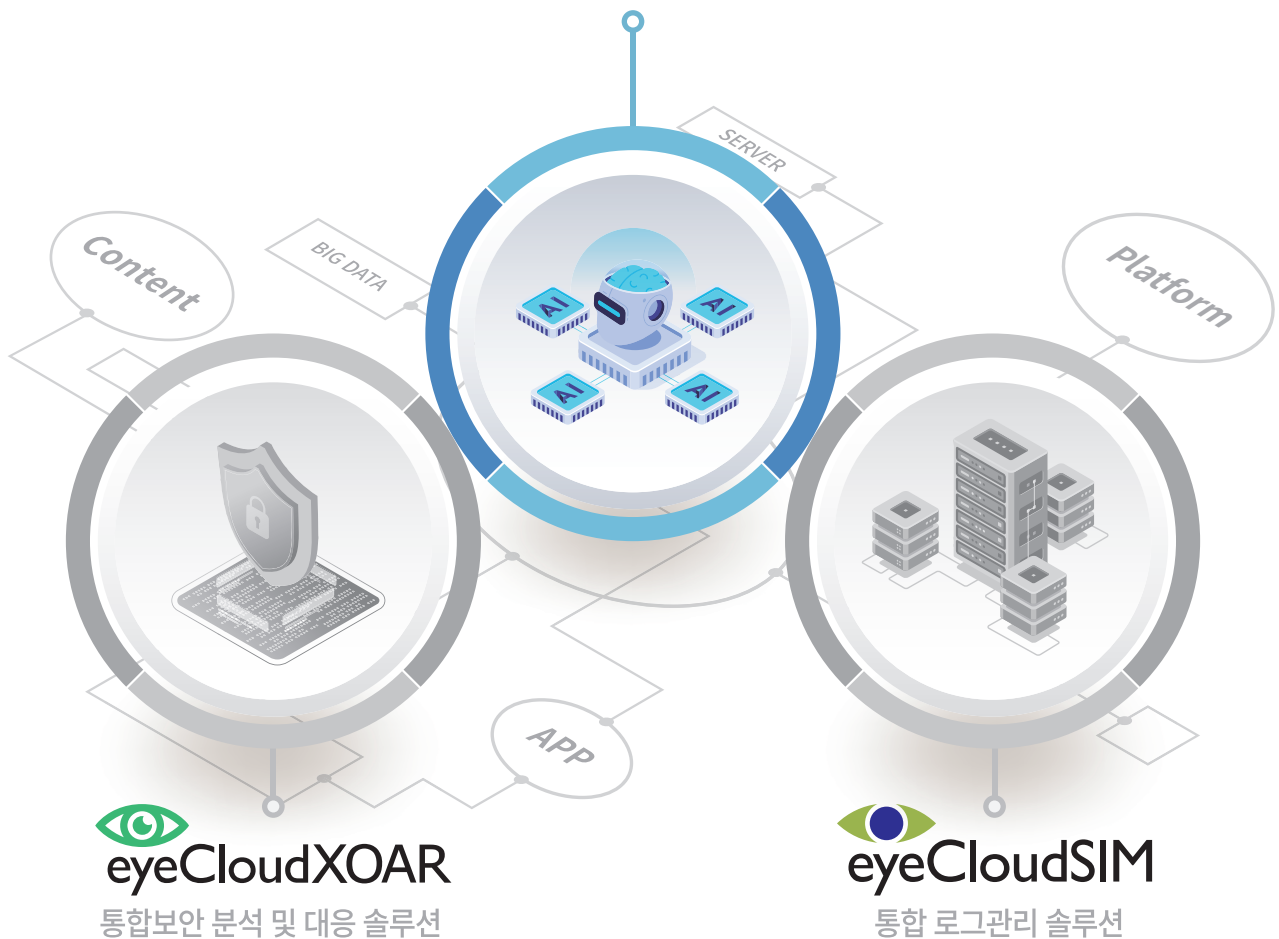


# 시큐레이어가 제공하는 차세대 보안관리 시스템

## eyeCloudAI

인공지능 분석 및 지원 솔루션



데이터를 더 빠르고 정확하게 판단합니다

# eyeCloudAI

인공지능 분석 및 지원 솔루션

GOOD Software GS인증 1등급

관련 특허 누적 18개 보유

조달청 디지털서비스몰

통합 로그관리 솔루션  
‘아이클라우드심’

통합보안 분석 및 대응 솔루션  
‘아이클라우드쏘아’

