OOOO반도체

OOOO반도체 (21년)

내부 시스템 이용 내역 가시화로 정보유출 위험에 대한 즉각적인 대응체계 구축

고객사 소개

OOOO반도체는 통신, IoI 가전, 산업, 자동차 등의 애플리케이션에 탑재되는 아날로그 및 혼성 신호 반도체를 설계 생산하는 기업입니다.

구축 제품 및 서비스

eyeCloudXOAR v4.0 - SIEM (통합보안분석솔루션)

eyeCloudXOAR v4.0 - SOAR (통합보안대응솔루션)

eyeCloudXOAR v4.0 - UEBA (이상행위분석솔루션)

Background(도입 배경)

다양한 형태의 기술 유출 위험에 대해 다각적인 탐지 및 분석이 가능한 시스템이 필요하였고 각의 보안 시스템들의 데이터 통합 관리 및 모니터링이 가능한 시스템을 찾고 있었습니다. 특히, 보안시스템과 내부 업무시스템간의 상관 분석을 포함한 다양한 이벤트 설정 및 탐지 기능이 필수 요소 였습니다. 검토한 보안 시나리오 외에도 솔루션 제안사가 정보유출이 일어날 수 있는 다양한 시나리오를 도출하여 지원해 주었으면 하는 요건으로 향후 연동 대상 시스템이 추가될 경우에도 장비 연동이 수월하고 관리방안에 대한 지원도 보장되어야 했습니다.

Reason for selection(선정 사유)

이상징후 탐지 시나리오를 도출하여 여러 이벤트를 설정하고, 사용자 별 발생한 이벤트 내역이 가시회 되어 이상징후 발생 시 신속한 원인 규명이 가능해 졌습니다. 도입 후, 정보 유출 방지를 위한 대책이 보완되어 보다 안심이 되는 바이며 내부 정보유출 방지를 포함한 전사적 보안관리를 All-in-One으로 구축하려는 기업이 있다면, eyeCloudXOAR 도입을 적극 추천 합니다.

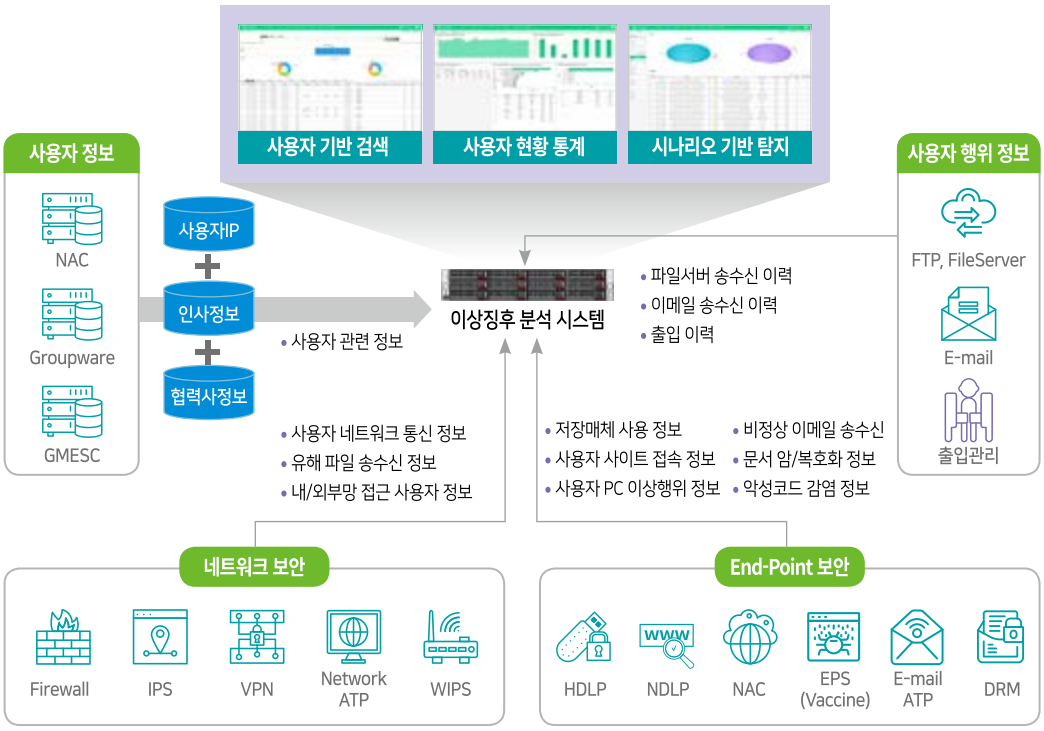
프로젝트 기간

2021년 09월 ~ 2021년12월

Solution(구축 내용)

기본적으로, 수집되는 로그와 인사 관련 정보를 연관 분석하여 모든 데이터의 사용자를 식별하도록 하였습니다. 여러 서버 장비, 엔드포인트, 휴대용 저장매체, 내/외부망 네트워크로 송수신되는 모든 데이터에 의해 사용자 기반으로 검색 할 수 있도록 하였으며 각 사용자의 사용내역에 대한 통계를 시각화함으로써 보안사고에 철저히 대비 할 수 있는 기반을 마련하도록 구축 하였습니다. 모든 시스템의 데이터 가능하도록 하여 다양한 위협에 신속히 대응하도록 하였습니다. eyeCloudXOAR는 다양한 위협 요소에 대응할 수 있도록 매우 정교하고 다양한 패턴의 이벤트 설정이 가능합니다. 각각의 탐지 시나리오를 이벤트로 등록하여 해당 이벤트가 탐지될 시 사용자 정보를 바로 식별할 수 있도록 구현 하였습니다. 또한 전 용 대시보드 기능으로 특정 사용자 기준으로 발생한 이벤트를 한번에 확인할 수 있게 하였습니다.

Concept map(개념도)



Benefit(도입 효과)

시큐레이어가 구축한 이상징후 탐지 시스템을 사내에도 주의환기 시키고, 사용자별 이벤트 발생 내역이 가시화 되었습니다. 정보 유출 위협 발생시 표준화된 대응 프로세스대로 상당부분 자동으로 처리되고 담당자에 의한 처리 후 보고서 작성까지 일련의 프로세스를 깔끔하게 끝낼 수 있게 되어 업무가 훨씬 수월해 졌습니다.

그리고 무엇보다도 정보 유출 방지에 대한 체계 정립과 후속조치 대책이 투명해져서 안심이 됩니다. 보안 대응 티켓 관리 및 자동화와 이상징후 탐지를 All-in-One으로 구축하려는 기업이 있다면 eyeCloudXOAR를 도입을 적극 추천 합니다.

요약

1. 수집되는 로그와 인사 관련 정보를 연관분석하여 모든 데이터의 사용자를 식별
2. 각 시스템 주요 로그와 사용자 정보를 통한 행위 데이터 기반 분석 환경 구성
3. 업무 분석과 협의를 통한 사용자 이상행위 탐지 시나리오 도출