



한국동서발전(주) (23년)

차세대 보안관제 업무 자동화시스템 구축

고객사 소개

한국동서발전은 정부의 전력산업구조개편 정책에 따라 지난 2001년 한국전력공사로부터 분리·발족한 발전회사입니다.
당진 화력을 핵심발전소로 하여 울산화력, 호남화력, 동해화력, 일산열병합 등 전국에 모두 6개의 발전소를 운영하고 있습니다.

구축 제품 및 서비스

eyeCloudXOAR v4.0 - SIEM
(통합보안분석솔루션)

eyeCloudXOAR v4.0 - SOAR
(통합보안대응솔루션)

Background(도입 배경)

2016년 시큐레이어의 통합로그관리시스템 eyeCloudSIM v2.5, 침해사고대응시스템 BlueBird가 노후화되어 데이터 처리 및 분석에 제약이 따르게 되었습니다.

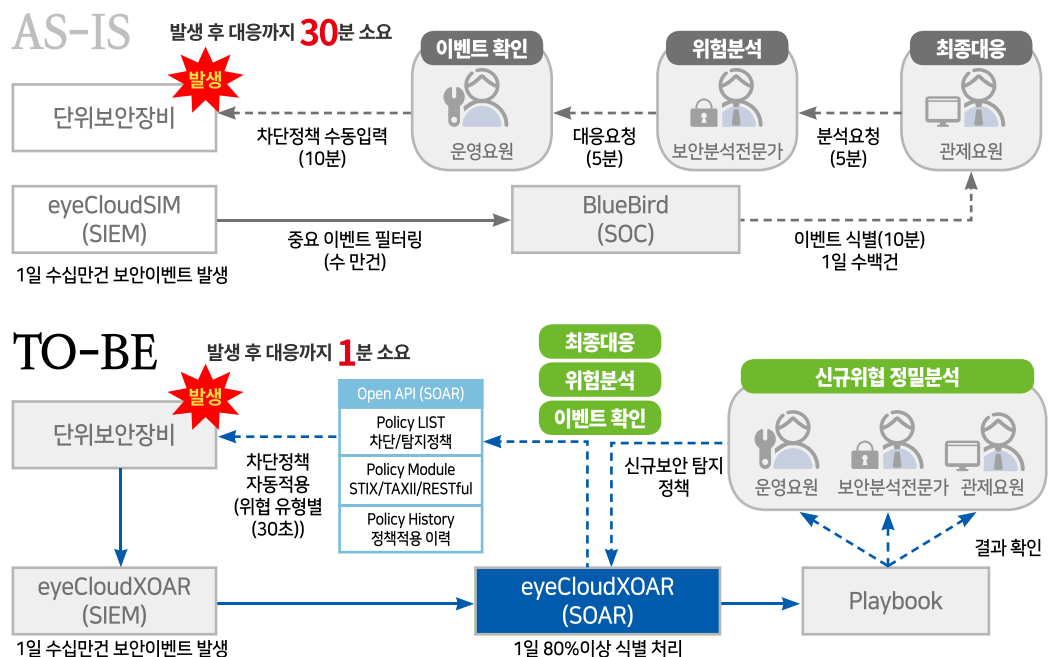
이에 따라 증가하는 로그 수집량에 대응하기 위한 시스템 증설과 티켓 업무자동화 처리 시스템 도입 계획을 수립하였습니다.

기존 제품과 연계성, 보안관제업무 무중단 이관 환경 등을 고려하여 시큐레이어의 eyeCloudXOAR v4.0 제품을 선정, 구축하였습니다.

프로젝트 기간

2023년 07월 ~ 2023년 12월

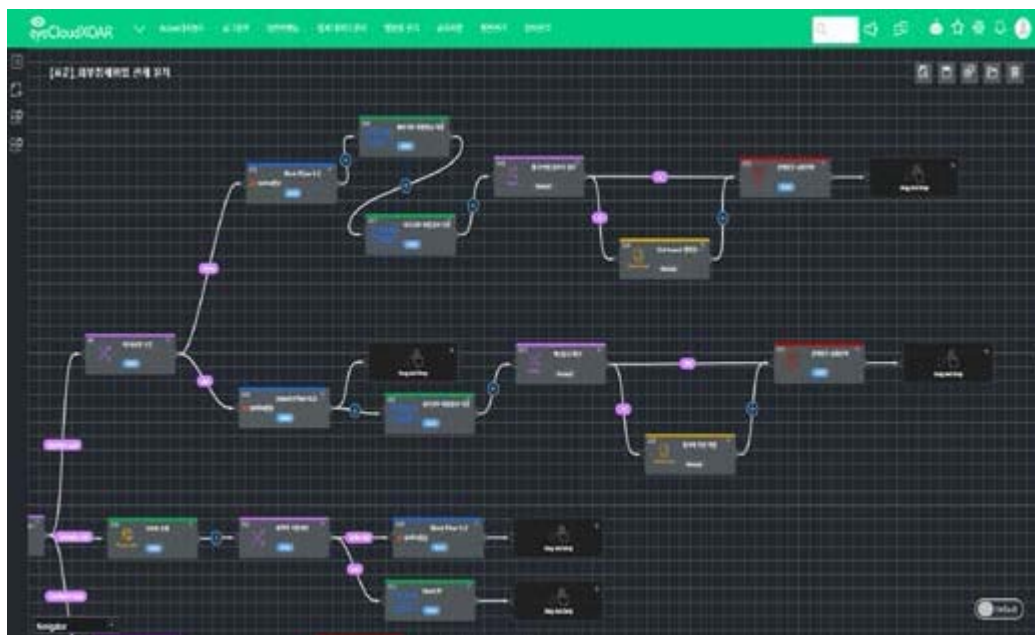
Concept map(개념도)



Solution(구축 내용)

기존 eyeCloudSIM 연동장비 이관과 신규 도입장비 연동을 통해 보안장비, 서버 등 약 100식 연동하였으며, 일일 100GB, 약 3억건 로그를 수집 분석할 수 있는 시스템을 구축하였습니다.

업무 자동화 플레이북 구현을 통해 일일 보안위협 평균 50건 자동 대응합니다.



Benefit(도입 효과)

기존의 수동관제 업무포털(SOC)의 작업 방식에서 벗어나 플레이북을 도입함으로써 위협 대응 업무를 자동화하였습니다.

이 사업으로 보안 담당자가 동일한 최적의 대응 프로세스를 따르게 함으로써 개인의 역량 차이에 관계없이 대응 품질이 일정 수준 이상으로 상향 평준화되는 결과를 가져올 수 있었습니다.

특히 PALOALTO 방화벽과의 차단 연동을 통해 보안 대응 시간이 기존 30분에서 1분 이내로 대폭 단축되었다는 점은 주목 할만 합니다.

또한 각 사례별 대응 상황을 가시화하여 실시간으로 모니터링하고 체계적으로 관리할 수 있게 되었습니다.



요약

1. 시큐레이터 eyeCloudSIM v2.5에서 eyeCloudXOAR v4.0 업그레이드 구축
2. 수동기반 SOC에서 표준화, 자동화 보안업무절차 플레이북 적용
3. 팔로알토방화벽 차단연동을 통해 보안대응시간 단축(기존 30분 → 1분 이내)