농협정보시스템

농협정보시스템 (23년)

농협정보시스템 통합보안관제 고도화 사업

고객사 소개

농협정보시스템은 농협중앙회, 지역농협, 농협계열사, 농림수산 관련기관, 시중 금융기관 등의 시스템 개발, 시스템 유지보수 사업을 영위하는 농협중앙회의 자회사로 범농협에 대한 정보화 사업을 효과적으로 지원하고, 농업·농촌 정보화를 위한 사업에 앞장서는 경쟁력 있는 IT전문회사입니다.

구축 제품 및 서비스

eyeCloudXOAR v4.0 – SIEM
(통합보안분석솔루션)

eyeCloudXOAR v4.0 – SOAR
(통합보안대응솔루션)

Background(도입 배경)

농협정보시스템은 금융·유통·경제 분야의 IT 인프라를 운영하며, 보안 위협이 금융 서비스의 안정성과 고객 신뢰도에 직접적인 영향을 미치는 환경에서 보다 정밀한 보안 관제 체계를 구축할 필요성이 있었습니다. 기존의 보안 시스템은 개별적인 위협 분석과 대응에 초점을 맞추고 있었으나, 실시간 탐지 및 연계 분석 부족으로 인해 복합적인 보안 위협에 대한 대응이 지연되는 문제가 있었습니다.

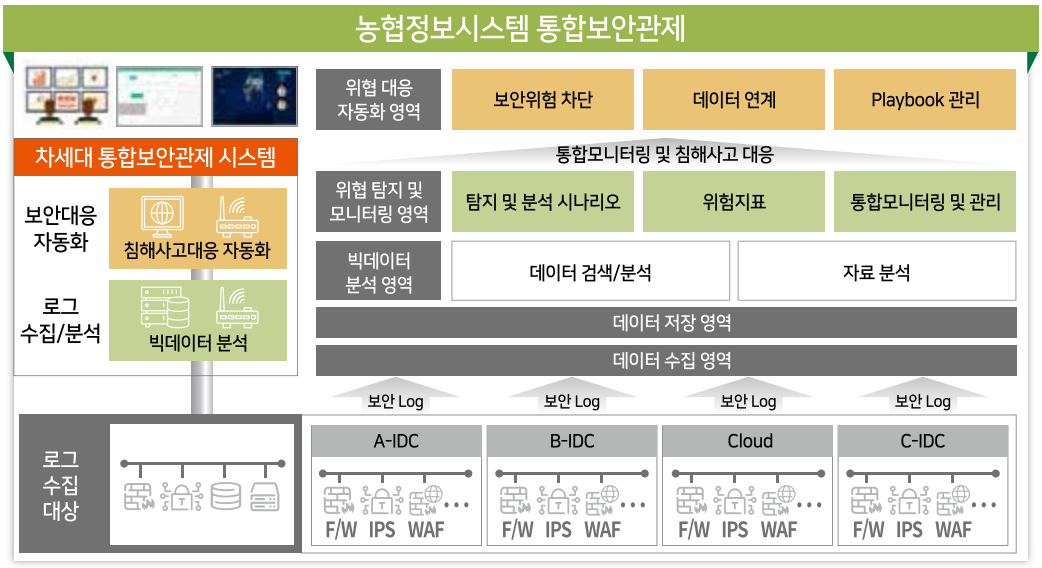
농협IDC는 농협 계열사 및 외부 고객에게 IT 서비스를 제공하는 중요한 역할을 담당하고 있습니다. 기존 보안 시스템의 취약성으로 인해 고객 정보 유출 및 시스템 장애 등의 문제가 발생할 경우 고객 만족도가 크게 저하될 수 있기에 농협정보시스템은 SIEM을 통해 시스템 전반의 보안 로그를 통합 분석하여 위협 요소를 사전에 탐지하고, SOAR을 도입해 금융거래 및 내부에서 발생하는 보안 이벤트에 대한 자동화된 대응 체계를 마련하였습니다.

이를 통해 거래 데이터를 보호하고, 보안 이벤트 대응을 단순 경보 수준이 아닌 유기적인 분석과 조치가 가능한 체계로 개선하여 금융 서비스의 연속성과 신뢰성을 한층 강화할 수 있었습니다.

