



중앙행정기관 등의 정보자원 관리
및 전자정부 기반 구축을 위한
범정부 데이터 센터

대한민국, 대전
www.nirs.go.kr

국가 정보 자원 관리원은 (구, 정보 통합 전산 센터) 2005년 세계 최초의 범정부의 데이터 센터로서, 흩어져있던 전자정부 시스템을 한곳에 모으는 역할을 했습니다. 현재 정부 기관의 자료들을 한 곳에서 효율적으로 관리하고 있습니다.

다양한 기기종 장비에서 끊임없이 늘어나는 데이터와 지속되는 위협요소들의 통합 관리가 불가피해졌습니다. 이에대한 해결책으로 국가 정보 자원 관리원은 2013년 차세대 보안 관제 시스템을 구축하는것을 목표로 삼았고, 시큐레이어의 솔루션이 그 성능과 기능을 공정한 시험과정을 통해 인정받아 채택되었습니다.

시큐레이어 구축 제품 및 서비스

- eyeCloudSIM
(빅데이터 로그분석 솔루션)
- Blue Bird (SOC 포털)
- Guppy for Big Data
(장기데이터 배치분석)
- 전문인력 7명 파견

“시큐레이어의 솔루션을 도입한 뒤, 이벤트 분석에 소요된 시간이 몇시간에서 몇 분으로 현저하게 줄었습니다.

필요한 정보를 얻기위해 다른 종류의 장비에 일일이 접근하지 않아도 하나의 시스템에서 수집, 분석, 모니터링이 가능해졌기때문에 업무 효율이 굉장히 올라갔습니다.”

- nSIMS, 국가 정보 자원 관리원

프로젝트 목표

- 업무 생산성과 작업 흐름 효율성 증진
- 빅데이터 관리 시스템 통합
- 진화하는 사이버 위협에 대한 대응

프로젝트 결과 및 도입 효과

- 다양한 장비로부터 수집된 로그의 실시간 연관분석을 통해 향상된 공격 대응 능력
- 다양한 정보 자원으로부터의 로그 통합 관리
- 사이버 위협과 사고의 문맥상의 이해를 통한 행위 분석
- 연관 분석을 통해 향상된 공격 징후 탐지율
- 표준화 된 이벤트 티켓팅 시스템으로 인한 신속한 의사 결정

	nSIMS 도입 전 (2011)	nSIMS 도입 후 (2018)	
검색 성능 (1일 / 1개월)	3 시간 / 10 일	1 초 / 20 초	10,800% 증가
데이터 보관 및 분석 (6 개월)	수 십 GB	7 PB	70,000% 증가
시스템 장애 복구	1 시간	5 분	120% 증가
시스템 장애 분석	10 일	3 시간	800% 증가