광주은행 (24년)

ESM 시스템 업그레이드 구축 사업(침해사고대응 3단계 구축)

고객사 소개

광주은행은 1968년 설립된 대한민국의 지방은행으로, JB금융지주의 자회사입니다.
광주광역시와 전라남도를 기반으로 하며, 지역 경제 활성화에 기여하고 있습니다. 개인 및 기업 고객에게 다양한 금융 상품과 서비스를 제공하며, 편리한 디지털 뱅킹 서비스를 통해 고객 만족도를 높이고 있습니다. 최근에는 해외 시장 진출에도 적극적으로 나서고 있으며, 사회공헌 활동에도 힘쓰고 있습니다.

구축 제품 및 서비스

eyeCloudXOAR v4.0 – SIEM
(통합보안분석솔루션)

Background(도입 배경)

광주은행은 디지털 금융 환경이 빠르게 변화함에 따라, 점점 지능화되는 사이버 공격에 대응하고 금융 서비스의 연속성을 보장하기 위해 통합 보안 관제 체계를 구축하였습니다. 금융권은 고객의 자산 및 개인정보를 보호해야 하는 핵심 산업으로, 보안 위협이 금융 사고로 이어질 경우 신뢰도 저하와 직접적인 피해가 발생할 수 있습니다. 이에 따라 은행 내부 시스템뿐만 아니라 고객과의 금융 거래 과정에서도 발생할 수 있는 다양한 보안 위협을 종합적으로 분석하고 대응할 수 있는 체계 마련이 필요하였습니다.

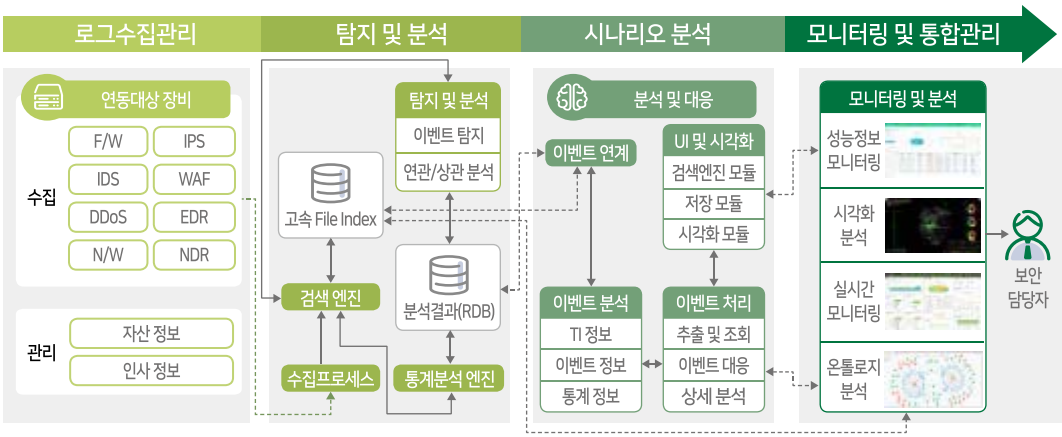
기존의 보안 운영 방식은 각 보안 솔루션이 개별적으로 운영되면서 로그 수집 및 분석이 분산되고, 실시간 위협 탐지가 어려운 문제가 있었습니다. 또한, 급증하는 보안 이벤트를 효과적으로 분석하고 대응할 수 있는 체계를 구축하지 못하면 금융 서비스의 안정성이 저하될 위험이 있었습니다.

이에 따라, 광주은행은 SIEM 기반의 통합 로그 분석 체계를 도입하여 금융 IT 인프라에서 발생하는 보안 이벤트를 중앙에서 관리하고, FCTI 연계를 통해 최신 금융권 보안 위협 정보를 실시간으로 반영할 수 있는 환경을 구축하였습니다. 또한, EDR·NDR 연계를 통해 단말 및 네트워크 보안 체계를 강화하고, 위협 탐지 및 빠른 대응을 가능하게 하는 체계를 마련하여 금융 보안 사고를 예방하고 신뢰할 수 있는 서비스 운영 환경을 조성하고자 하였습니다.

