INNOBIZ 기술혁신형 중소기업

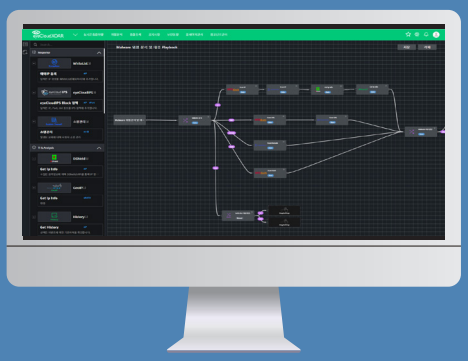
기술보증기금 벤처기업인증

SecuLayer

eyeCloudXOAR Introduction

eyeCloudXOAR

제품 소개



국내외 다양한 위협 인텔리전스 연계 활용 및
여러 보안 장비와의 정책 연동에 의한 대응 자동화로
이상적인 보안 관제 업무 환경을 실현합니다.

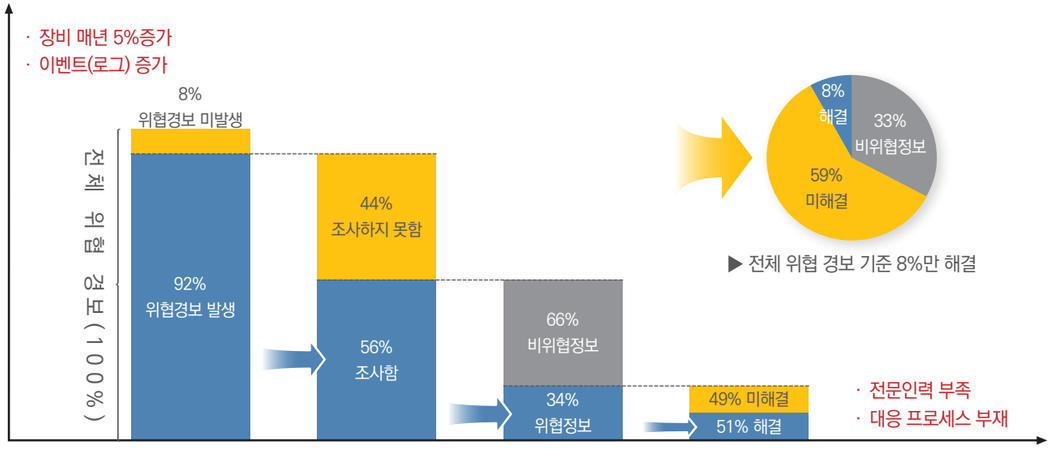
Why eyeCloudXOAR? ①

보안 관제 현실

해마다 증가하고 있는 보안 장비와 함께 점점 늘어나는 빅데이터…
하지만 전문 인력 부족, 대응 프로세스 부재로 인해 보안 환경은 나날이 취약해지고 있습니다.

보안 위협은 점점 진화하고 다양해지고 있으나, 휴먼 기반의 대응으로는 한계가 있습니다.
그리고, 기존 관제 시스템과 수 많은 보안 장비를 일일이 관리하고 활용하기는 너무나도 어렵습니다.

이와 같은 이유로, 보안 관제 환경에서 발생하는 전체 위협 경보 중에 약 8%만 해결되고 있는 것이 현실입니다.



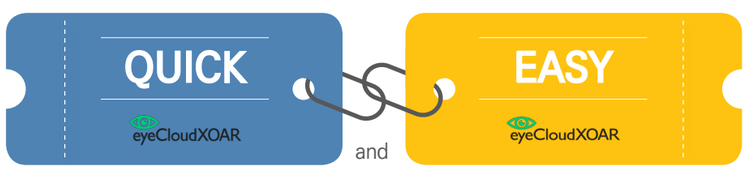
▶ 전체 위협 경보 기준 8%만 해결

*출처: CISCO 2019 연례 사이버보안 보고서

해답은 Quick & Easy

점차 늘어나는 보안 위협에 비해 부족한 대응 인력을 보완하기 위해서는
탐지, 분석, 대응 업무를 더욱 신속하게 처리하여 개별 업무량을 줄여야 합니다.

eyeCloudXOAR는 신속하고 간편한 업무 환경 실현에 중점을 둔 시스템/자동대응 기반의 SOAR 솔루션입니다.
위협 대응 프로세스의 상당 부분을 자동화하여 보안 담당자의 수고를 크게 덜어주고
기존 운용중인 보안 장비의 활용 가치를 높임으로써 보안 관제 업무 환경을 크게 개선시킬 수 있습니다.

