

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 최대 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 구성 시 연계/분석/통계 지표 정보로 활용

▶ 글로벌 표준 위협정보 분류 체계 적용 자동화

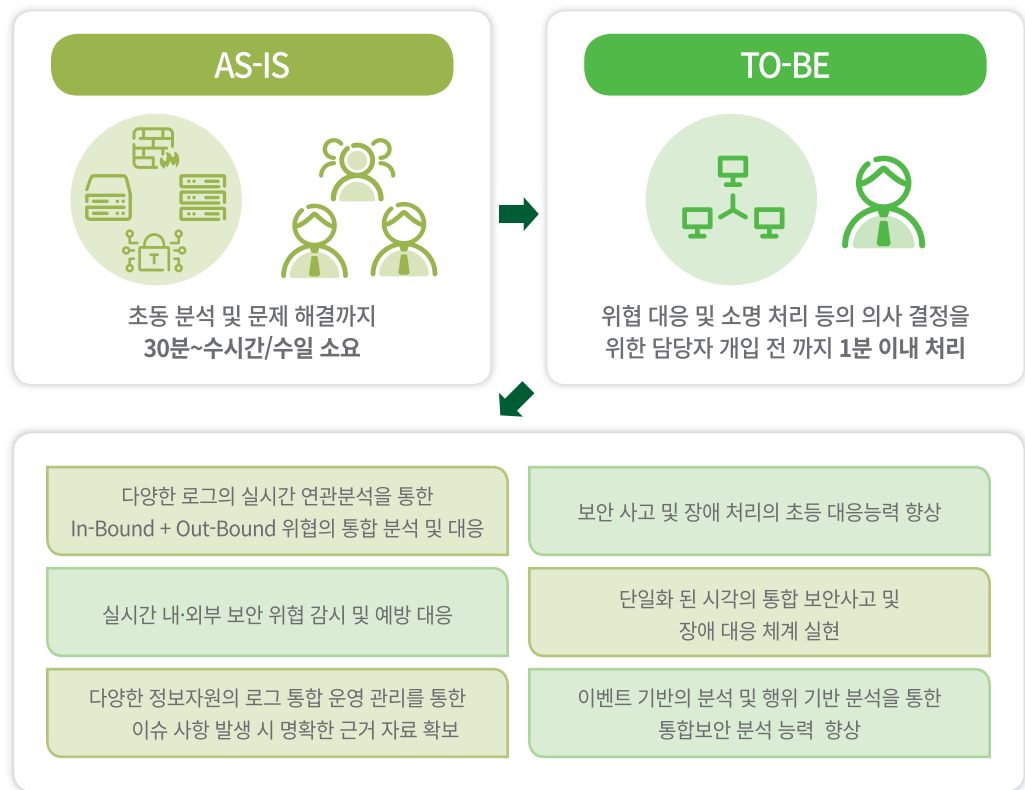
- 글로벌 표준 위협정보 분류 체계인 MITRE ATT&CK Matrix 정보 자동 수집 및 관리
- MITRE ATT&CK Navigator 모니터링 : 위협 이벤트 탐지 시 MITRE ATT&CK Attack ID와 매핑하여 공격 흐름의 시뮬레이션과 방어 기술을 제시하는 실시간 모니터링