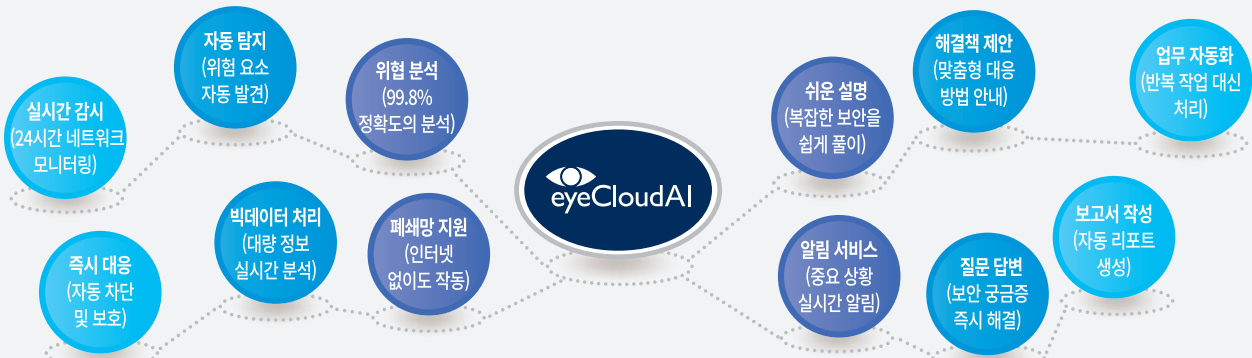
인공지능 분석 및 지원 솔루션  
‘아이클라우드에이아이’

eyeCloudAI는 기업의 사이버 보안을 지켜주는 똑똑한 AI 보안 솔루션입니다.

사이버 위협 탐지, 분석, 대응을 자동 수행하며, 복잡한 보안 문제와 해결 방법을 AI 도우미가 쉽고 빠르게 설명해 줍니다.

이를 통해 보안 담당자의 업무 부담을 획기적으로 줄이고, 더 중요한 업무에 집중할 수 있도록 돕습니다.

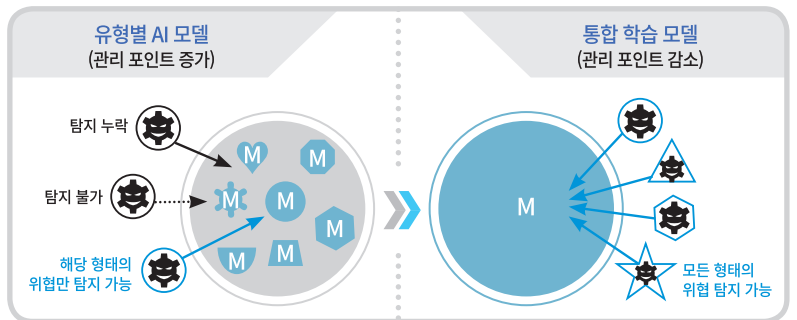
인터넷이 연결되지 않은 환경에서도 안전하게 작동하여, 지능화된 사이버 공격으로부터 기업을 빈틈없이 보호합니다.



## 특장점

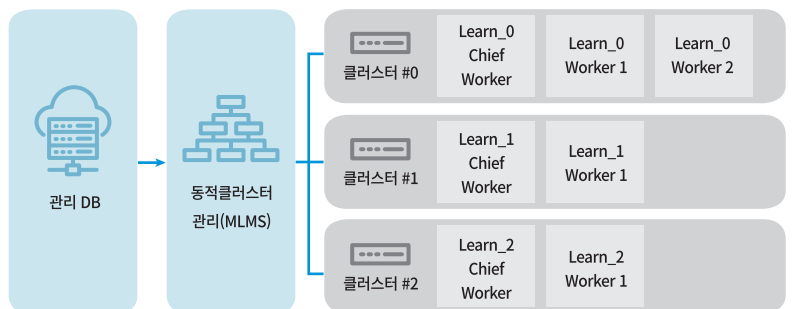
### ▶ 관리 포인트는 줄이고, 위협 탐지는 늘리고 통합 학습 모델(One Model Multi Use)

- 여러 개로 나뉜 위협 판별 시스템을 하나로 합쳐 관리 포인트를 줄이고 효율성 극대화
- 별도 연결 작업 없이 새로운 위협이나 변종 공격도 모두 감지 할 수 있음
- 새로운 공격 데이터만 추가하면 시스템이 스스로 학습해 위협 범위를 자동 확장



