한국남부발전(주) (24년)

인공지능기반 보안관제시스템 고도화

고객사 소개

한국남부발전은 2001년 한국전력공사에서 분리되어 설립된 발전 전문 공기업입니다. 부산에 본사를 두고 있으며, 하동, 신인천, 부산, 남제주 등 전국 각지에 발전소를 운영하며 국민들에게 안정적으로 전기를 공급하고 있습니다. 석탄, LNG, 유류 뿐 아니라 풍력, 태양광과 같은 신재생에너지를 활용하여 전기를 생산하고 있으며, 친환경 에너지 개발에도 적극적인 기관입니다.

구축 제품 및 서비스

- eyeCloudXOAR v4.0 – SIEM (통합보안분석솔루션)
- eyeCloudXOAR v4.0 – SOAR (통합보안대응솔루션)

Background(도입 배경)

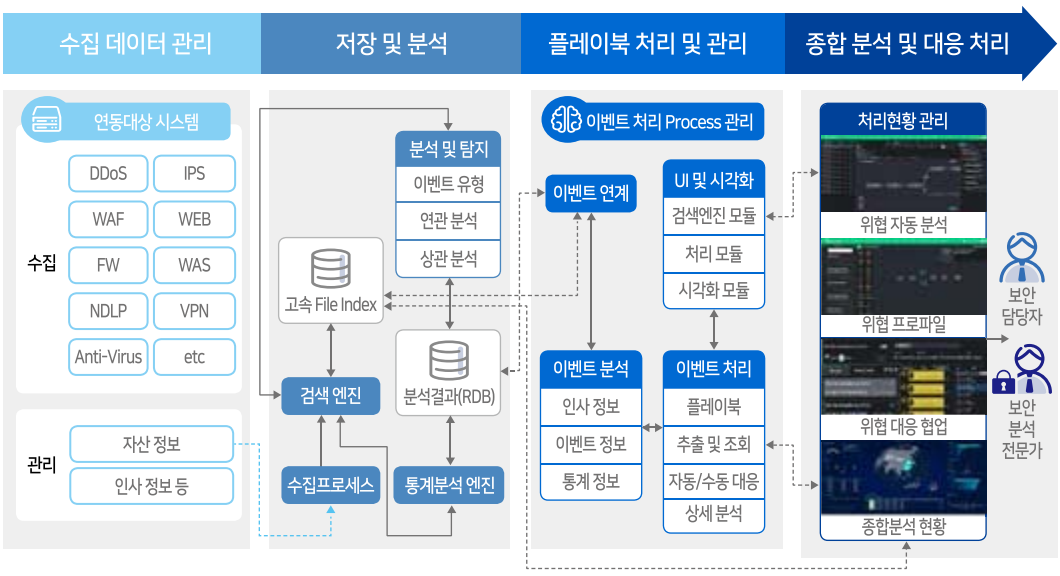
한국남부발전은 국가 주요 기간산업인 에너지 공급망을 운영하는 기관으로, 사이버 위협이 가중되는 환경에서 발전소 및 에너지 관리 시스템의 보안성을 높이고, 안정적인 전력 공급을 유지하기 위해 통합보안관제시스템을 구축 하였습니다. 기존 보안 체계는 개별 시스템 중심으로 운영되면서 전력 인프라에 대한 위협을 종합적으로 분석하고 대응하는 데 한계가 있었으며, 주요 설비와 IT 인프라에서 발생하는 보안 이벤트를 실시간으로 감지하고 대응할 수 있는 체계적 시스템이 요구되었습니다.

한국남부발전은 이번 사업을 통해 국가 기간산업의 보안성을 한층 높이고, 사이버 위협에 대한 대응력을 강화하여 지속 가능한 전력 공급과 안전한 에너지 운영 환경을 유지할 수 있는 기반을 마련하였습니다.

프로젝트 기간

2024년 12월 ~ 2025년 01월

Concept map(개념도)



Solution(구축 내용)

국가 에너지 인프라 보호를 위한 통합 보안 관제 체계 구축

한국남부발전은 국가 주요 기간산업인 에너지 생산 및 공급망을 보호하고, 사이버 위협에 대한 대응력을 강화하기 위해 SIEM 및 SOAR 기반의 통합보안관제시스템을 구축하였습니다.

이번 구축을 통해 발전소 및 주요 운영 시스템에서 발생하는 보안 로그를 SIEM을 활용하여 중앙에서 통합 관리하고, 주요 설비 및 원격지 발전소에서 발생하는 보안 이벤트를 실시간으로 분석할 수 있도록 보안 관제 체계를 고도화하였습니다.

또한, SOAR을 활용하여 보안 이벤트 발생 시 자동화된 분석 및 대응 프로세스를 구축하여 보안 운영 효율성을 극대화하였습니다. 탐지된 위협에 대해 즉각적인 대응이 가능하도록 보안 정책을 자동으로 업데이트하고, 발전소 운영에 영향을 주지 않도록 보안 관제 프로세스를 최적화하였습니다.

운영 측면에서는 보안 로그의 장기 보관 및 분석 기능을 강화하여, 발전소 및 원격지 설비에서 발생하는 이상 행위를 보다 정밀하게 분석할 수 있도록 개선하였습니다. 또한, 국내외 에너지 보안 규제 준수를 위한 감사 체계를 정비하여, 국가 주요 인프라 운영 기관으로서의 보안 관리 역량을 한층 강화하였습니다.

Benefit(도입 효과)

국가 에너지 인프라 보호 및 사이버 보안 대응 역량 강화

한국남부발전은 국가 기간산업의 핵심인 전력 생산 및 공급망을 안정적으로 운영하기 위해 통합보안관제시스템을 구축하였습니다. 발전소 및 에너지 관리 시스템은 국가 기반시설의 핵심 요소로, 사이버 공격이 발생할 경우 물리적 피해와 전력 공급 차질로 이어질 위험이 높습니다.

이번 구축을 통해 한국남부발전은 발전소 및 원격지 설비에서 발생하는 모든 보안 로그를 중앙에서 통합 관리하고, 보안 이벤트를 실시간으로 분석할 수 있는 체계를 마련하여 보안 관제의 일관성을 확보하고, 전력망 보호를 위한 통합적 대응 체계를 마련하였습니다.

또한, SOAR 기반의 보안 자동화 기능을 활용하여 발전소 운영에 영향을 주지 않으면서도 신속하게 위협을 차단할 수 있는 환경을 조성하였습니다. 이를 통해 보안 사고 발생 시 신속한 대응이 가능해졌으며, 운영 중단 없이 안전한 전력 공급이 가능하도록 보안 프로세스를 최적화하였습니다.

이번 사업을 통해 한국남부발전은 국가 에너지 인프라의 보안성을 높이고, 급변하는 사이버 보안 환경 속에서도 효율적인 보안 운영을 지속할 수 있는 체계를 마련하였습니다.

요약

1. 발전소 및 원격지 설비 보호를 위한 통합 보안 관제 체계 구축 및 실시간 위협 대응 역량 확보
2. SOAR 기반 보안 운영 자동화를 통한 위협 대응 속도 향상 및 발전소 운영 안정성 강화
3. 전력망 및 주요 에너지 설비의 보안 가시성 확보를 통한 지속 가능한 보안 운영 체계 구축