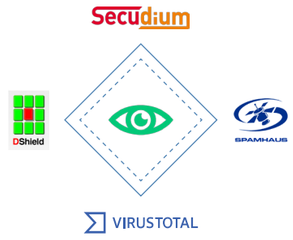


Why eyeCloudXOAR? ②

특장점

다양한 업체의 보안 장비와 정책 연동하여 (국내 최다) 위협 대응 업무의 상당 부분을 자동화!

국내 여러 보안 장비 (방화벽, WAF, IPS, TMS 등)와 연동하여 각 장비의 정책을 eyeCloudXOAR에서 직접 설정할 수 있습니다. 위협 종류별 동작 설정이 가능하고 상당 부분의 작업을 자동화 함으로써 보안 담당자는 보다 중요한 의사결정 업무 등에 집중할 수 있습니다.



국내외 여러 TI 연동 활용 및 자동화 대응으로 점차 진화하는 각종 위협에도 보다 안심하고 대응 가능!

보안 관제 서비스 분야 대표 기업인 SK인포섹의 Secudium Intelligence를 비롯하여 국내, 해외 여러 TI 및 공격/바이러스 검사 시스템과 연계되어 있어 다양한 위협에 대해 원활한 대처가 가능합니다. 또한 해당 프로세스 대부분이 자동화 처리되어 보다 쉽고 빠른 업무 처리가 가능합니다.

자체 개발한 빅데이터 처리 원천기술로 최고 속도 구현

eyeCloudXOAR의 데이터 처리 속도는 데이터 인덱싱 성능 기준만으로 1,000,000 EPS 를 발휘합니다 (장비간 데이터 전송 기준 최대 2배). 시큐레이어가 독자적으로 개발한 실시간 이벤트 수집/분석 기술, 머신러닝 기반 데이터 정형화 처리 기술로
본 제품 관련 특허만 15건 보유하고 있습니다.(2021년 1월 기준, 추가 특허 출원 중)

Parser Generator로 쉽고 빠른 데이터 정형화 가능 자체 쿼리 언어 SeQL 사용으로 다채로운 방법의 분석 가능

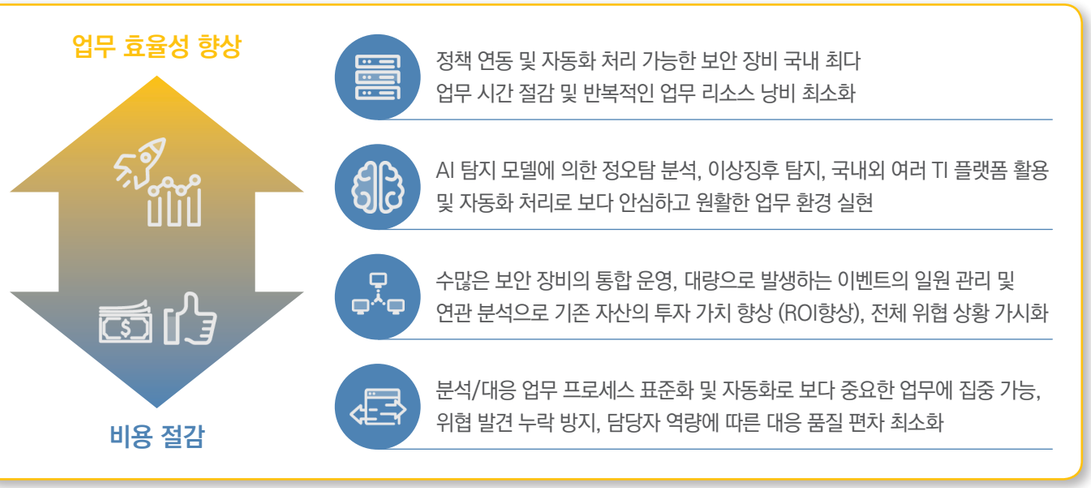
오직 시큐레이어에서만 제공하는 Parser Generator는 UI 기반 파싱 툴로써 데이터 수집, 파싱 작업의 수고를 크게 덜어주며, 장비 타입별 파싱 방법을 자동으로 추천해 주는 기능으로 데이터 정형화를 쉽고 빠르게 처리할 수 있습니다. 또한, 시큐레이어 자체 개발 쿼리 언어 SeQL은 300종 이상의 함수 및 명령어를 지원하여(지속 업데이트), 다양하고 유연한 분석을 가능하게 하며 전용 쿼리 브라우저를 통해 간편한 편집이 가능합니다.

