1등급 GOOD Software

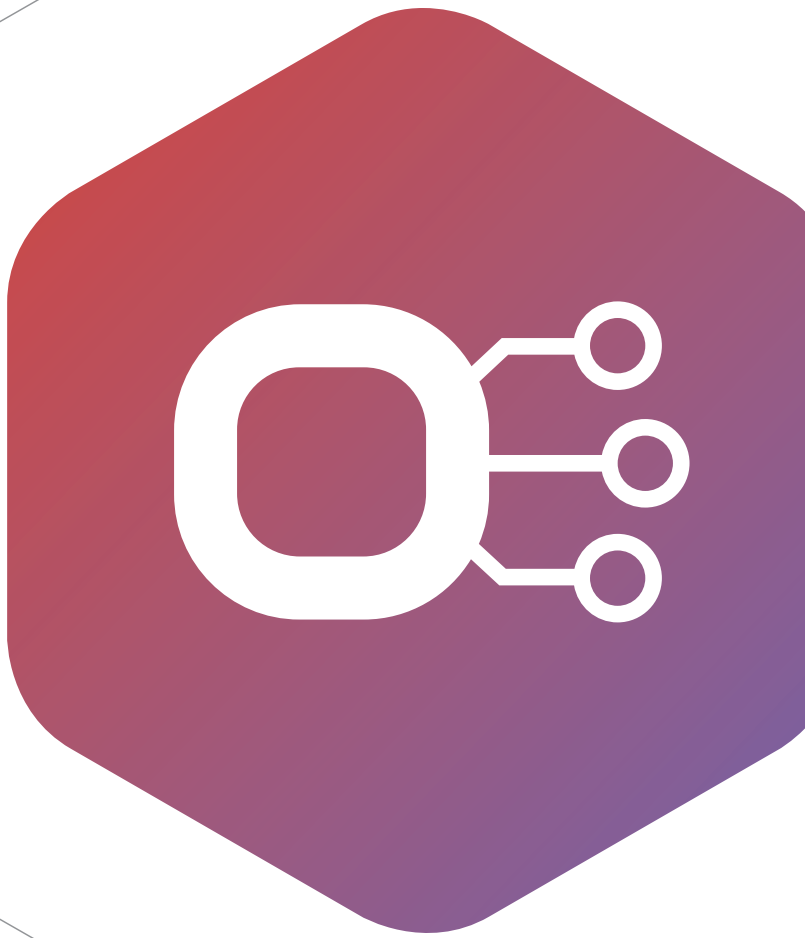
디지털서비스몰

한국기계전기전자시험연구원

SECURE ORCHESTRA

AI Driven SOAR

AI 기반 통합 보안 관리 플랫폼



SECURE SYSTEMS
beyond your security

SECURE ORCHESTRA

Secure Orchestra는 30년간 축적된 보안전문가의 침해사고 대응 실무 노하우를 기반으로 개발한 제품으로 보안위협 탐지부터 분석, 대응까지 모든 과정을 자동화하여 보안 운영과 위협 대응 효율성을 극대화한 **AI 기반 통합 보안 관리 플랫폼** 입니다.

SOAR (Security Orchestration Automation & Response)는

끊임없이 쏟아지는 보안 이벤트와 다수의 보안 솔루션, 전문인력 및 기술 부족으로 인한 문제를 해결합니다. 매일 수동으로 수행해야 하는 단순 반복적인 업무를 표준화 및 자동화하여 보안관리 효율을 극대화하고 보안 전문가들은 중요한 업무에 집중할 수 있습니다.

기존 보안관리	
대응 지연	수동 작업으로 대응 속도 저하
인력 부족	보안 담당자의 단순·반복 작업 과다
가시성 부족	다수 솔루션 데이터 분석, 통합 곤란
보안수준 저하	우선순위 관리 및 중요 위협 대응 곤란

SOAR 보안관리	
신속 대응	자동화된 대응과 신속한 의사 결정
인력 효율화	전문 인력의 중요 업무 위주 투입
가시성 확보	가시성 확보로 데이터 통합 분석
보안수준 향상	우선순위에 따른 자동 대응과 집중

Secure Orchestra 특장점

플레이북 기반의 빠른 자동 대응

- 업계 최다 수준의 플레이북 제공
- 국가 주도 위협그룹(APT그룹) 대응 최적화 플레이북 제공

AI 정오탐 분석 엔진(AI CERT)