▶ AI의 손쉬운 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



- **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



통합보안 분석 및 대응 솔루션



다양한 위협을 정확하게 분석하고 신속하게 대응합니다





통합보안 분석 및 대응 솔루션

- GS인증 1등급
- CC인증 EAL2
- 관련 특허
누적 38개 보유
- 조달청 디지털서비스물

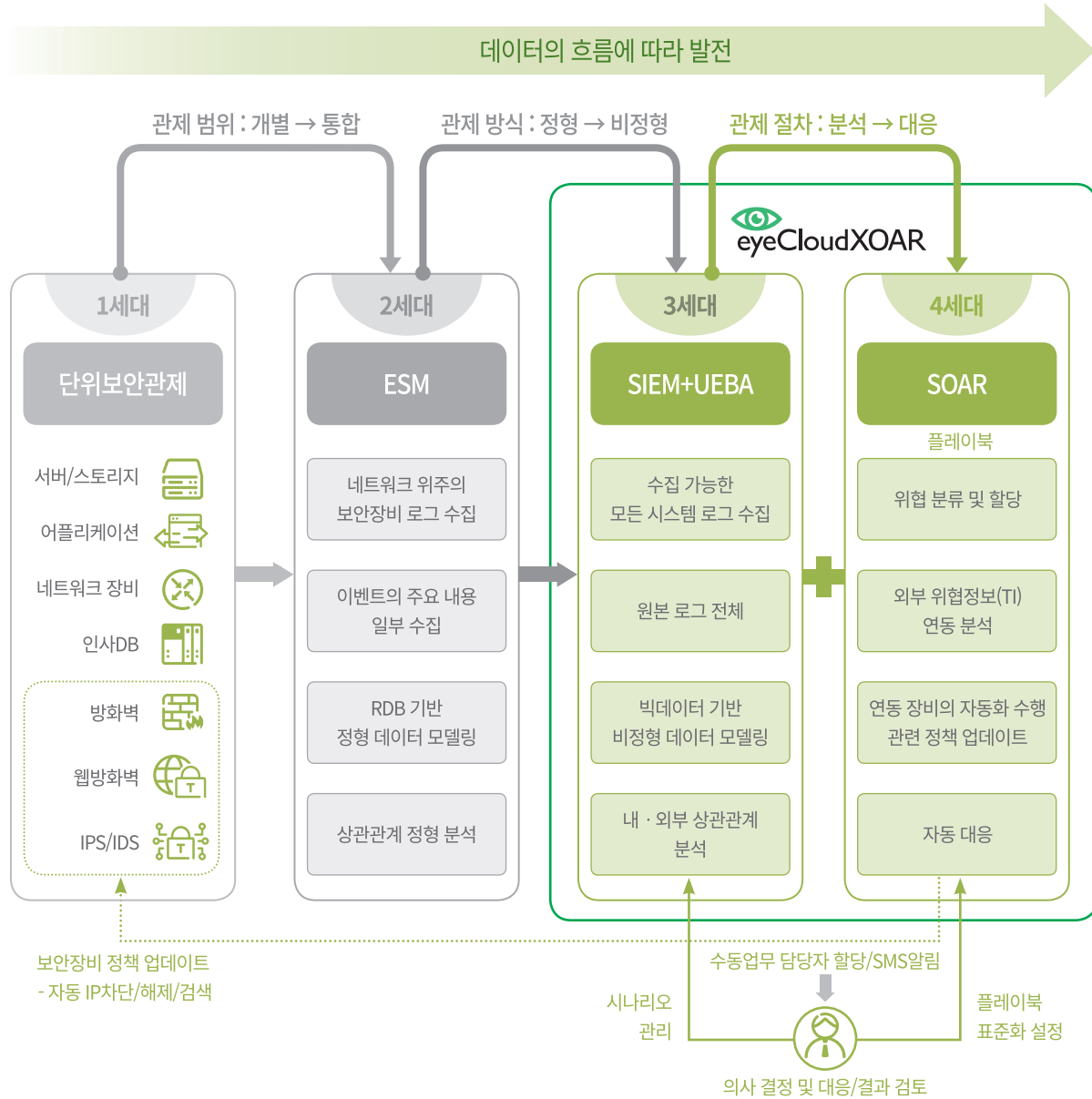


특장점

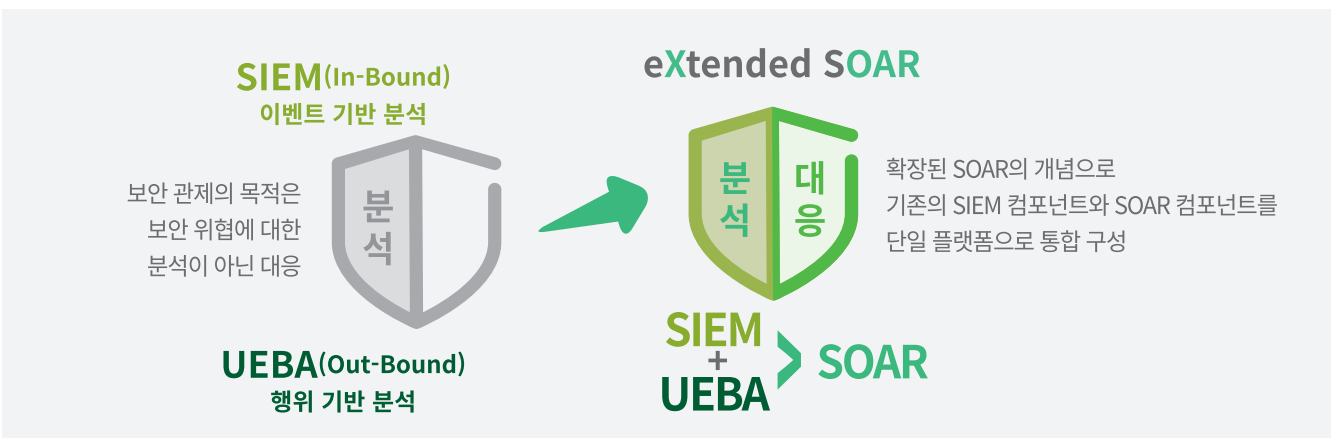


보안관계 패러다임의 변화

▶ 세대별 보안관계시스템의 명칭



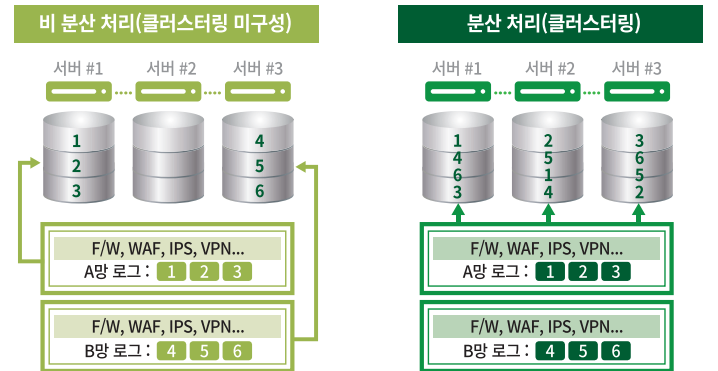
▶ XOAR(eXtended SOAR)



SIEM

