교보생명 (22년~23년)

이상징후탐지시스템 고도화 구축

고객사 소개

교보생명은 대한민국의 선도적인 생명보험사로, 1958년에 설립되어 재정적 안정과 고객의 미래를 보장하는 다양한 보험 상품과 서비스를 제공하고 있습니다. 창립자 신용호의 비전 아래, 교보생명은 고객 중심의 경영 철학과 지속 가능한 성장을 추구하며, '좋은 성장'을 목표로 삼고 있습니다.
혁신적인 금융 솔루션과 탁월한 고객 서비스로 업계를 선도하고 있으며, 100년 기업을 향한 끊임없는 발전을 지속하고 있습니다.

구축 제품 및 서비스

- eyeCloudXOAR v4.0 – SIEM (통합보안분석솔루션)
- eyeCloudXOAR v4.0 – SOAR (통합보안대응솔루션)
- eyeCloudXOAR v4.0 – UEBA (이상행위분석솔루션)

Background(도입 배경)

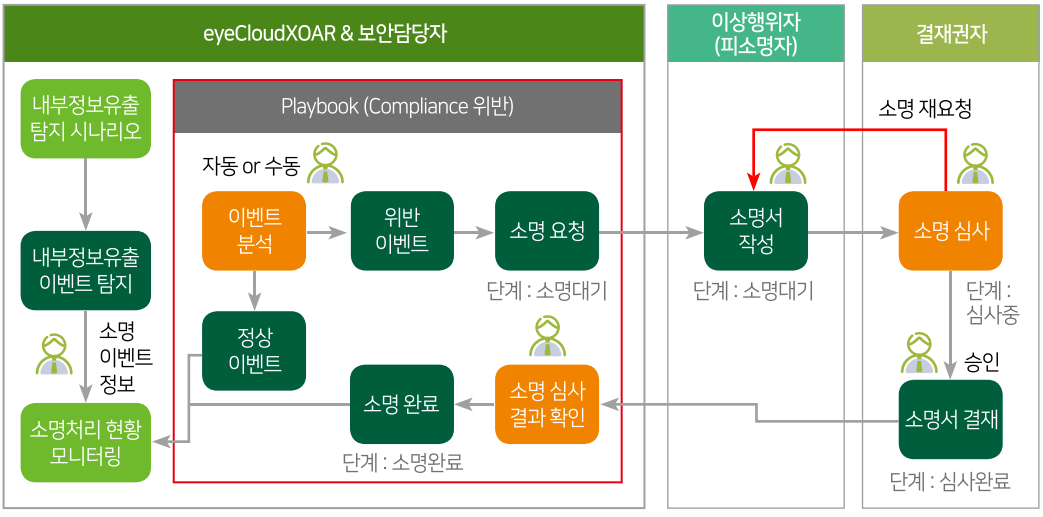
교보생명은 디지털 금융 확산에 따라 고객정보 보호와 내부 보안 통제 강화를 위해 이상징후탐지시스템을 고도화하였습니다. 금융업의 특성상 개인정보 유출 및 내부 정보 오남용에 대한 리스크가 커지고 있으며, 기존 보안 체계만으로는 복합적인 위협 탐지와 대응이 어려운 상황이었습니다.기존에 운영 중이던 A사 기반 보안 시스템의 운영체계(OS) 및 소프트웨어 서비스 종료(EOS)로 인해 유지보수 및 보안 취약점 대응이 어려운 문제가 있었습니다. 이에 따라, SIEM을 도입하여 개인정보처리시스템 및 보안 솔루션의 로그를 통합 분석하고, SOAR을 활용하여 자동화된 대응 및 소명 프로세스를 강화하였습니다. 특히, 사용자의 고객정보 유출 행위를 탐지하는 시나리오를 정교화하고, 연관·상관 분석을 적용하여 이상징후 탐지 정확도를 향상시켰습니다.

이번 고도화를 통해 교보생명은 고객정보 보호 역량을 강화하고, 금융 보안 규제에 선제적으로 대응할 수 있는 체계를 마련하여 보다 안전하고 신뢰할 수 있는 금융 서비스를 제공할 수 있는 기반을 확보하였습니다.