프로젝트 기간

2022년 12월 ~ 2023년 06월

Concept map(개념도)



Solution(구축 내용)

차세대 보안 위협 대응을 위한 빅데이터 기반 통합보안관제 체계 구축

농협정보시스템은 최신 해킹 및 침해사고에 대한 대응력을 강화하고, 보안 관제 시스템을 현대화하기 위해 차세대 통합보안관제시스템을 구축하였습니다. 이번 사업을 통해 빅데이터 분석 기술을 활용한 실시간 보안 로그 수집·분석 체계를 마련하고, 자동화된 위협 탐지 및 대응 시스템을 도입하였습니다.

기존 보안 환경에서는 대량의 보안 이벤트를 개별적으로 분석해야 했으며, 실시간 탐지 및 대응 체계가 부족하여 위협 대응 속도가 저하되는 한계가 있었습니다. 이를 개선하기 위해 일일 평균 80GB 이상의 로그를 실시간으로 수집·분석할 수 있도록 빅데이터 기반 아키텍처를 도입하고, 실시간 분석을 통해 탐지 성능을 향상시켰습니다.

또한, SOAR을 활용한 자동화 대응 체계를 구축하여 보안 이벤트 탐지 후 즉각적인 대응이 가능해졌으며, 플레이북 기반의 위협 대응 프로세스를 적용하여 보안 정책 자동 반영 및 차단 프로세스를 최적화하였습니다.

농협정보시스템의 금융 IT 환경에 맞춰 내부망 및 외부 거래망에서 발생하는 보안 이벤트를 구분하여 분석할 수 있도록 시스템을 설계하였으며, 특화된 위협 인텔리전스(TI) 데이터를 활용하여 위협 대응력을 높이고, 금융권 특성에 맞는 보안 정책을 최적화하였습니다.

Benefit(도입 효과)

금융 IT 환경에서의 안전성과 운영 효율성의 극대화

농협정보시스템은 급변하는 금융 IT 환경에서 발생하는 다양한 보안 위협에 선제적으로 대응하기 위해 통합보안관제시스템을 혁신적으로 고도화했습니다. 이번 사업을 통해 보안 이벤트 탐지, 분석, 대응 전 과정이 자동화되고 실시간 보안 운영 효율성 및 대응 속도가 획기적으로 향상되었습니다.

기존 수작업으로 이루어지던 보안 이벤트 분석 및 대응 프로세스가 자동화됨에 따라, 실시간 탐지된 위협에 즉각적인 대응이 가능해 졌으며, 특히, SOAR 기반의 대응 자동화를 통해 방화벽 정책을 갱신하고, 금융 거래망에서 탐지된 위협을 신속하게 대응함으로써 고객 정보 및 금융 서비스 보호 수준을 대폭 강화했습니다. 또한, 내·외부망 보안 이벤트를 구분하여 분석하는 체계를 도입함으로써 금융 IT 시스템의 보안 운영이 더욱 정밀해졌으며, 외부 침입 탐지 및 대응 역량이 강화되었습니다.

금융 규제 준수를 위한 로그 보관 및 감사 체계를 정비하여, 보안 감사 및 사고 분석 과정의 효율성을 증대했으며, 보안 이벤트 분석의 정확도와 대응 속도를 향상시켜 금융서비스의 안전성을 강화 하였습니다.

이번 통합보안관제 고도화 사업을 통해 농협정보시스템은 더욱 안전하고 효율적인 금융 IT 환경을 구축하여 고객에게 신뢰받는 금융 서비스를 제공할 수 있게 되었습니다.

요약

1. 차세대 통합보안관제 시스템의 침해사고 대응 자동화 기능을 통해 보안위협에 대한 실시간 자동 대응위협 헌팅, 식별, 등록 등 공동대응 프로세스 고도화
2. IDC 및 범농협 계열사 IT전산인프라의 침해사고대응 체계 강화
3. 금융 규제 준수를 위한 로그 관리 및 감사 체계 정비로 보안 운영 신뢰성 확보