한국거래소 (23년)

지능형 사이버공격 대응역량 강화를 위한 통한보안관리시스템 재구축

고객사 소개

한국거래소는 증권 및 파생상품 등의 공정한 가격 형성과 원활한 매매 및 효율적 시장관리를 목적으로 설립된 기관입니다. 부산 본청과 서울 사옥 지역적 분리된 영역과 인터넷망, 업무망 환경적으로 분리된 영역에 통합보안관리시스템을 재구축하여 디지털 전환 가속에 의한 신·변종 지능형 사이버 공격 대응 역량을 강화 하였습니다.

구축 제품 및 서비스

eyeCloudXOAR v4.0 - SIEM
(통합보안분석솔루션)

eyeCloudXOAR v4.0 - SOAR
(통합보안대응솔루션)

Background(도입 배경)

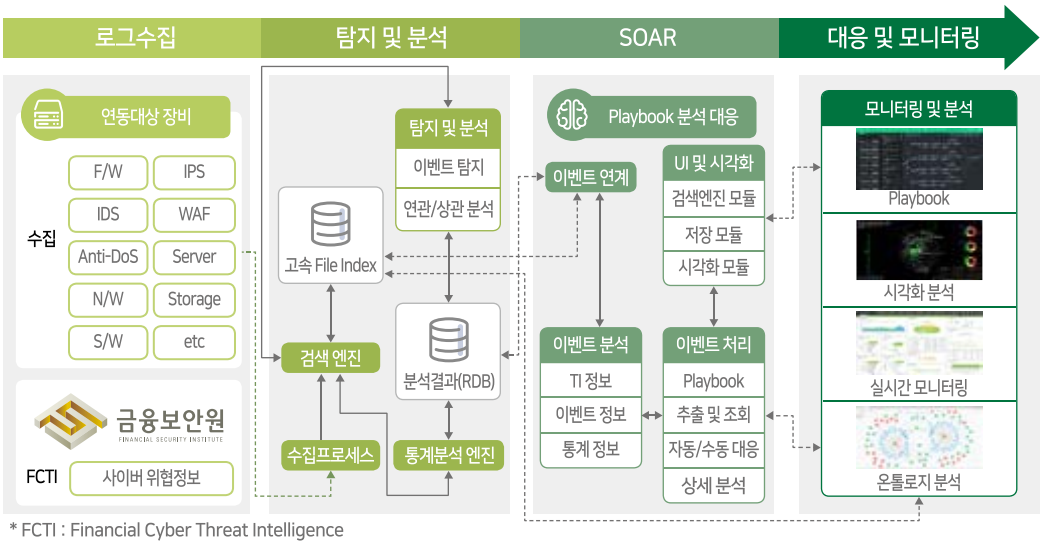
날로 지능화되고 다양한 공격 기법의 빈도와 양이 빠르게 증가하고 있어, 단일 서버에서 단일 이벤트 처리만 가능한 기존의 보안관제시스템으로는 이러한 신종 사이버 위협 분석과 대응이 불가하게 되었습니다. 따라서 한정된 인력으로 폭증하는 사이버공격에 정확하게 분석하기 위해서는 로그 수집 대상과 범위를 확대해야 하며, 방대한 데이터를 신속하고 대응하기 위해서는 분산 처리 기반의 데이터 수집 및 분석 플랫폼 구축이 필요했습니다.

한국거래소는 성능과 기능이 검증된 솔루션으로 시스템을 재구축하기 위해 시큐레이어의 eyeCloud XOAR SIEM과 SOAR 제품을 선택하였습니다. 독보적 자체 데이터 분산처리 기술, 정확하고 일관된 하이브리드 분석, 유연한 복합 시나리오 분석 기능 등 그 성능과 기능이 검증된 솔루션으로서 40TB/일의 국내 최대의 일일 데이터 처리 사이트와 해당 분야에서 가장 많은 구축 경험을 보유한 솔루션을 선정하였습니다.

프로젝트 기간

2023년 04월 ~ 2023년 08월

Concept map(개념도)



* FCTI : Financial Cyber Threat Intelligence

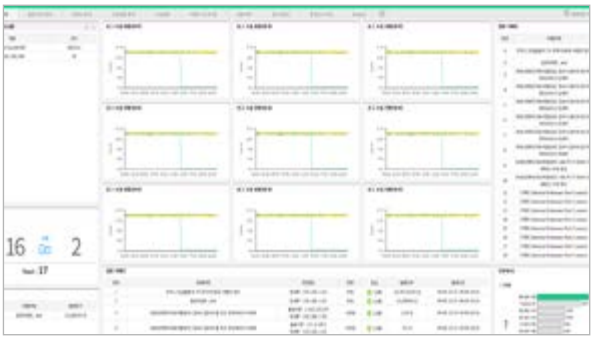
Solution(구축 내용)

한국거래소는 보안관제를 위해 보안장비 및 정보시스템 약 300여대를 연동하여 일일 약 300GB의 데이터를 수집하며 한국거래소에 특화된 업무처리 플레이북과 금융보안원의 FCTI 위협정보를 활용하여 SOAR 기반의 업무 대응체계를 구축하였습니다.

중요 정보 모니터링을 위한 다양한 대시보드를 구성하여 운영중이며, 개인별 업무 특성에 맞는 대시보드를 통해 업무에 활용하고 있습니다.

종합대시보드

성능 모니터링 대시보드



Benefit(도입 효과)

알려진 보안 위협의 루틴과 특징을 추출하여 이벤트로 등록하고, 이벤트 발생 시 정보를 즉시 식별할 수 있습니다. 또한 자동화를 통해 기존보다 다양한 신규 위협을 식별하고 침해 분석 및 대응 범위를 확장하여, 새로운 패턴과 위협을 신속하게 파악하고 대응할 수 있습니다.

금융보안원 위협정보(FCTI) 연동을 통해 다양한 기관과 신규 위협의 지속적인 공유를 통해 더욱 강력한 보안 네트워크를 구축하고 있으며, 보안관리 업무의 처리시간을 기존 대비 1/6로 단축하여, 신규 위협에 더욱 빠르게 대응할 수 있게 되었습니다.

요약

1. 3세대 ESM 수집범위, 성능한계를 극복하는 4세대 SIEM 및 SOAR 구축
2. FCTI의 위협정보기반 상관분석을 통해 선제적인 금융보안위협 대응
3. 보안관제뿐만 아니라 장애성능 모니터링시스템 구축