- CERT의 완벽한 전처리를 거친 학습데이터 사용
- 인공지능 모델러 경량화로 적은 리소스 사용

위협 인텔리전스(TI) 서비스

- KISA C-TAS 연동
- NCSC KCTI 정보 수집
- 자체 봇 기반 전세계 위협 및 평판정보 수집

ASM으로 자산 가시성 확보

- 불법 시스템 탐지 및 차단
- Trust 정보자산 서비스 변화 관리
- Shodan 취약점 스캔
- 서비스 포트 스캐너 제공

다차원 분석으로 고도화된 탐지

- N차 상관분석 및 프로파일 분석
- N차 DPI 시그니처 탐지 분석
- N차 위협 인텔리전스 분석
- N차 인공지능 분석

초고속 수집·저장 및 검색

- 수집 340만/680만eps(공인시험성적서 기준)
- 검색 21억건 /0.001초
- DB to DB, Server to Server, Agent/Agentless 등 다양한 방식으로 로그 수집

최고의 자율 연동생태계를 지원하는 Playbook

시큐어오케스트라 Playbook은 **CERT의 침해사고 대응 절차를 4단계로 축약하여 설정**하고 자동 대응을 지원합니다.

이벤트 발생!
Playbook Start

01 IOC 설정

- 기탐지된 이벤트, 프로파일 이벤트, 상관관계 이벤트와 연계된 동적 대응 설정
- 플레이북 자체에서 자유로운 탐지 정책 설정 후 동적 대응 연계

02 분석 설정

- 1단계에서 탐지된 이벤트 위협분석
- TI분석(Virus Total, IBM Xforce, 소만사, ESTsecurity, KCTI, CTAS, Native TI 등)
- AI분석(AI R1, R2, R3, RLLM 등)
- DPI분석(탐지시그니처)

03 경고 설정

- 다양한 경고 방식 설정(GUI, Telegram, SMS, E-mail 등)