### ▶ 모든 자원을 가상화하여 더욱 빠르게 GPU 가상화 기반의 분산 처리

- 하나의 고성능 GPU를 여러 개로 나누어 동시에 여러 작업을 사용할 수 있는 기술
- Kubernetes(쿠버네티스)가 GPU와 컴퓨터 자원을 필요에 따라 자동으로 배분하고 조절
- 여러 컴퓨터가 AI 학습을 나누어 처리하고 결과를 공유해 더 빠른 성능 구현



### ▶ AutoML과 XAI 기술을 통해 AI 모델을 손쉽게 만들고, 그 판단 과정까지 투명하게 이해

- **AutoML** : 인공지능 모델 생성 과정을 자동화 하여 데이터 정제, 전처리함수, 매개변수 추천(하이퍼 파라미터 자동 추천 엔진, HPRS 등) 등을 간편하게 해줌
- **XAI(eXplainable AI)** : 인공지능 판단의 근거를 명확하게 제시하여 사용자 이해를 높여줌

### ▶ 누락 없는 정밀 탐지 (LLM기반)

기존 보안 시스템의 한계인 정해진 패턴(키워드) 의존성을 탈피하여 '문장 벡터 분석' 기반의 AI 탐지 기능을 제공

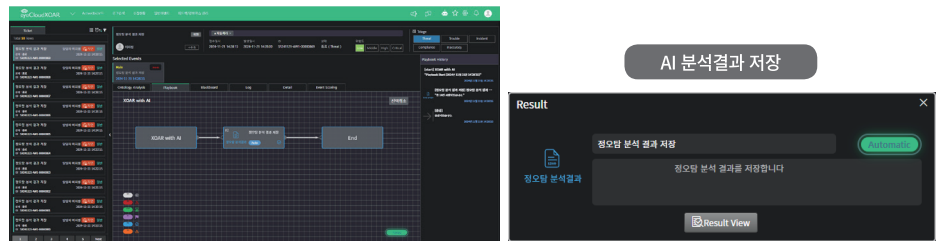
- **오탐 최소화** : 문장 전체의 맥락을 이해하여 오탐을 최소화하고, 기존 방식으로는 놓칠 수 있었던 신·변종 공격까지 정확하게 탐지
- **자동 탐지** : 특정 키워드에 의존하지 않고도 위협을 탐지하므로, 보안 담당자가 일일이 위험 단어를 추가할 필요가 없음
- **강화된 탐지 범위** : 패턴에 의존하지 않아 교묘하게 변형된 공격이나 신·변종 공격까지 놓치지 않고 찾아냄

### ▶ 빠르고 효율적인 강화 학습

- **즉각적인 피드백 반영** : 기존 AI 모델은 보안 담당자의 의견을 반영하려면 전체 시스템을 처음부터 다시 학습시켜야 해서 몇 시간에서 며칠까지 걸렸음 하지만 eyeCloudAI는 한 문장 수준의 간단한 피드백만으로도 즉시 모델에 적용되어 학습 효율성이 매우 뛰어남
- **높은 탐지 일관성** : 유사한 유형의 데이터에 대해서도 오탐과 정탐이 혼재 되었던 기존 모델과 달리, 벡터 기반 모델은 의미를 기준으로 일관된 결과를 제공하여 오탐을 대폭 줄임. 이러한 벡터 기반 모델을 통해 eyeCloudAI는 보안 분석가가 불필요한 키워드 관리나 오탐 분석에 시간을 낭비하지 않고, 본질적인 위협 대응에 집중할 수 있도록 도움

