SOAR

▸ 사용자 정의 플레이북 구성 및 보안장비 연동 컴포넌트 보유

- GUI 기반 사용자 정의 플레이북 구성 등 관리 기능 제공
- 사용자가 직접 제작해서 사용할 수 있는 플레이북 컴포넌트 통합 개발 환경(IDE) 지원
- 국내 최다 보안장비 정책 연동 컴포넌트 보유

▸ 위협 이벤트 정보의 사용자 정의 온톨로지화 관리

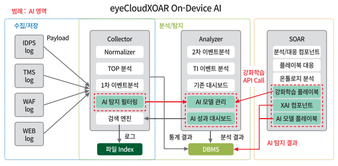
- 온톨로지-노드 관리 : Ticket(위협이벤트)에 대한 주요 Feature(위협정보지표)를 사용자정의에 따른 관리, 시각화 분석 및 플레이북 구동 시 연계/분석/통계 지표 정보로 활용

▸ 글로벌 표준 위협정보 분류 체계 적용 자동화

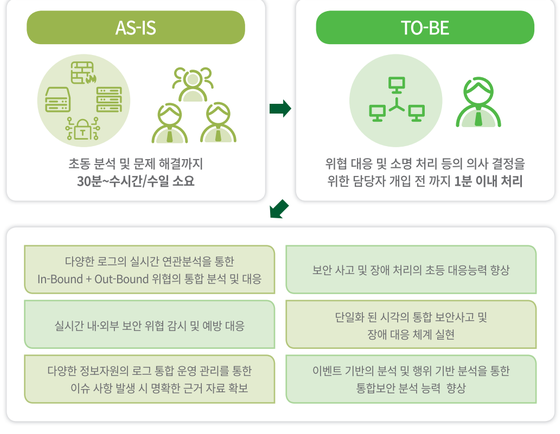
- 글로벌 표준 위협정보 분류 체계인 MITRE ATT&CK Matrix 정보 자동 수집 및 관리
- MITRE ATT&CK Navigator 모니터링 : 위협 이벤트 탐지 시 MITRE ATT&CK Attack ID와 매핑하여 공격 흐름의 시뮬레이션과 방어 기술을 제시하는 실시간 모니터링

▸ AI의 손 쉬운 사용을 통해 수 없이 많은 이벤트를 더욱 정확하게 분석

- 별도 학습이 필요 없는 On-Device 형태의 AI 제공 (추가 옵션, 업데이트 별도 제공)
- 풍부한 데이터를 통해 학습된 검증된 AI
- 다양한 컴포넌트 조합으로 복잡한 분석 및 대응 프로세스 구성
- AI의 판단 과정까지 투명하게 이해할 수 있는 XAI



도입효과



SecuLayer

본사 서울시 성동구 성수일로 4길 25 서울숲코오롱디지털타워 14F
대전지사 대전광역시 유성구 죽동로297번길 83, 대울빌딩 3층
대구지사 대구광역시 동구 팔공로 241 태왕아너스타워 104호(봉무동)
광주지사 광주광역시 북구 첨단과기로208번길 43-22, 첨단와이어스파크 A동 1012호

TEL. 1800-6713
FAX. 02-499-7605
구매문의. contact@seculayer.com
기술문의. tech@seculayer.com

시큐레이어가 제공하는

차세대 보안관리 시스템

eyeCloudXOAR

통합보안 분석 및 대응 솔루션

eyeCloudAI
인공지능 분석 솔루션

eyeCloudSIM
통합 로그관리 솔루션

다양한 위협을 정확하게 분석하고 신속하게 대응합니다

SecuLayer

eyeCloudXOAR

통합보안 분석 및 대응 솔루션

GS인증 1등급

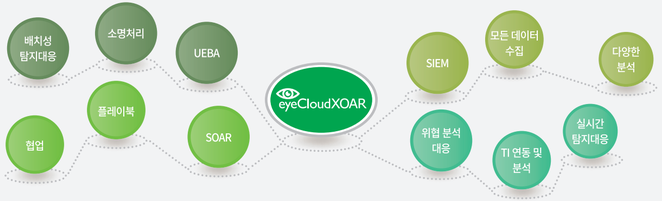
CC인증 EAL2

관련 특허
누적 38개 보유

조달청 디지털서비스몰

통합 로그관리 솔루션 ‘아이클라우드심’ | **통합보안 분석 및 대응 솔루션 ‘아이클라우드쏘아’** | 인공지능 분석 솔루션 ‘아이클라우드에이아이’

eyeCloudXOAR는 빅데이터 처리 플랫폼을 기반으로 데이터 수집부터 보안위협 분석, 대응까지 플레이북을 통한 자동화 업무 프로세스를 정의하여 보안관제 업무효율을 향상시키는 All-in-One 통합보안 분석 및 대응 솔루션입니다.



