국세청 (24년)-공공

국세청 스마트 보안관제시스템 구축용 소프트웨어 구매사업

고객사 소개

국세청은 대한민국 정부기관으로, 국가의 재정 수입을 담당하는 기관입니다. 납세자들이 세금을 성실하게 신고하고 납부하도록 지원하고, 탈세 행위를 방지하여 조세 정의를 실현하는 데 힘쓰고 있습니다.
또한, 국민들에게 세금 제도와 관련된 정보를 제공하고, 납세 편의를 증진하기 위한 서비스를 지속적으로 개선하고 있습니다. 국세청은 투명하고 효율적인 세정 운영을 통해 국가 발전에 기여하고, 국민들의 삶에 도움이 되는 기관으로 자리매김하고자 노력하고 있습니다.

구축 제품 및 서비스

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

Background(도입 배경)

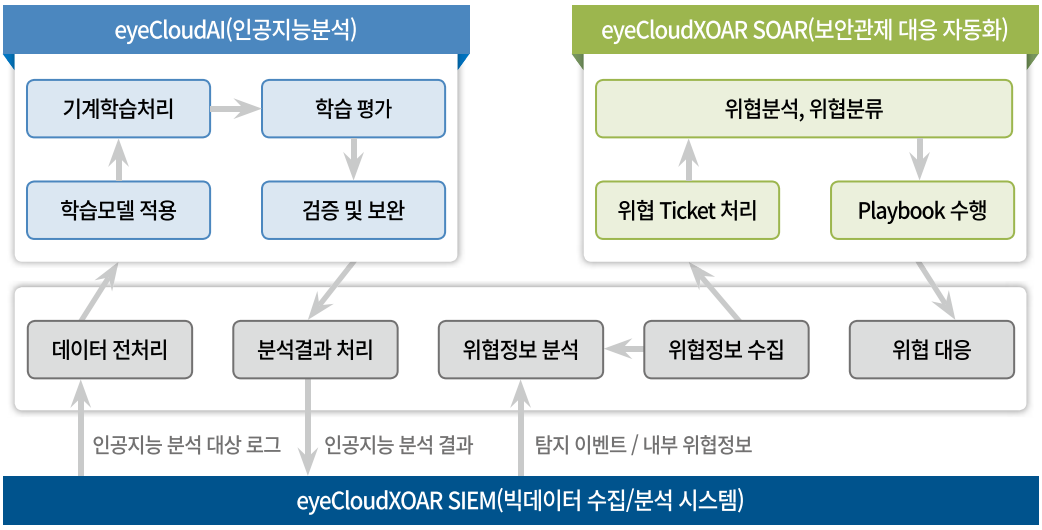
국세청은 스마트 보안관제시스템 구축 사업을 통해 최신 사이버 위협에 효과적으로 대응하고, 보안 운영의 자동화를 실현하고자 했습니다. 기존의 수동적인 보안 운영 방식으로는 지능화된 위협을 신속하게 분석하고 대응하는 데 한계가 있었으며, 이에 따라 첨단 기술을 활용한 자동화된 대응 체계 도입이 필수적이었습니다.

이에 따라, 시큐레이어의 SOAR 솔루션을 도입하여 반복적인 탐지·분석·대응 업무를 자동화하고, 보안관제의 효율성을 극대화하였습니다. PlayBook 기능을 활용해 실시간 위협 정보를 자동 분석하고 대응할 수 있도록 체계를 최적화하였으며, AI 기반의 보안관제 시스템을 통해 사이버 위협을 사전에 예측하고 신속한 대응이 가능하도록 하였습니다. 이를 통해 실시간 보안 위협 탐지 및 대응 속도를 단축하고, 보안 운영의 효율성을 높이며, 보다 안정적인 정보 보호 환경을 구축할 수 있었습니다.

