해양수산부 (21년)-공공

인공지능 기반의 보안관제체계 구축 및 AI 서비스모델 고도화 사업

고객사 소개

해양수산부는 해양정책, 수산, 어촌 개발 및 수산물 유통, 해운·항만, 해양환경, 해양조사, 해양수산자원개발, 해양과학기술연구·개발 및 해양안전심판에 관한 사무를 관장하는 대한민국의 중앙행정기관 입니다.
해양수산수 및 소속·산하기관 43개 기관에 대해 24시간 365일 무중단 사이버보안 관제를 통한 사이버위협에 대응을 위해 본 프로젝트 구축 및 고도화 사업을 진행 하였습니다.

구축 제품 및 서비스

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

Background(도입 배경)

해양수산부는 국가 해양·수산 데이터를 보호하고 사이버 위협 대응 역량을 강화하기 위해 인공지능 기반 보안관제체계 구축 사업을 추진하였습니다. 디지털 전환이 가속화되면서 기존 보안 운영 방식으로는 지능화된 공격을 실시간 탐지하고 신속히 대응하는 데 한계가 있었습니다.

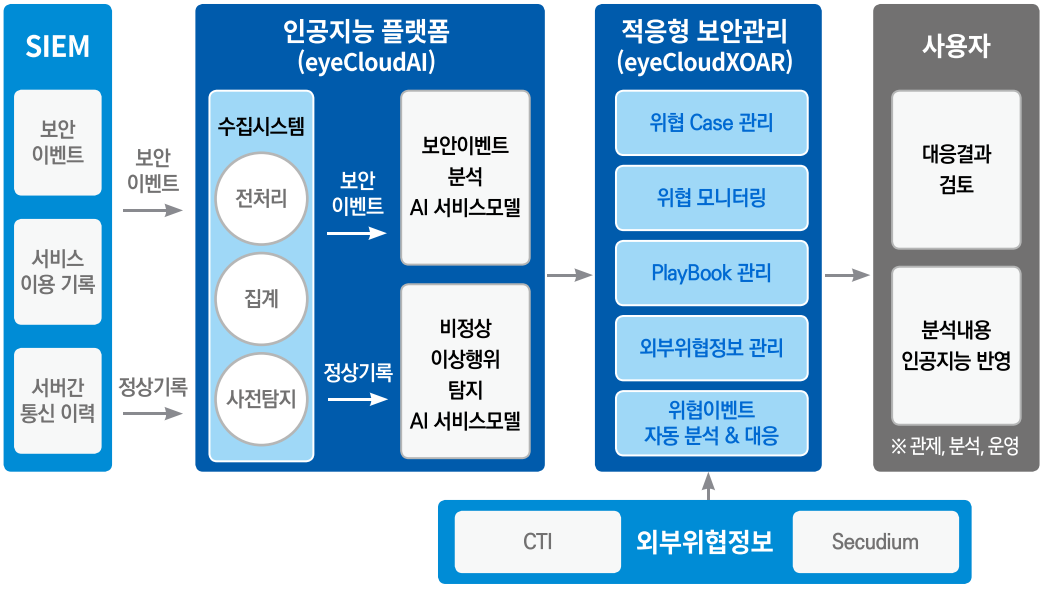
해양수산부는 SIEM을 통해 보안 로그를 통합 분석하고 위협 탐지 역량을 강화하였으며, SOAR을 활용해 자동화된 대응 체계를 마련하여 보안 이벤트 발생 시 신속한 차단이 가능하도록 했습니다. 또한, AI 기반 위협 분석을 적용해 탐지 정밀도를 높이고 알려지지 않은 위협에 대한 대응 역량을 향상시켰습니다.

이를 통해 해양수산부는 보안 이벤트 대응 속도를 단축하고, 보다 안정적이고 효율적인 보안 운영 환경을 확보할 수 있었습니다.

프로젝트 기간

2021년 09월 ~ 2021년 12월

Concept map(개념도)



Solution(구축 내용)

AI 기반 보안 관제 체계 고도화를 통한 탐지 정확도 향상 및 자동화 대응 구현

해양수산부는 AI 기반 보안관제 시스템을 고도화하여 보안 위협 탐지 정확도를 높이고, 자동화된 대응 체계를 구축하기 위해 SIEM, SOAR, AI를 도입하였습니다. 이를 통해 보안 이벤트를 보다 정밀하게 분석하고, 신속한 대응이 가능한 환경을 마련하였습니다.

기존에는 탐지 정확도가 낮아 반복적인 분석 업무가 많고, 보안 이벤트의 실시간 대응이 어려운 한계가 있었습니다. 이번 구축을 통해, AI 탐지 모델을 업그레이드하여 최신 공격 키워드 1.5만 개를 추가하고, 강화학습을 적용하여 탐지 정확도를 99.3% 이상으로 향상시켰습니다.

또한, 1개의 피드백 데이터만으로도 실시간 모델 반영이 가능하도록 개선하여 탐지 및 대응 자동화의 효과를 극대화하였습니다. Siem을 활용해 보안 이벤트를 통합 관리하고 soar를 통해 탐지 위협에 대한 자동화 대응을 구현하여 위협 대응 역량을 강화하였습니다.

운영 측면에서는 맞춤형 대시보드를 통해 실시간 모니터링을 지원하고, GPU 가상화를 활용하여 AI 학습 성능을 최적화하였습니다.

이번 구축으로 해양수산부는 AI 기반 보안 관제 체계를 고도화하고, 자동화된 대응 프로세스를 통해 보안 위협을 보다 신속하고 정밀하게 탐지·대응할 수 있는 환경을 마련하였습니다.

Benefit(도입 효과)

해양수산부의 AI 보안관제 고도화, 사이버 위협 대응 역량 강화

해양수산부는 보안 위협 탐지 정밀도를 높이고, 자동화된 대응 체계를 구축하여 실시간 보안 운영을 최적화하였습니다. 기존에는 탐지 정확도가 낮고, 보안 이벤트 분석 및 대응 속도가 느린 한계가 있었습니다.

이번 구축을 통해, AI 기반 탐지 모델을 적용하여 정확도를 95% 이상으로 향상시키고, TMS 로그의 99%를 자동 분석하여 보안 관제 인력의 업무 부담을 줄였습니다.

또한, SOAR을 활용한 자동화 대응을 통해 보안 이벤트 간 연관 분석 기능을 강화하고, 대응 시간을 단축하였습니다.

운영 측면에서도 맞춤형 대시보드를 활용한 실시간 위협 모니터링이 가능해졌으며, GPU 가상화를 통해 AI 학습 속도를 최적화하였습니다.

이를 통해 해양수산부는 AI 기반 보안 관제 체계를 고도화하여 탐지 정확도를 향상시키고, 자동화된 대응 프로세스를 구축하여 보안 위협에 대한 선제적 대응이 가능한 환경을 마련하였습니다.

요약

1. 43개 기관에 24시간 365일 대응 가능한 사이버위협 자동대응 체계 마련 및 사이버 보안관제 효율성 향상
2. 보안 시스템 및 SIEM에서 발생하는 보안이벤트의 자동식별 및 분석 체계 탐지율 향상 (30% → 80% 모델 정확도 향상 99.3%)
3. 사이버침해 위협 대응 자동화 기반 마련으로 서비스 품질 향상 및 업무 효율화