특장점

성능과 기능

클러스터링, MITRE ATT&CK 등 최신 기술 적용

- 독보적인 제조사 자체 클러스터링 기술을 통한 데이터 분산 처리, 동기화 및 밸런싱
- 국내 최고 성능의 공인 시험성적서 보유
- MITRE ATT&CK Matrix 기반 Navigator, 온톨로지 노드 관리, 실시간 보안장비 정책 적용 및 모니터, 플레이북 관리 등 최신 기술 적용
- 머신러닝 기반 분석, 알려지지 않은 이상행위 탐지로 분석의 정확도 제고

유연성

제한없는 DATA 수집과 ON-DEMAND 분석

- 분석 대상이나 방식에 제한이 없는 하이브리드 분석 도구 (자체 개발 Query Browser)
- Agent 및 Agentless방식을 통한 모든 대상의 로그 수집과 타 시스템 연계를 위한 eyeCloud API 제공
- 맞춤형 소명처리 프로세스를 통한 업무 생산성 향상

확장성

안전성이 확보된 컴포넌트 형식의 플랫폼 확장

- 수직 구성 : SIEM+UEBA+SOAR 통합 플랫폼으로 확장성 제공
- 수평 구성 : Scale-Out을 통한 무한 확장 가능
- 국내에서 가장 많은 보안장비 정책 연동 및 컴포넌트 제공
- On-device AI 컴포넌트 보유

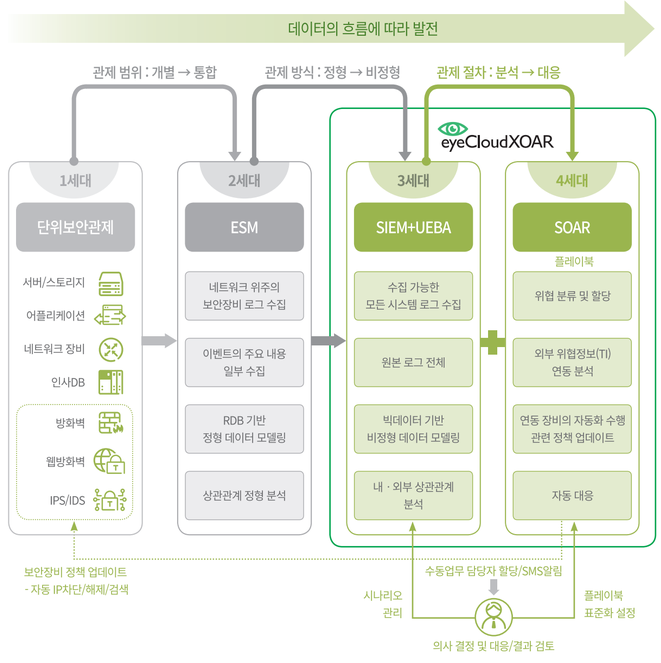
검증된 솔루션

국내 최다 레퍼런스 및 KNOW-HOW 보유

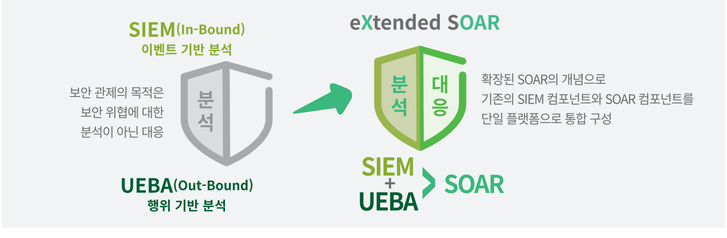
- 국내 최대 실시간 데이터 처리 레퍼런스 (국가정보자원관리원, 38TB/일)
- 공공, 국방, 금융, Cloud 등 국내 최다 레퍼런스 보유

보안관제 패러다임의 변화

▸ **세대별 보안관제시스템의 명칭**



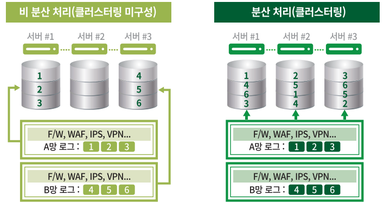
▸ **XOAR(eXtended SOAR)**



SIEM

▸ **다수 서버 운영 효율 최대화를 통한 빠른 성능과 안정성**

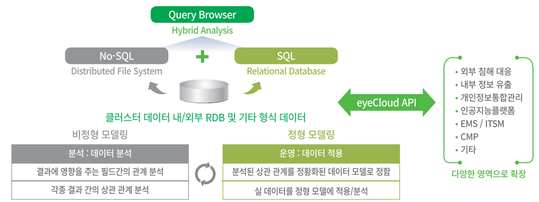
- 최초 제품 출시부터 다수 서버의 운영 효율 최대화를 위한 데이터 클러스터링 기반 독보적인 자체 분산 처리 기술 적용



▸ **공인된 국내 최초 단일서버의 초고속 빅데이터 처리 및 검색 성능**

▸ **어떠한 데이터라도 필요에 따라 하나의 도구를 통하여 일관되고, 정확하게 분석(On-Demand)**

- 분석 대상이나 방식에 제한이 없는 하이브리드 분석 도구(Query Browser)



UEBA

▸ **고급 분석을 통한 분석의 정확도 제고**

- 머신러닝 기반 분석을 통한 알려지지 않은 이상행위 탐지 (온디바이스 AI 컴포넌트)
- 사용자 및 개체의 행위에 대한 프로파일링 분석을 통한 선제 대응
- 행위 기반 위험 지수화에 따른 개인/그룹별 위험 관리

▸ **내재화된 지식 기반 콘텐츠를 통한 완성도 보장**

- 600+ 사이트에서 축적된 콘텐츠 내재화를 통한 검증된 Know-How 제공 (표준 시나리오 및 소명처리 플레이북)
- 표준 콘텐츠 맵 및 워크북을 통한 전반 업무 프로세스 통합 관리

▸ **맞춤형 소명 처리 프로세스를 통한 업무 자동화**

- 다양한 컴포넌트 및 사용자 제작 컴포넌트를 통한 소명처리 프로세스의 유연성 및 확장성 향상
- 소명 처리 업무 자동화를 통한 업무 생산성 향상