프로젝트 기간

2024년 04월 ~ 2024년 10월

Concept map(개념도)



Solution(구축 내용)

대규모 행정 데이터를 보호하기 위한 AI 기반 보안 관제 체계 구축

국세청은 국가 행정 시스템에서 발생하는 방대한 데이터를 보호하고, 사이버 위협에 대한 신속한 대응 체계를 마련하기 위해 스마트 보안관제시스템을 구축하였습니다. 이번 사업을 통해 최신 위협 정보를 활용하여 실시간 탐지 및 대응을 강화하고, AI 기반 보안 관제 체계를 적용하여 탐지 정확도를 높였습니다.

기존에는 1일 400GB 이상의 방대한 보안 로그를 분석하는 과정에서 탐지 속도가 느리고, 오탐·정탐 판별이 어렵다는 한계가 있었습니다. 이를 개선하기 위해 다수의 타 기관 구축 경험을 통한 정오탐 통합모델 제공과 자체 데이터셋 및 국세청의 데이터셋을 통합하여 국세청데이터에 적합한 모델을 제작하여 탐지 정확도 및 속도를 향상시켰습니다.

SOAR을 활용한 자동화 대응 체계도 도입하여 위협 정보 탐지 시 방화벽 등의 보안 정책을 자동으로 갱신하고, 상황 전파 및 조치를 지원하는 국세청 환경에 최적화된 자동 대응 체계를 구현하였습니다.

운영 측면에서는 맞춤형 대시보드를 통해 보안 담당자가 실시간으로 보안 이벤트를 모니터링할 수 있도록 지원하고, 다양한 분석 기능을 제공하여 보안 위협에 대한 대응 속도를 단축하였습니다.

이번 구축을 통해 국세청은 대규모 보안 로그를 효과적으로 분석하고, AI 기반의 자동화 탐지 및 대응 시스템을 통해 보안 위협을 보다 신속하고 정밀하게 탐지·대응할 수 있는 환경을 마련하였습니다.

Benefit(도입 효과)

AI 기반 보안 관제 도입을 통한 납세자 정보 보호 및 사이버 보안 혁신

국세청은 인공지능(AI) 기반의 사이버 보안관제 시스템을 도입하여 납세자의 과세 정보를 안전하게 보호하고, 사이버 위협에 대한 대응 역량을 획기적으로 강화하였습니다. 챗GPT 등 AI 기술의 발전으로 보안 위협이 지능화되는 상황에서 국세청은 이러한 디지털 환경 변화와 새로운 보안 위협에 선제적으로 대응하고자 사람 중심의 보안 관제를 AI 기반으로 전환하였습니다.

새롭게 구축된 AI 보안관제 시스템은 보안 위협의 탐지, 분석, 대응, 전파 등 전 과정을 자동화하여, 수만 건의 공격 시도를 1초 이내에 분석하고 차단할 수 있습니다. 이를 통해 대량의 공격 시도가 발생하더라도 모든 보안 위협에 대한 신속하고 정확한 대응이 가능해졌습니다. 특히, 10월 개통 이후 2개월간의 안정화 기간 동안 일 평균 수백 건의 보안 위협을 분석·차단하여 단 한 건의 사고도 발생하지 않았습니다.

이번 시스템 도입으로 국세청은 AI를 활용한 보안 공격을 AI로 방어하는 체계를 구축하여, 납세자의 소중한 정보를 더욱 안전하게 보호하고 있습니다. 또한, 최신 보안 기술의 지속적인 도입과 시스템 확충을 통해 사이버 보안 환경 변화에 선제적으로 대응하고, 국세 행정의 디지털 혁신을 이끌어가는 기반을 마련하였습니다.

요약

1. AI 기반 보안 관제 시스템 도입을 통한 납세자 정보 보호 및 사이버 위협 대응 강화
2. 실시간 위협 분석 및 자동화 대응 체계 구축을 통한 위협 탐지 및 차단 속도 향상
3. 사이버 보안 환경 변화에 선제적으로 대응하는 디지털 보안 혁신 실현