한국국제협력단(KOICA) (22년)-공공

KOICA 정보보안시스템 구축 용역

고객사 소개

한국국제협력단(KOICA)은 대한민국 정부의 대외 무상원조를 전담하는 외교부 산하 공공기관으로, 개발도상국의 경제·사회 발전을 지원하고 국제협력을 강화하는 역할을 수행하고 있습니다.
KOICA는 보건·교육·농업·산업·행정·환경 등 다양한 분야에서 개발협력 사업을 추진하며, 지속 가능한 발전을 위한 글로벌 협력체계를 구축하고 있습니다.

구축 제품 및 서비스

- eyeCloudXOAR v4.0 – SIEM (통합보안분석솔루션)
- eyeCloudXOAR v4.0 – SOAR (통합보안대응솔루션)
- eyeCloudAI v3.0 (인공지능분석솔루션)

Background(도입 배경)

향후 디지털 전환 및 국내/외 사무소(45개) 시스템에 대한 로그 수집 시 , 수집 데이터 증가에 따라 통합로그시스템 라이선스 부족 현상이 발생하였고, 기 운영중인 통합로그시스템의 경우 용량 증설 시 안정적인 성능 확보가 되지 않아 통합로그시스템을 수집 서버 및 분석서버로 분리 구축하여 운영 안정성에 대한 확보가 불가피해졌습니다.

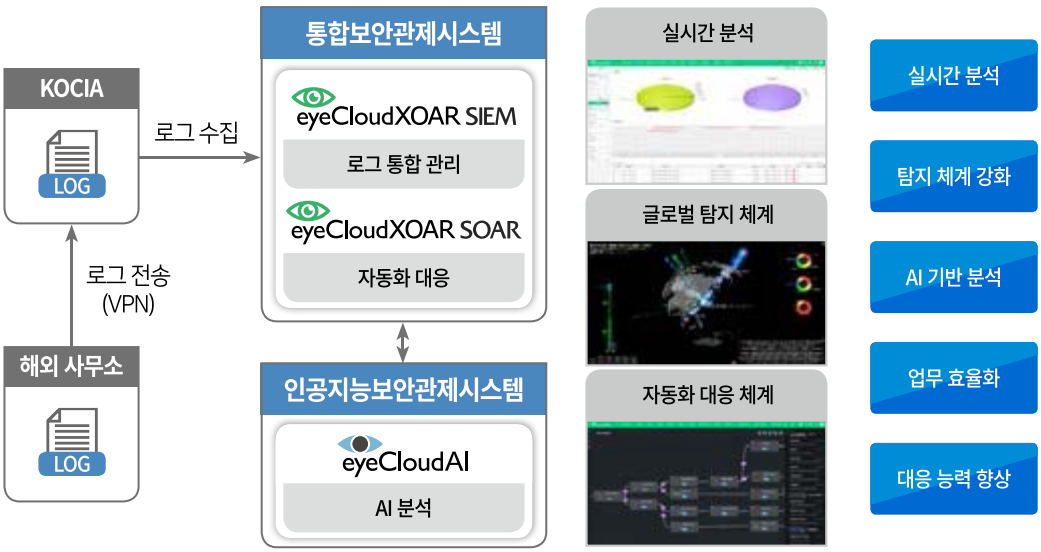
KOICA는 SIEM을 도입하여 국내외 시스템에서 발생하는 보안 로그를 통합 수집·분석하여 위협을 탐지하고, SOAR을 활용하여 자동화된 대응 프로세스를 구축하고 위협 대응 속도를 높였습니다. 또한 AI를 적용하여 고도화된 보안 위협 탐지 및 분석 기능을 강화하고, 지능형 위협 탐지 체계를 마련하였습니다.

이를 통해 KOICA는 보안 이벤트를 보다 효과적으로 관리하고, 빠른 대응을 통해 기관의 정보자산을 보호하며, 안정적인 국제 협력 사업 운영을 가능하게 하였습니다.

프로젝트 기간

2022년 11월 ~ 2022년 12월

Concept map(개념도)



Solution(구축 내용)

글로벌 협력 환경의 보안 강화를 위한 통합 보안 관제 시스템 구축

한국국제협력단(KOICA)은 국제 협력 사업에서 발생하는 다양한 보안 위협을 신속하게 탐지·대응하기 위해 SIEM, SOAR, AI 기반의 통합 보안 관제 시스템을 구축하였습니다. 기존 보안 체계는 각 시스템에서 개별적으로 로그를 관리하여 위협 대응 속도가 느리고, 실시간 분석 및 자동화 대응 기능이 부족한 한계가 있었습니다.

이번 구축을 통해 KOICA는 SIEM을 활용하여 글로벌 네트워크 및 정보 시스템에서 발생하는 보안 이벤트를 통합 관리하고, SOAR을 적용하여 탐지된 보안 이벤트에 대한 자동화된 대응 체계를 구축 하였습니다. 자동화 대응을 통해 시큐아이, 안랩 장비의 자동 차단 및 정책 설정으로 보안성을 강화하였습니다. 또한, AI 기반 위협 분석 기능을 도입하여 알려지지 않은 보안 위협을 보다 정밀하게 탐지하고 대응할 수 있도록 개선하였습니다.

보안 운영 측면에서도 보안 이벤트의 연관 분석 기능을 강화하여 위협 요소를 보다 신속하게 식별할 수 있도록 하였으며, 맞춤형 대시보드를 통해 관리자가 실시간으로 위협 상황을 모니터링하고 즉각적인 조치를 취할 수 있도록 지원하였습니다.

이를 통해 KOICA는 전 세계에서 발생하는 보안 위협에 보다 효과적으로 대응하고, 국제 협력 사업의 안전성을 강화할 수 있는 보안 환경을 구축하였습니다.

Benefit(도입 효과)

AI 기반 보안 위협 탐지 및 대응 체계 강화

한국국제협력단(KOICA)은 SIEM, SOAR, AI 기반의 통합 보안 관제 시스템 구축을 통해 보안 위협 탐지 및 대응 역량을 대폭 향상시켰습니다.

SIEM 도입을 통해 보안 로그를 중앙에서 수집·분석함으로써 위협 탐지의 정확도를 높이고, SOAR을 활용하여 보안 이벤트 발생 시 자동화된 대응이 가능하도록 구축되었습니다. 또한, AI 기반의 위협 분석 기능을 적용하여 기존 룰 기반 탐지의 한계를 보완하고, 알려지지 않은 보안 위협을 조기에 탐지할 수 있도록 개선되었습니다.

운영 측면에서도, 보안 이벤트의 연관 분석을 통해 글로벌 협력 네트워크에서 발생하는 위협을 보다 체계적으로 관리할 수 있게 되었으며, 맞춤형 대시보드를 통해 보안 담당자가 실시간으로 위협 상황을 모니터링하고 즉각적으로 조치할 수 있는 환경을 마련하였습니다.

이를 통해 KOICA는 국제 협력 사업을 안전하게 수행할 수 있도록 보안성을 강화하고, 보안 운영의 효율성을 극대화할 수 있는 체계를 구축하였습니다.

요약

1. 정보보안시스템을 고도화하고 보안 위협 감지 및 대응 능력을 강화
2. SOAR를 활용한 자동화된 보안 이벤트 대응 및 차단 체계 구축
3. AI 기반 위협 분석 적용을 통한 보안 운영 최적화 및 실시간 모니터링 강화