW, 설계도	

II. 기술의 개념 및 내용

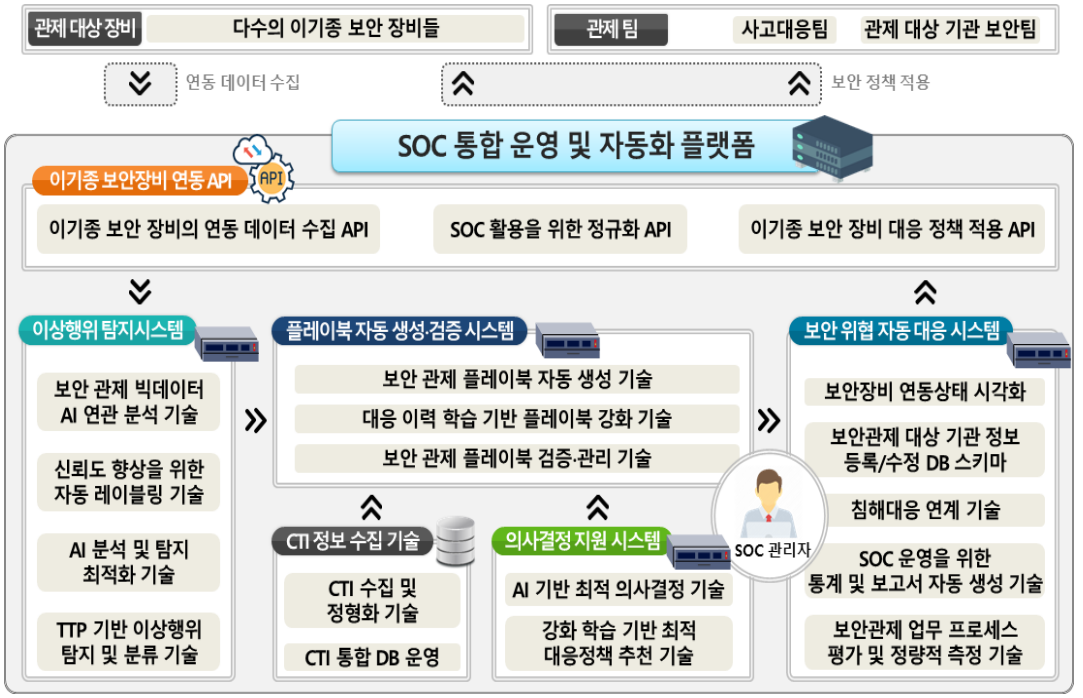
➢ 보안관제센터의 탐지 - 위협분석 - 대응 全업무 프로세스를 자동화하는 보안관제 오케스트레이션 및 대응 자동화 기술

- (연동 · 탐지) 이기종 보안 장비 연동 API(공개) 및 이상행위 탐지 기술
- (위협분석 · 자동화) 빅데이터 기반 전주기적 사이버 보안관제 업무 프로세스를 위한 시나리오(플레이북) 생성 및 자동화 기술
- (의사결정) 보안관제센터에 특화된 AI 기반 보안사고 대응 의사결정 지원 및 판단 기술

* 본 내용은 김태은 책임연구원(☎ 061-820-1273, tekim31@kisa.or.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함



[그림 1] 기술개념도

- (대응) 이기종 보안 장비의 보안사고 자동 대응 기술
- (실증) 보안관제센터 대상 보안관제 오케스트레이션 및 대응 자동화 기술 실증

III. 국내외 기술 동향 및 경쟁력

1. 기술의 특성 및 성능

➢ 보안관제센터에서 로그 수집을 위해 연동되는 다양한 이기종 보안 장비 연동을 위한 API 제공

- 보안관제 빅데이터를 기반으로 한 전 주기적 사이버 보안관제 업무 프로세스 자동화
- 보안관제 이력 데이터 등의 빅데이터를 활용한 특화된 보안사고 대응 의사결정 지원
- 이기종 보안 장비의 보안사고 자동 대응