### ▶ eyeCloudXOAR와의 통합

- eyeCloudAI는 eyeCloudXOAR와 연계되어 AI 분석 결과를 바탕으로 자동 대응 및 보안 위협 탐지를 강화



## AI 기반 통합 보안 관제, 실시간 위협 대응 자동화

#### 빅데이터 기반 보안 플랫폼

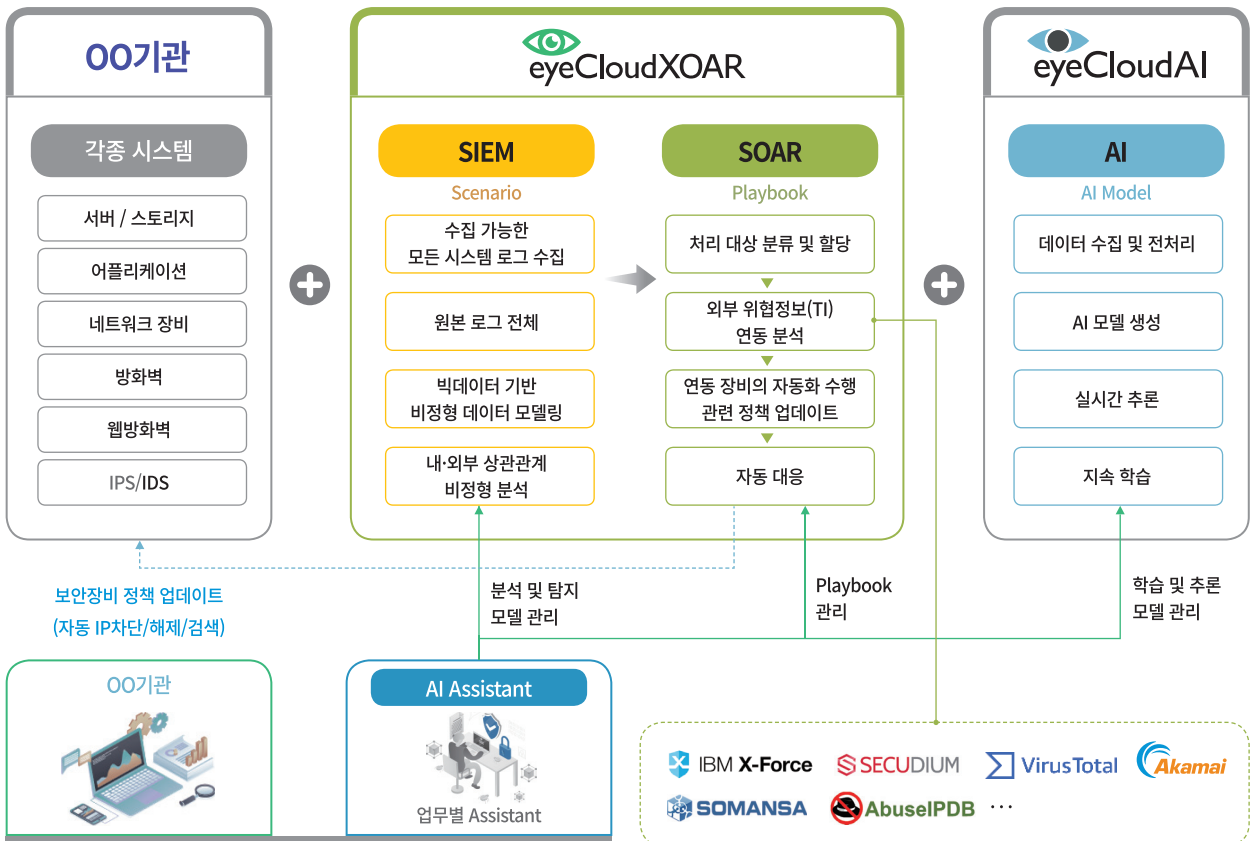
수집된 데이터를 AI가 분석하여 보안 위협을 자동 탐지 및 대응

#### 실시간 보안 위협 대응

SIEM과 SOAR를 연계하여 위협 탐지부터 차단까지 자동화된 프로세스 구축

#### 효율적인 보안 운영 지원

AI Assistant가 보안 관제 업무를 최적화하여 업무 부담 감소 및 대응 속도 향상

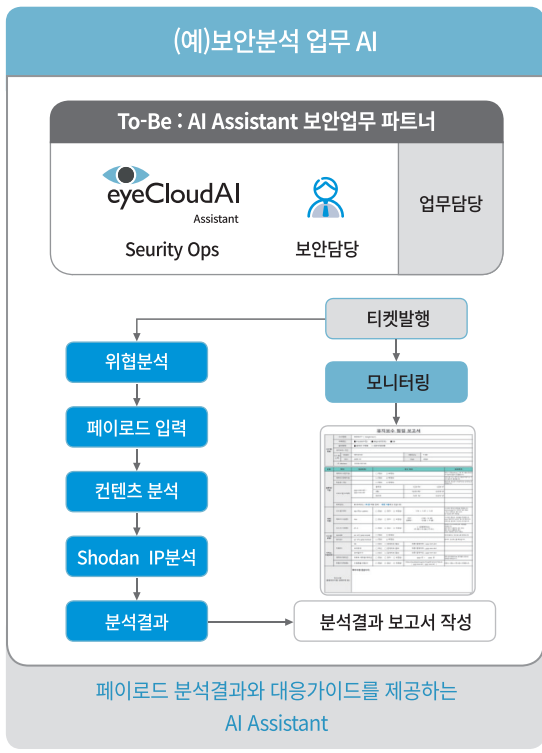
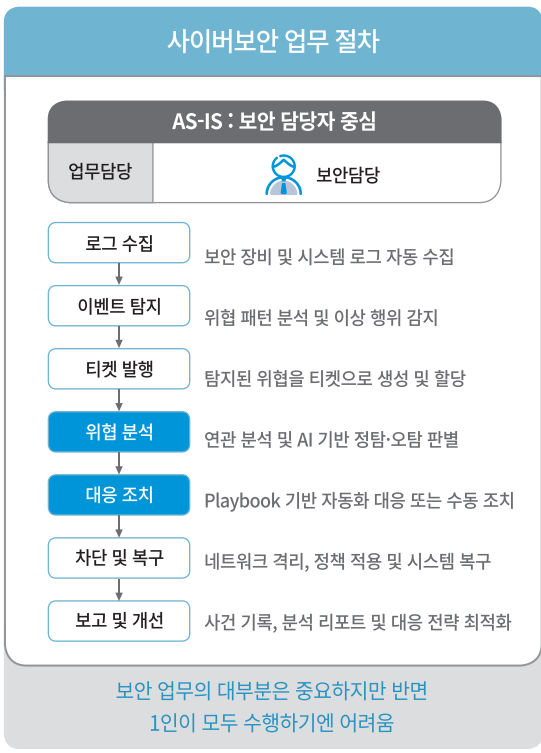