▶ 다수 서버 운영 효율 최대화를 통한 빠른 성능과 안정성

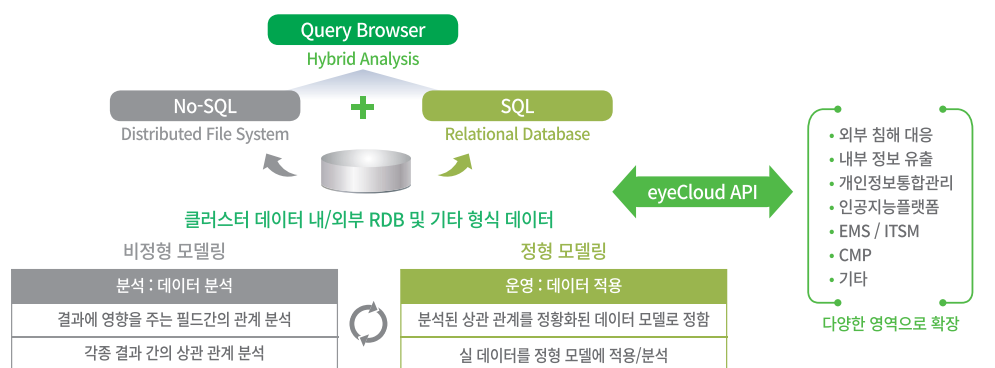
- 최초 제품 출시부터 다수 서버의 운영 효율 최대화를 위한 데이터 클러스터링 기반 독보적인 자체 분산 처리 기술 적용



▶ 공인된 국내 최초 단일서버의 초고속 빅데이터 처리 및 검색 성능

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

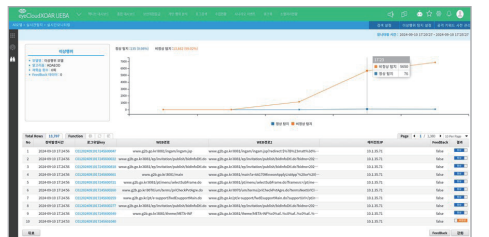
- 분석 대상이나 방식에 제한이 없는 하이브리드 분석 도구(Query Browser)



UEBA

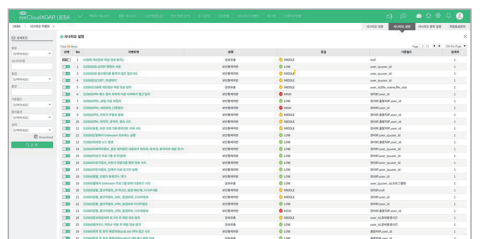
▶ 고급 분석을 통한 분석의 정확도 제고

- 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

