한국인터넷진흥원(KISA) (24년)-공공+민간

사이버위협 공동대응 플랫폼 구축을 위한 솔루션 도입

고객사 소개

한국인터넷진흥원(KISA) 대한민국의 인터넷 진흥, 인터넷 정보보호 및 그에 대한 국제 협력 업무를 수행하는 과학기술 정보통신부 산하 위탁집행형 준정부기관 입니다. 사회 전 분야로의 사이버 안전망 구축 확대 및 데이터 경제 활성화 기반 조성에 힘쓰고, 블록체인·5G 등의 신기술을 기반으로 한 기반시설 구축 및 혁신 서비스 발굴에도 앞장서는 인터넷 정보보호 전문기관 입니다. 이외 ICT·정보보호 산업 및 인재 육성에도 집중하고 있습니다.

구축 제품 및 서비스

eyeCloudXOAR v4.0 - SIEM
(통합보안분석솔루션)

eyeCloudXOAR v4.0 - SOAR
(통합보안대응솔루션)

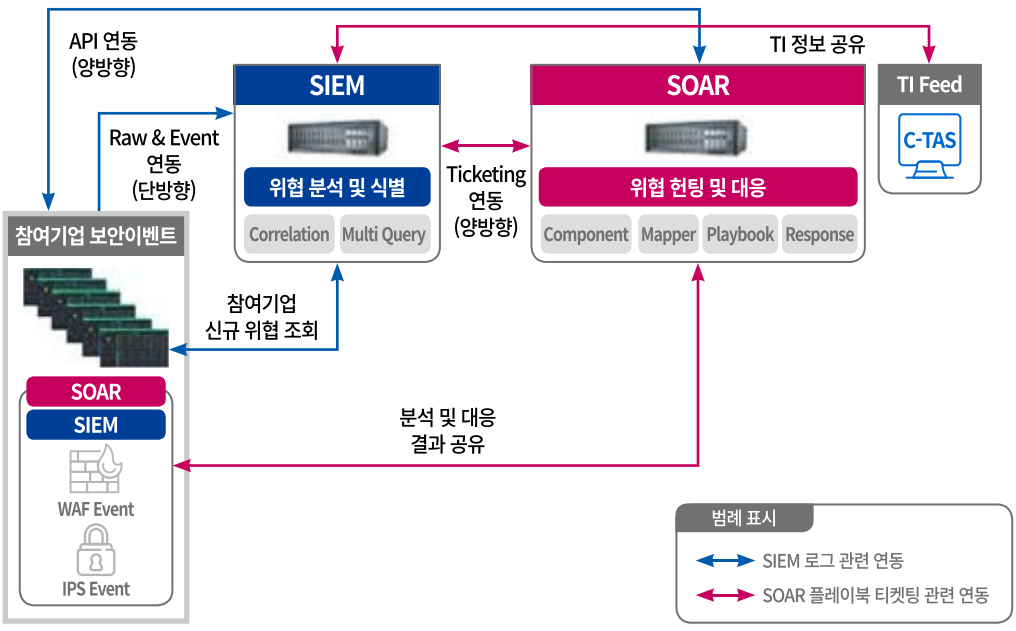
Background(도입 배경)

민간 영역에서 발생하는 사이버 위협을 실시간으로 파악하고 신속하게 대응하기 위해 참여기업(ISP, 호스팅, 원격 관제 등 7개 기업)과 함께 보안위협 탐지·분석 및 공동대응 플랫폼을 구축 사업을 진행하게 되었습니다. 이를 통해 KISA는 민간 영역에서 발생하는 사이버 위협에 대한 실시간 정보를 수집하고, 기업들이 효과적으로 대응 할 수 있도록 지원하기 위해 시큐레이어의 eyeCloudXOAR 제품을 선정하여 구축하게 되었습니다.

프로젝트 기간

2023년 07월 ~ 2023년12월

Concept map(개념도)



Solution(구축 내용)

22년부터 진행된 사업으로 3개사에서 자동화 공동대응체계를 구성하여 진행 하였으며, 24년의 경우 기존 3개사에서 추가적으로 4개가 늘어난 7개사에서 자동화 공동대응체계 구축을 통해 참여 기업 확대를 통한 위협 정보 수집 및 분석 부분이 강화 되었으며, 공동대응을 통한 프로세스의 고도화를 통해 역량 강화와 효율성이 증대 되었습니다.(위협 헌팅, 위협 식별, 위협 등록)

Benefit(도입 효과)

사이버 위협 정보의 신속한 공유로 공공기관과 민간기업 간의 정보 공유를 통해 위협을 보다 빠르게 탐지하고 대응할 수 있으며, 통합된 위협 분석을 통해 다양한 출처의 데이터를 통합하여 분석함으로써, 보다 정교한 위협 인식과 대응 전략을 수립할 수 있습니다.

자동화된 대응 메커니즘으로 AI와 빅데이터 기술을 활용하여 위협에 대한 자동화된 대응이 가능해 졌으며, eyeCloudXOAR 제품 도입을 통해 국내 사이버 보안 역량이 전반적으로 향상 될 것으로 예상됩니다.

Participation(참여 안내)

KISA에서는 다수의 사업자에게 서비스를 제공하는 실시간 위협·탐지 대응이 필요한 기업을 대상으로 매년 신규 모집을 하고 있습니다.

해당 사업에 관심이 있는 기업은 아래 KISA 담당자에게 문의 바랍니다.

• **사업 문의 :** AI위협데이터대응팀 송은지 책임(02-405-5290), 장대현 선임(02-405-5158)

요약

1. 자동화 공동대응 체계 구축을 통해 위협 정보 공유 및 분석 자동화
2. 참여 기업 확대를 통한 위협 정보 수집 및 분석 강화
3. 위협 헌팅, 식별, 등록 등을 포함한 공동대응 프로세스 고도화