보건복지부

보건복지부 (24년)-공공

보건복지부 통합보안관리시스템(보안관제 분석,수집 시스템) 구매

고객사 소개

보건복지부는 국민의 건강과 복지를 책임지는 대한민국 중앙행정기관입니다. '모든 국민이 건강하고 행복한 삶을 누리는 포용적 복지국가 실현'을 목표로, 질병 예방 및 관리, 의료 서비스 제공, 건강보험 운영, 사회복지 서비스 지원 등 다양한 정책을 수립하고 시행하고 있습니다.주요 업무는 건강보험 제도 운영, 의료 서비스 질 향상, 감염병 및 만성질환 예방 관리, 취약 계층 의료비 지원, 노인, 장애인, 아동 등을 위한 사회복지 서비스 제공 등을 포함합니다. 국민의 건강 증진과 삶의 질 향상을 위해 끊임없이 노력하는 기관입니다.

구축 제품 및 서비스

eyeCloudXOAR v4.0 – SIEM
(통합보안분석솔루션)

eyeCloudXOAR v4.0 – SOAR
(통합보안대응솔루션)

Background(도입 배경)

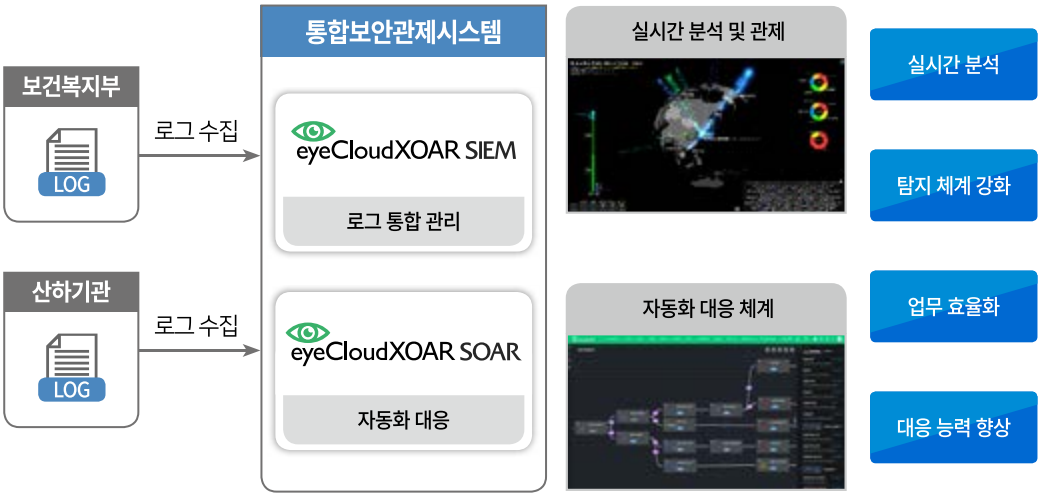
보건복지부는 통합보안관제시스템 재구축 사업을 통해 노후화된 보안 시스템을 개선하고, 자동화된 보안 관제 체계를 구축하여 보안 운영의 효율성을 높이고자 했습니다. 기존 시스템으로는 방대한 의료·행정 데이터를 보호하고, 증가하는 사이버 위협을 실시간으로 탐지·대응하는 데 한계가 있었습니다.

보건복지부는 SIEM을 도입하여 의료원 및 산하기관의 보안 로그를 통합 수집·분석하고, SOAR을 활용해 탐지된 위협에 대한 자동화된 대응 체계를 구축하였습니다. 또한, 플레이북 기반의 보안 프로세스를 마련하여 웹해킹, 악성코드 감염, 비정상 통신 등 주요 보안 이벤트를 신속하게 탐지·대응할 수 있도록 개선하였습니다. 이를 통해 보건복지부는 보안 위협 탐지 및 대응 속도를 향상시키고, 보다 체계적이고 자동화된 보안 운영 환경을 확보할 수 있었습니다.

프로젝트 기간

2024년 02월 ~ 2024년 09월

Concept map(개념도)



Solution(구축 내용)

빅데이터 기반 보안 관제 고도화 및 자동화 대응 체계 구축

보건복지부는 노후화된 보안 관제 시스템을 재구축하고, 자동화 기술을 적용하여 실시간 보안 위협 탐지 및 대응 역량을 강화하였습니다. 이번 사업을 통해 빅데이터 클러스터링 기반의 통합 보안 관제 시스템을 구축하여 대량의 보안 로그를 효과적으로 수집·분석하고, 자동화된 대응 프로세스를 도입하였습니다.

기존에는 보건복지부 산하기관 및 의료원에서 발생하는 방대한 보안 로그를 개별적으로 관리하여 실시간 위협 탐지 및 대응이 어려웠습니다. 이를 개선하기 위해 총 432대의 보안 장비와 연동하여 데이터 수집 및 정규화를 수행하고, 기존 탐지 정책 783개를 100% 이관 및 검증하여 탐지 체계를 강화하였습니다.

SOAR을 활용한 자동화 대응 시스템도 구축하였습니다. 웹 해킹, 비정상 통신, 악성코드 감염 등 총 10종의 보안 위협 탐지를 위한 자동화 프로세스를 구현하고, 방화벽과의 API 연동을 통해 자동 차단 및 조치 프로세스를 마련하였습니다.

이번 구축을 통해 보건복지부는 보건·의료 데이터 보호를 위한 선진화된 보안 관제 체계를 구축하고, 보안 위협 탐지 및 자동화 대응 체계를 통해 보다 신속하고 정밀한 보안 운영 환경을 실현하였습니다.

Benefit(도입 효과)

보건·의료 데이터 보호를 위한 통합 보안 관제 체계 구축 및 자동화 대응 강화

보건복지부는 노후화된 보안 관제 시스템을 재구축하여, 디지털 환경 변화에 맞춰 보건·의료 데이터 보호를 강화하고 사이버 위협 대응 역량을 획기적으로 강화하였습니다.

이번 시스템 재구축을 통해 보건복지부 산하기관 및 의료원에서 발생하는 방대한 보안 로그를 통합 관리하고, 기존 시스템 탐지 정책을 100% 이관·검증하여 탐지 체계를 강화하고 주요 보안 위협을 자동 탐지할 수 있도록 SOAR 기반의 자동화 대응 시스템을 적용하였습니다.

또한, SOAR을 활용한 자동화 대응 시스템을 구축하여 웹 해킹, 비정상 통신, 악성코드 감염 등 총 10종의 보안 위협에 대한 자동화된 대응 프로세스를 구현하였습니다. 이러한 자동화된 대응 체계는 보안 인력의 업무 부담을 경감시키고, 대응 속도를 획기적으로 향상시켰습니다.

통합적이고 자동화된 보안 관제 시스템의 도입은 보건복지부의 사이버 보안 역량을 강화하고, 보건·의료 데이터의 안전한 보호를 위한 기반을 공고히하였습니다.

요약

1. 92개 산하기관 432대의 장비 연동으로 24시간 365일 대응 가능한 사이버위협 자동대응 체계 마련 및 사이버 안전센터 통합보안관제시스템 효율성 향상
2. 기존 시스템의 안정적 연동 및 이관으로 안전한 보안관제 시스템 구축
3. 자동화 기술 도입을 통한 보건·의료 데이터 보호 및 사이버 보안 역량 강화