프로젝트 기간

2022년 09월 ~ 2023년 02월

Concept map(개념도)



Solution(구축 내용)

개인정보 보호 강화를 위한 통합 보안 체계 구축

교보생명은 금융권의 보안 요구사항을 충족하고, 개인정보 유출 및 내부 정보 오남용을 방지하기 위해 SIEM 기반의 이상징후탐지시스템을 고도화하였습니다. 기존 시스템은 각종 보안 솔루션과 개인정보처리시스템에서 발생하는 로그를 개별적으로 관리하여 이상 행위 탐지 및 분석이 어려운 구조였습니다.

이번 구축을 통해 SIEM을 도입하여 교보생명의 다양한 금융 IT 시스템에서 발생하는 보안 로그를 통합 분석하고, 실시간 탐지 및 대응 체계를 강화하였습니다. 특히, SOAR을 활용하여 이상 행위 탐지 시 자동화된 대응 및 소명 프로세스를 구축하였으며, 보안 이벤트 발생 시 즉각적인 조치를 수행할 수 있도록 대응 속도를 향상시켰습니다.또한, 사용자의 고객정보 접근 행위를 정밀하게 분석하기 위해 연관·상관 분석 기능을 적용하여 이상징후 탐지의 정확도를 높이고, 단순 패턴 탐지가 아닌 복합적인 이상 행위 탐지가 가능하도록 개선하였습니다. 이를 통해 내부 정보 유출 및 비정상적인 데이터 접근을 조기에 차단하고, 보안 사고 예방을 위한 체계를 강화하였습니다.

보안 담당자가 실시간으로 이상징후를 모니터링하고, 탐지된 이벤트에 대한 대응 프로세스를 체계적으로 관리할 수 있도록 최적화하였습니다. 또한, 개인정보 보호법 및 금융 보안 규제 준수를 위한 감사 체계를 정비하여 보안 운영의 신뢰성을 높이고, 법적 대응 역량을 강화하였습니다.

Benefit(도입 효과)

고객정보 보호 체계 강화 및 금융 보안 신뢰성 확보

교보생명은 디지털 금융 서비스 확산과 마이데이터 시대 도래에 따라 고객정보 보호를 최우선 과제로 삼고, 내부 정보 오남용을 효과적으로 탐지하고 대응할 수 있는 체계를 마련하였습니다. 기존에는 보안 로그가 개별 시스템에 분산되어 있어 이상 행위를 종합적으로 분석하는 데 한계가 있었으며, 내부 직원 및 협력사의 고객정보 접근이 증가하면서 보다 정교한 분석 체계가 필요했습니다.

고도화된 연관·상관 분석을 적용하여 탐지 정확도를 향상시키고, 자동화된 대응 체계를 통해 보안 운영을 보다 효율적으로 관리할 수 있도록 개선하였습니다. 또한, 금융 보안 규제 준수를 위한 감사 체계를 정비함으로써 보안 사고 발생 시 신속한 원인 분석과 대응이 가능해졌으며, 내부 감사 및 외부 보안 감사 대응 역량이 강화되었습니다.

이번 사업은 단순한 시스템 개선을 넘어, 금융 보안 환경 변화에 선제적으로 대응할 수 있는 장기적인 보안 운영 체계를 마련하는 데 중점을 두었습니다. 이상징후 탐지의 자동화 및 대응 프로세스 정비를 통해 보안 운영의 신뢰성을 확보하였으며, 보안 관제 인력의 업무 부담을 줄이는 동시에 금융 IT 환경 전반의 안정성을 높였습니다. 이를 통해 교보생명은 보안 사고를 예방하고, 지속적으로 변화하는 금융 보안 환경에 유연하게 대응할 수 있는 역량을 확보하였습니다.

요약

1. 이상징후탐지시스템 고도화 구축을 통한 내부 보안 강화 및 업무 효율성 향상
2. 보안 이벤트 탐지, 분석, 대응 프로세스 자동화를 통한 업무시간 단축 방안 마련
3. 금융 보안 규제 준수 및 감사 체계 정비로 법적 대응 역량 강화