프로젝트 기간

2023년 12월 ~ 2024년 04월

Concept map(개념도)



Solution(구축 내용)

금융 보안 강화를 위한 통합 보안 관제 체계 구축

광주은행은 금융권의 사이버 위협 대응 역량을 강화하고, 보다 안정적인 금융 서비스를 제공하기 위해 SIEM 기반의 통합 보안 관제 체계를 구축하였습니다. 이번 사업을 통해 FCTI 연계를 강화하여 금융권에 특화된 위협 정보를 실시간으로 수집·분석하고, 사이버 공격에 대한 대응력을 향상하였습니다.

기존에는 각종 보안 솔루션이 독립적으로 운영되면서 보안 이벤트 간의 연관 분석이 어려웠고, 대응 체계가 분산되어 신속한 조치가 제한적이었습니다. 이를 개선하기 위해 광주은행의 금융 IT 인프라 전반에서 발생하는 로그를 SIEM을 통해 통합 수집하고, FCTI 연계를 통해 최신 금융 보안 위협 정보를 실시간으로 반영하는 체계를 구축하였습니다. 또한, EDR·NDR을 통해 단말 및 네트워크에서 발생하는 위협을 분석하여, 금융 서비스 보호 수준을 한층 강화하였습니다.

이번 구축을 통해 광주은행은 보안 위협 탐지 및 대응 역량을 강화하고, FCTI 및 EDR·NDR 연계를 통한 금융권 맞춤형 보안 체계를 구축하여 보다 안전한 금융 서비스를 제공할 수 있는 기반을 확보하였습니다.

Benefit(도입 효과)

금융권 맞춤형 보안 관제 체계를 구축하여 사이버 위협 대응 역량 강화

광주은행은 디지털 금융 환경에서 보안 위협이 지속적으로 증가함에 따라, 금융 서비스의 안전성과 고객 신뢰도를 높이기 위해 통합 보안 관제 체계를 구축하였습니다. 금융권은 국내외 규제 준수뿐만 아니라, 고객의 민감한 금융 데이터를 보호하기 위한 강력한 보안 체계를 요구받고 있으며, 이에 대응하기 위해 보다 정교하고 체계적인 보안 운영이 필수적입니다.

이번 구축을 통해 SIEM을 기반으로 광주은행의 금융 IT 인프라 전반에서 발생하는 보안 로그를 중앙에서 통합 관리하고, FCTI 연계를 통해 금융권 특화된 위협 정보를 실시간으로 반영할 수 있도록 최적화하였습니다. 또한, EDR·NDR 연계를 통해 단말과 네트워크 보안 체계를 강화하고, 금융 시스템 내 위협 요소를 종합적으로 분석하여 선제적인 대응이 가능하도록 개선되었습니다. 보안 이벤트에 대한 가시성을 확보하고, 금융권에서 빈번하게 발생하는 특정 위협 유형을 보다 신속하고 정밀하게 분석할 수 있는 환경을 마련하였습니다.

이번 사업을 통해 광주은행은 급변하는 금융 보안 환경에 선제적으로 대응할 수 있는 역량을 확보하고, 금융권의 보안 규제 요구사항을 충족하며, 장기적으로 보안 운영의 신뢰성과 효율성을 높일 수 있는 기반을 마련하였습니다. 이를 통해 보안 사고를 예방하고, 금융 서비스의 연속성을 보장하는 체계를 확립하였습니다.

요약

1. ESM의 한계를 극복하는 차세대 관제시스템 SIEM 도입을 통한 금융권 맞춤형 보안 관제 체계 구축
2. 기 운영시스템의 한계를 극복하고 관제 업무 연속성을 위한 3단계 완벽한 전환 구축 수행
3. 기존 미 연동 장비 및 EDR/NDR 로그 수집으로 분석 범위 확대 및 고도화