04 대응 설정

- 국내외 다양한 솔루션과 차단 API 설정
- SIRP를 통한 티켓처리시스템 설정
- PB Workflow 분석 대응 처리 로깅

* 5~6분 소요

* 시큐어오케스트라 플레이북 4단계 설정 화면

EASY

손쉬운 워크플로우 셋업

- 마우스 Drag & Drop 으로 워크플로우 이지 셋업
- 사용자 설정에 대한 워크플로우 검증 시뮬레이션

6,800 +

업계 최다 수준의 플레이북

- 사전 정의 플레이북 6800건 이상
- 국가 배후 해커그룹(Kimsuky, Lazarus 등) 대응 플레이북 100건 이상

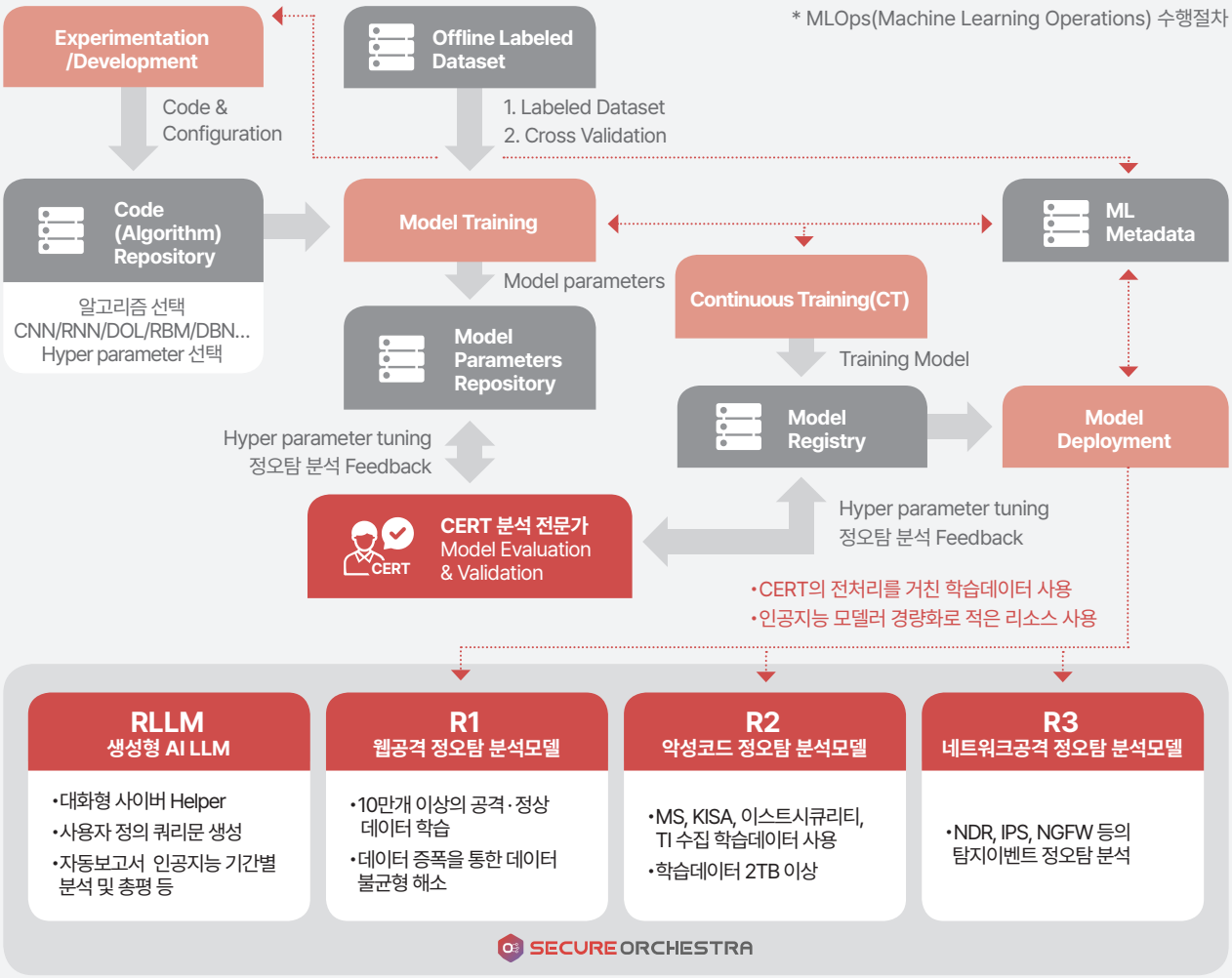
AI

AI 기반 분석 및 이상행위 탐지

- 온톨로지, MITRE ATT&CK 공격 Matrix 분석 및 AI 유사도 분석
- AI 기반 유사 해킹 워크플로우 추론 정책 추천

인공지능 정오탐 분석 엔진 AI CERT (Computer Emergency Response Team)

시큐어오케스트라는 **지속적으로 인공지능 정오탐 분석 모델러 R의 개발 및 업그레이드**를 지원하는 분석 중심의 통합 보안 관리 플랫폼입니다.(Model Orchestration)



해커가 접근할 수 있는 공격면 관리 ASM

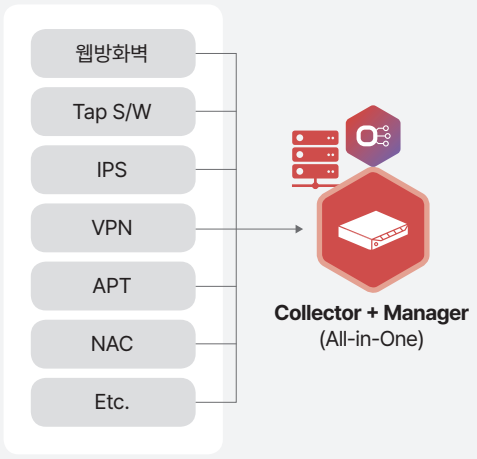
ASM(Attack Surface Management, 공격 표면 관리)는 악의적인 행위자의 무단 액세스 수단으로 악용될 수 있는 디지털 자산과 취약점으로 구성된 조직의 공격 표면을 모니터링 및 관리하는 프로세스로 사이버 위협에 대한 **가시성 확보 방안**입니다.

ASM 기능

- 네트워크 토폴로지 자동 생성 및 삭제
- 자산 서비스 상태 점검, 온오프 추적
- 자산 증감 변동 시 경고
- 식별되지 않은 자산의 식별 및 경고
- Playbook을 연동한 비식별자산 자동 차단
- Shodan 취약점 점검 및 추적
- 포트스캐닝 기능
- 주요시스템 선택 관리
- 자산별 서비스 포트 추적 보고서 추출

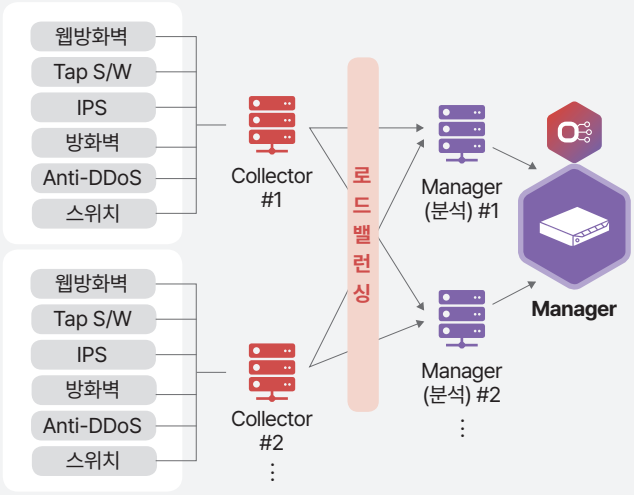
All-in-One Single Mode / Multi Load Balancing Mode

