한국인터넷진흥원(KISA) (24년)-공공

24년 협업기반 통합보안 모델 개발 시범사업

고객사 소개

한국인터넷진흥원(KISA) 대한민국의 인터넷 진흥, 인터넷 정보보호 및 그에 대한 국제 협력 업무를 수행하는 과학기술 정보통신부 산하 위탁집행형 준정부기관 입니다.
사회 전 분야로의 사이버 안전망 구축 확대 및 데이터 경제 활성화 기반 조성에 힘쓰고, 블록체인·5G 등의 신기술을 기반으로 한 기반시설 구축 및 혁신 서비스 발굴에도 앞장서는 인터넷 정보보호 전문기관 입니다. 이외 ICT·정보보호 산업 및 인재 육성에도 집중하고 있습니다.

구축 제품 및 서비스

- eyeCloudXOAR v4.0 – SIEM (통합보안분석솔루션)
- eyeCloudXOAR v4.0 – SOAR (통합보안대응솔루션)
- OPEN XDR (오픈(OPEN) 확장형 탐지·대응(XDR) 통합보안 플랫폼)

Background(도입 배경)

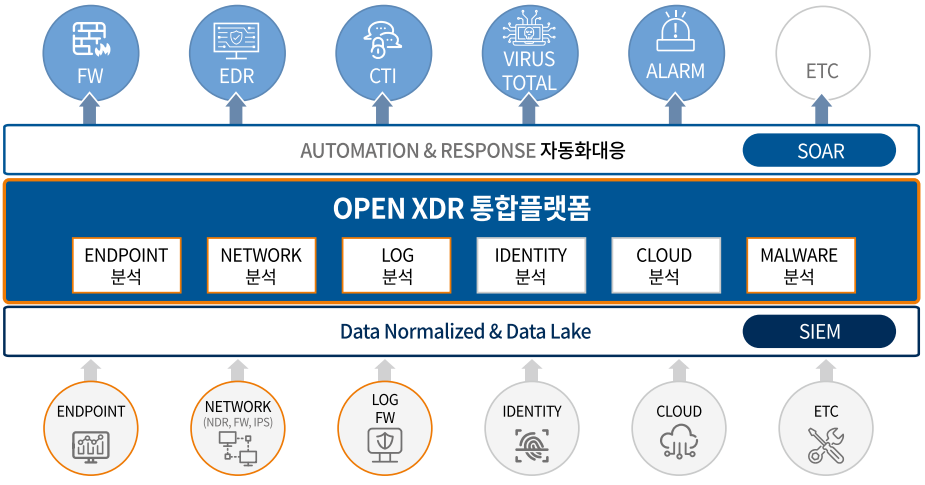
KISA는 기존 보안 솔루션 간 연동 부족으로 인한 운영 비효율성을 해결하고, 통합적인 위협 탐지 및 대응 체계를 구축하기 위해 통합보안모델 개발 시범사업을 추진하였습니다. 개별 보안 시스템이 독립적으로 운영되면서 SIEM, EDR, NDR 등 보안 데이터의 연계 분석이 어렵고, 위협 탐지의 일관성이 부족한 문제가 있었습니다. 이는 국내 보안 시장의 경쟁력 약화로 이어져, 글로벌 시장에서의 도태 가능성마저 제기되고 있는 실정입니다. 이러한 문제점을 해결하고자 2024년 협업기반 통합보안 모델 개발 시범사업의 일환으로 OPEN XDR 사업을 추진하게 되었습니다.

본 사업은 사이버 위협에 대한 효율적인 대응 및 시장 경쟁력 강화를 목표로 특히, 개방형 보안 플랫폼 구축을 통한 다양한 보안 솔루션 연동, 위협 정보 공유 및 협력 증진, 국내 보안 산업의 기술력 향상 및 경쟁력 강화 에 중점을 두고 있습니다. OPEN XDR 사업을 통해 시큐레이어는 국내 보안 시장의 혁신을 선도하고, 사이버 위협으로부터 안전한 디지털 환경을 조성하는데 기여할 것으로 기대됩니다.

프로젝트 기간

2024년 05월 ~ 2024년 11월

Concept map(개념도)



Solution(구축 내용)

협업 기반 통합보안 플랫폼 구축을 통한 위협 대응력 및 운영 효율성 강화

KISA는 다양한 보안 솔루션 간 연계성과 데이터 통합을 강화하기 위해 개방형 아키텍처(OPEN XDR) 기반의 통합보안 모델을 구축하였습니다. 이를 통해 보안 이벤트 분석의 정확도를 높이고, 신속한 대응 체계를 마련하여 보안 운영의 효율성을 극대화하였습니다

기존에는 각 보안 솔루션이 독립적으로 운영되면서 위협 탐지의 일관성이 부족하고, 보안 데이터의 상관 분석이 제한적이었습니다. 이번 구축을 통해, SIEM, EDR, NDR 등의 보안 솔루션을 통합하여 중앙에서 위협 탐지를 수행하고, 실시간 상관 분석을 통해 보안 이벤트의 연계성을 강화하였습니다

API 기반의 표준 연동 기술을 활용하여 다양한 보안 솔루션 간 호환성을 확보하고, 협업 기반의 위협 정보 공유 체계를 구축하였습니다. 이를 통해 공공기관과 금융권 등 다양한 산업 분야에서 적용할 수 있는 확장성을 갖춘 보안 모델을 실현하였습니다

이번 구축을 통해 KISA는 다양한 보안 솔루션 간 연계를 최적화하고, 실시간 위협 탐지 및 자동화 대응을 통해 보안 관제의 효율성을 극대화할 수 있는 환경을 마련하였습니다.

Benefit(도입 효과)

Open XDR 기반 실시간 위협 대응 및 보안 운영 최적화

KISA는 OPEN XDR 기반의 통합보안모델을 구축하면서, 기존 단일 솔루션 중심의 보안 운영에서 벗어나 실시간 위협 탐지 및 대응 체계를 한층 강화하였습니다.

보안 이벤트 간의 상관관계를 분석하기 위해 SIEM, EDR, NDR을 연계하여 단일 솔루션으로 탐지하기 어려웠던 잠재적 위협을 식별할 수 있는 체계를 마련하였으며, SOAR 기반의 자동화 대응을 적용하여 보안 이벤트 탐지부터 대응까지의 시간을 단축하고 운영 부담을 최소화하였습니다.

또한, API 기반 표준 연동 기술을 활용하여 보안 솔루션 간 호환성을 확보하고, 협업을 통한 위협 정보 공유 체계를 구축하였습니다. 이러한 접근 방식은 공공기관과 금융권 등 다양한 산업 분야에서 활용할 수 있도록 보안 모델의 확장성을 높이는 데 기여하였습니다.

KISA는 이번 구축을 통해 다양한 보안 솔루션 간 연계를 최적화하고, 실시간 위협 탐지 및 자동화 대응을 통해 보안 관제의 효율성을 극대화할 수 있는 환경을 마련하였습니다.

요약

1. 보안 통합 관리와 위협 대응 체계를 효과적으로 구축하기 위한 OPEN XDR 통합플랫폼 개발
2. API 기반 연동을 통한 확장성 확보 및 보안 정보 공유 체계 구축
3. OPEN XDR 통합보안 플랫폼 도입을 통한 위협탐지 및 대응 시간 감소, 운영비용 절감 등 효율적인 통합 운영