OT, IoT분야 융복합 보안 관제 솔루션으로의 확장

미국 CLAROTY 사의 CTD (Continuous Threat Detection) 와의 연동 개발로 산업용 제어 시스템의 보안 위협 탐지 및 대응 솔루션으로 확장할 수 있습니다. 제조, 전력시설, 스마트팩토리의 보안 관제, 데이터 센터 인프라 관리 (서버, 전력, 항온, 항습 등) 등 다양한 분야의 위협 분석 및 대응이 가능합니다.

Why eyeCloudXOAR? ③

도입 효과



주요 기능 (1/2)

업무 프로세스 표준화 (Playbook)

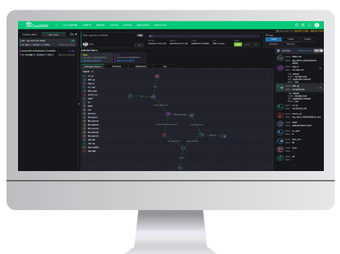
- 위협 분석/대응 업무를 플레이북으로 표준화 및 자동화하여 분석 및 대응 시간을 줄이고 담당자들이 개입이 필요한 조치에 집중할 수 있도록 지원
- 고객처별 또는 사이버안전센터 현장별로 특화된 플레이북을 쉽고 유연하게 생성 및 관리 (드래그 앤 드롭 지원)

다양한 컴포넌트 지원

- Secudium Intelligence를 비롯한 국내외 다양한 TI 및 분석시스템을 활용한 분석 컴포넌트 제공
- 여러 보안 장비가 위협 종류 또는 프로세스 별로 자동화된 동작을 수행하도록 각 장비의 정책별 컴포넌트 지원 및 설정 가능

위협 상황 가시화

- 온톨로지 분석 (Ontology Analysis)으로 복수 이벤트를 연관 분석. 이벤트, 자산명/종류, 출발지/목적지의 IP 및 포트 등 각 개체를 가시화 하여 전체 위협이 어떻게 진행되었는지 신속히 파악 가능
- 플레이북에서 위협별 대응 프로세스의 진행 상황, 컴포넌트별 자동/수동 처리 결과를 직관적으로 파악할 수 있어 업무효율 향상



Why eyeCloudXOAR? ④

주요 기능 (2/2)

AI에 의한 정오탐 분석, 이상행위 탐지

- Cyber Kill Chain 상황, KISA 위협 분석 유형, ATT&CK 분석 현황을 한 화면에서 확인 가능
- AI 모델에 의해 탐지된 이벤트에 대해 관련 이벤트 및 외부 위협 정보와의 상관 분석을 수행
- 탐지된 위협 경보를 자동 또는 수동으로 그룹화하고 대응 우선순위를 지정하여 심각한 위협 Case부터 우선 처리

3D Network Map으로 연동자산 가시화

- 서버, 네트워크 장비, End-Point장비, 보안장비 등 연동 자산을 대상으로 한 자동화 Network Topology를 가시화
- 사이버 위협의 Flow 현황, 각 연동자산의 트래픽 통계 정보 표시
- Nmap에 의한 자산 정보 및 서비스 정보 스캐닝, TraceRoute 기술을 통해 Network Topology 정보를 간편하게 생성 가능

3D Global Map으로 이벤트 현황 가시화

- 수집된 이벤트를 시간, 이벤트별로 집계하여 3D Global Map 및 차트로 시각화함으로써 전체 이벤트 현황을 한눈에 확인 가능
- 특정 국가별 집계 확인, 3D Global Map의 Zoom-In/Out 기능, 실시간 모니터링 및 특정시간 검색, 데이터 현황에 대한 Pie Chart 확인 가능

다양한 종류의 이벤트 분석 가능

- 수집 로그의 속성에 따른 자산 기반의 이벤트 분석 기능과 이벤트 분석 결과를 기초로 자산별 또는 그룹별 위험도 산출 기능 제공
- 장애별, 유해IP별, 상관분석별로 자유로운 이벤트 설정 및 알람기능 제공
- 시큐레이어의 관제 및 고객지원 이력데이터를 활용한 주요 레퍼런스 이벤트의 자동 업데이트 가능