단일 구성 올인원 싱글모드



1 대의 시스템에 All-in-One 구성 기본 제공

다중 및 계층 구성 멀티 로드 밸런싱 모드



대용량 이벤트 분산, 단위 또는 부문 노드 구축을 위한 다중 계층구조 지원

* 멀티 로드 밸런싱 모드는 고객 환경에 따라 컨설팅 후 구성

주요 기능

사용자 정의 자동화 보고서
- 시간대별, 일간, 주간, 월간, 기간별 정기 보고서
- 보고서 생성 스케줄 지정 및 E-Mail 발송

정규화 파싱 분류
- 이기종 이벤트 정규화 기능
- 비정형 데이터의 정형화 작업을 보다 쉽게 활용 가능

다양한 시각화 기능
- 11종의 시각화 기능 제공(3D/2D)
- 위젯, 프리셋 지정 및 자동 넘김 기능

3D 멀티 대시보드
- 사이버보안 기상도
- 사용자 정의 위젯, 자동 화면 전환

초고속 모니터링
- 1 Index의 21억 건의 데이터당 0.001초 소요
- NoSQL 기반

실시간 종합 모니터링
- 실시간 이벤트 조회를 통한 실시간 모니터링 지원
- 침해사고 분석에 필요한 다양한 Tool 제공

Cyber Kill Chain
- 공격이벤트의 사이버 킬체인 분류 및 스펙트럼 분석
- 사이버 킬체인 모니터링

MITRE ATT&CK
- 공격이벤트의 MITRE ATT&CK 분석
- 조직의 보안 태세 파악 지원

모바일 지원
- 이동 매체를 통한 긴급대응 Smart Mobiliance
- 반응형 웹 UI 지원

My Page
- 사용자별 / 그룹별 열람 권한 부여 및 My Page 제공
- 계정별, 메뉴별 설정을 통해 열람 권한 조정

Hyper NMS
- NMS 모듈 기본 제공
- Alive Check 다중설정으로 정확도 향상

프로파일링 연관분석
- 프로파일링 기반 상호연관분석
- 출발지 IP, 출발지 Port 등의 통계정보 및 Criminal Mind 기반 상호 연관된 이벤트 정보 탐지

자체 취약성 점검
- ISMS 기반 자체 취약성 점검 엔진
- SOAR 시스템의 취약점을 자동 또는 수동으로 점검

정오탐 자동분석 보고서
- 2차 정오탐 자동분석보고서 생성
- 생성된 보고서 관리자 전달 및 수정·삭제

시큐어시스템즈 SOC (Security Operations Center)

시큐어시스템즈 SOC는 시큐어오케스트라를 실제 운영에 사용하며 보안관제 기술 노하우를 시큐어오케스트라 주요 기능에 적극 반영하고 있습니다.

효율이 좋은 보안 시스템을 만드는 사람들

시큐어시스템즈

사이버 보안, 그 효율성의 장벽 너머까지
시큐어시스템즈가 함께 하겠습니다

회사명	주식회사 시큐어시스템즈
설립일	2019년 5월 14일
대표이사	손 동 식
사업분야	솔루션 개발, SOC서비스

SECURE ORCHESTRA

AI 기반의 SOAR시스템

보안 워크플로우와 프로세스를 자동화하여 외부 침입 및 위협에 대응하고 분석결과를 제공함으로써 Security Orchestration의 도구화 지원

SECURE Mail Trainer

악성메일 모의훈련 시스템

APT공격, DBD(Drive by download)공격, Phishing 공격을 E-mail을 통해서 Attack Simulation 해주는 Cyber Range 솔루션

SECURE CTF

모의해킹 훈련장 시스템

네트워크/시스템/응용프로그램 영역에서 보안 취약점, 암호화에 관련된 문제로 팀 또는 개인의 역량을 수련하는 시스템

SECURE MSS 24×365

보안관제 서비스 24×365

보안장비, 네트워크장비, 서버 등의 원격 보안관제 서비스

SECURE PLAYER

BAS(Breach & Attack Simulator)

해킹공격 및 악성코드 트래픽을 발생시켜 Security Hole을 탐지

ALYac XDR

XDR Powered by SECURE ORCHESTRA

알약EDR + 시큐어오케스트라 통합 개방형 XDR Platform

SECURE SYSTEMS
beyond your security

서울특별시 강동구 고덕비즈밸리로 2가길 67(고덕동 휴네시온 타워) 7층
Tel. 1833-9195 | E-mail. support@securesystems.co.kr
www.securesystems.co.kr