2. 경쟁기술/대체기술 동향 및 현황

➢ 국내 보안 오케스트레이션 및 자동 대응 솔루션 관련 기관·기업 현황

[표 1] 국내 솔루션 주요 현황

No.	기관·기업명	솔루션명	특장점/주요 내용
1	안랩	Ahnlab Sefinity AIR	- 다양한 솔루션과의 연동으로 오케스트레이션 개념을 업무에 도입 가능 - 표준화된 플레이북 및 자유로운 편집 기능 제공
2	시큐레이어	eyeCloudSOAR	- SIEM과 보안 오케스트레이션 자동화 및 대응 보안 운영관리와 결합 - AI 탐지 모델을 통한 Cyber Kill Chain, KISA 위협분석, ATT&CK 분석 - 데이터 수집에서 대응까지 자동화하는 사용자 정의 가능한 프로세스 구축
3	이글루시큐리티	SpiDERTM	- 지도 학습에 의한 경보 이벤트 사고 처리 자동화 - 비지도 학습에 의한 알려지지 않은 위협 탐지 - 국내외 위협정보 및 악성코드 최근 자료 수집
4	삼성 SDS	STORM AI for Web	- 삼성 SDS의 축적된 보안관제 노하우를 바탕으로 한 지도 학습과 비지도 학습을 종합하여 탐지율 고도화 - 공격 현황을 웹 구조 형태로 시각화
5	제이슨	JMACHINE SIEM	- 보안관제 전문가가 식별 불가한 Unknown 이상 징후를 AI 기술로 탐지 - 다양한 보안 데이터를 AI가 종합 분석
6	SK Infosec	Secudium MSS	- 국내 1위 보안관제 노하우 - 업계 최다 전문 보안관제 및 침해사고 대응 인력 보유 - 보안솔루션 통합 관리
7	Logpresso	통합보안관제	- 실시간 이벤트 연관분석과 배치 연관분석을 지원하는 유일한 단일 플랫폼 - 비지도 학습 머신러닝 모델을 통한 이상 징후 탐지 지원 - 위협 발생 시 보안 팀에 자동 티켓 할당, 위협분석내역 기록, 결재 프로세스 지원 - KISA C-TAS, 금융보안원 FCTI, 시큐디움 인텔리전스를 연동한 분석 및 탐지 지원

3. 우수성 및 차별성

경쟁기술	본 기술의 우수성/차별성
Ahnlab Sefinity AIR, SpiDERTM 등	- 국내외 이기종 보안장비의 연동(API) - AI·보안관제 빅데이터를 활용한 업무 자동화 및 의사결정 지원

4. 관련 보유특허

➢ 기술 개발 후, 기술이전 시 해당 기술의 특허 공개

Ⅳ. 국내외 시장 동향 및 전망

1. 국내외 시장 동향 및 전망

➢ (국외) 세계 보안 오케스트레이션 자동 대응 기술(SOAR) 시장은 2021년 11.6억 달러(한화 1.2조 원)에서 2027년 27.7억 달러(한화 3조 원)로, 연평균 15.6% 성장할 것으로 전망되고 있음(Markets and Markets, 2019.)

➢ (국내) 우리나라 · 말레이시아 · 싱가포르 보안 오케스트레이션 자동 대응 기술(SOAR) 시장은 2021년 0.9억 달러(한화 957억 원)에서 2027년 2.6억 달러(한화 2,914억 원)로, 연평균 20.4% 성장할 것으로 전망(Markets and Markets, 2019.)

구분	2021년	2025년	2027년
세계 시장 규모	11.6억 달러	20.71억 달러	27.68억 달러
한국 시장 규모 (말레이시아, 싱가포르 포함)	8,700만 달러	1.83억 달러	2.65억 달러

2. 제품화 및 활용 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
보안관제 고도화	- (정책적 활용) 국가CERT의 침해사고 대응을 위한 분석 · 대응 환경의 자동화 및 중 · 소기업의 사이버공격 대응을 위한 관제 서비스 지원 - (공공 · 민간 활용) 사이버 침해사고 공동대응 업무협약을 맺은 유관기관 등 보안관제센터를 운영하는 기관을 통한 기술 실증 및 보급 · 확산을 통한 기술 활용

V. 기대효과

1. 기술도입으로 인한 경제적 효과

➢ 연구·개발 완료 후, 정책적 기술 보급·활용 단계에서 기술개발 참여기업 및 기술이전 기업의 사업 참여 확대를 통해 보안 산업육성이 기대

➢ 본 과제의 경쟁 분야인 사이버 보안 관제 오케스트레이션 및 자동 대응 시장에서, 연구결과물을 활용한 선도적인 기술을 기반으로 세계 보안관제 시장에서 약 3,000억 규모의 경제적 파급효과 창출이 기대

- 2022년에 이르면 보안관제 서비스 시장이 43억 4,000만 달러(약 5조 2,000억 원)에 달할 것으로 전망되며, 약 6% 시장을 점유할 경우 약 3,000억 원의 시장 창출이 가능할 것으로 기대(프로스트 앤 설리번 참조)

2. 기술사업화로 인한 파급효과

➢ 공공 보안관제, 연구기관, 산업계의 연구·개발 협업을 통한 순환 구조[수요자 기술 요구 → 연구·개발 → 실증 → 상용화] 기반의 국가 기술 경쟁력 확보가 기대

➢ AI 기반 이상행위 탐지 기술, 보안관제 전 업무 프로세스 자동화 연구결과의 상용화로 국가 인프라 보안을 위한 보안관제센터 핵심기술 국산화에 기여할 것으로 기대

➢ 수 천만 건의 사이버 위협정보의 실시간 판별 및 보안관제 운영 자동화를 이루어 기존 인력 기반 체계에서 AI 시스템 기반의 신 정보보호 시장 개척이 기대

➢ AI·빅데이터 기반으로 신·변종 이상행위 공격에 대해 신속·정확하게 대응이 가능하여 선제적으로 사이버위협을 예방하는 선순환 효과가 기대