Customer

금융, 공공기관, 국방 포함 약 200+ 고객기업

국가정보자원관리원 책임운영기관

> 시큐레이어의 제품에서 지원하는 다양한 데이터 연계 기능을 활용하여 기업 내 인사DB 및 자산 정보, 사용자 정보를 모두 통합하여 보안 위협에 대한 시나리오를 완성하였으며 그 과정에서 **시큐레이어의 헌신적인 엔지니어링과 커스터마이징 지원**을 경험한 바가 있습니다.

NICE

> 필요한 정보를 얻기 위해 다른 종류의 장비에 일일이 접근하지 않아도 **하나의 시스템에서 수집, 분석, 모니터링이 가능**해졌기때문에 업무 효율이 굉장히 올라갔습니다.

PIOLINK

> 기존 로그 관리 시스템 또는 보안 관제 시스템이 갖고 있는 **기술적 한계를 뛰어넘는 국내 최우수 제품**으로, 다양한 통계 분석과 사용자 중심의 인터페이스, 고속의 데이터 처리 성능을 바탕으로 **다양해져 가는 고객의 요구사항에 대응하는 우수한 성능과 기능을 제공**합니다.

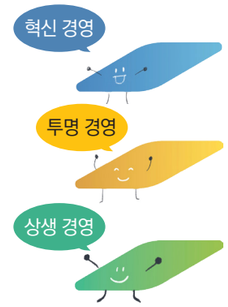
IBK 기업은행

> 시큐레이어 솔루션은 **검색 성능이 탁월하고 이벤트 수집과 심층분석이 원활**합니다. **도입 후 통합보안관제시스템 운영 효율이 크게 향상**되었습니다.

About SecuLayer

개요

회사명	(주)시큐레이어	**대표자**	전주호
설립일	2012년 02월 01일	**종업원수**	86명 (2020.11)
업종	소프트웨어 개발 및 공급		
사업내용	· 통합 보안 관리 소프트웨어 개발 및 공급 · 정보화시스템 기획 / 개발 / 유지보수 · 공공기관 침해사고 예방 대응 및 서비스		
주소	서울시 성동구 성수일로 4길 25, 서울숲코오롱디지털타워 14층	**대표전화**	070-4603-7320
		팩스	02-499-7605



Core Value of SecuLayer

사업분야

통합 보안 관제
- ICS & OT 융복합 보안
- SIEM, SOAR, FOAR 솔루션
  - 위협 분석 및 대응
  - 프로세스 설정 및 자동화

네트워크 계층별 데이터 수집/분석
- 네트워크/시스템별 데이터 수집, 분석
  - 침입 탐지 및 방어 솔루션
  - IT 자산 관리 솔루션

인공지능 플랫폼 사업
- 기계학습 기반 플랫폼
  - 보안 정보 취합, 실시간 분석
  - 장애 예측 및 사용자 지정 모델 생성

빅데이터 플랫폼 사업
- 빅데이터 분석/처리 플랫폼
  - 실시간 고속 검색, 장기 데이터 분석
  - 하둡 에코시스템과 솔루션의 모든 기능을 통합, 단일 제품으로 제공

수상 / 인증 / 특허

	건수	내용
표창장	4	· 행정자치부장관 표창 3건 · 제7회 대한민국 사랑받는 기업 (중소벤처기업부장관상)
상장	2	· ICT 특허경영대상 은상 · 제2회 대한민국SW품질대상 eyeCloudSIM 최우수상
인증	13	· CC인증 6건 · GS인증 7건
선정	5	· 기술혁신형 중소기업 (Inno-Biz) · 벤처기업확인서 · 청년친화강소기업선정서 – 임금/일생활균형/고용안정 우수 · 직접생산확인증명서 · 청년스마트 중소기업 일자리 선정서
특허	27	· 빅데이터, 사이버보안, 인공지능 분야 국내 25건, 해외 2건

eyeCloudXOAR

제품문의

SecuLayer

서울시 성동구 성수일로 4길 25
서울숲코오롱디지털타워 14F

TEL 070-4603-7320 | FAX 02-499-7605
http://www.seculayer.com | info@seculayer.com