## AI Assistant, 왜 필요한가요?

기존 AI 어시스턴트는 클라우드 기반으로 외부 데이터 사용에 따른 데이터 유출 위험과 지속적인 비용 발생이라는 한계를 가집니다. 또한, 일반적인 지식 학습에 기반하여 보안 관제 업무와 같은 전문적인 영역의 지원에는 한계가 있었습니다. 'eyeCloudAI Assistant'는 이러한 한계를 극복하고 **우리 조직의 환경을 이해하는, 나를 가장 잘 이해하는 '정보보호 자문 개인 비서'**가 되기 위해 개발되었습니다. 시큐어레이어의 10년 넘게 쌓아온 인공지능 기술력과 실제 보안 업무 현장의 경험을 바탕으로, 보안 담당자의 능력을 한층 더 강화시켜 사이버 위협에 더욱 효과적으로 대응할 수 있게 도와드립니다.

인공지능(AI) 기술을 활용하여 사용자의 요청을 이해하고 적절한 정보를 제공하거나 작업을 수행하는 소프트웨어 또는 시스템

▶▶▶ '사이버 보안 특화 AI 어시스턴트' 필요



## 기존 AI 어시스턴트 챗봇과의 차별점

	구독형(기존) AI 어시스턴트 (IaaS Solution)	eyeCloudAI 어시스턴트 (On-Premise AI Assistant)
운영 방식	Cloud Server-Based AI (클라우드 서버를 통한 외부 데이터 사용)	Edge AI (조직 내부에 On-Premise 구축)
장점	<ul style="list-style-type: none"> <li>초기 설치 비용이 적음</li> <li>업데이트가 자동으로 이루어짐</li> <li>다양한 일반 정보에 접근 가능</li> </ul>	<ul style="list-style-type: none"> <li>완벽한 데이터 보안 : 회사 정보가 외부로 유출되지 않음</li> <li>전문성 특화 : 보안 관제 업무에 최적화된 AI 지원</li> <li>맞춤형 학습 : 우리 회사 환경과 업무를 정확히 이해</li> </ul>
학습 방식	<ul style="list-style-type: none"> <li>공개된 일반 데이터로 기계학습</li> <li>특정 조직이나 업무에 대한 이해 부족</li> </ul>	<ul style="list-style-type: none"> <li>기관의 실제 업무 데이터로 맞춤 학습</li> <li>내부 업무 환경과 패턴을 정확히 이해</li> <li>업무에 특화된 모델 사용으로 조직 맞춤형 AI 구현</li> </ul>

▶
“정보보호 자문 개인 비서”

## 주요기능 및 특징

eyeCloudAI Assistant는 보안 전문 지식을 학습한 LLM 기반의 대화형 어시스턴트로, 다음과 같은 핵심 기능을 제공

<p><b>대화형 질의 응답</b></p> <p>“지난주에 로그인 실패가 많았던 사용자 알려줘”</p> <p>AI “홍길동, user123, admin...”</p> <p>전문 지식이 없어도 원하는 정보를 자연스럽게 찾아줌</p>	<p><b>표현의 다양성 인식</b></p> <p>“이 IP 주소, 의미 있는 정보 있어?”</p> <p>“페이로드 분석해줘”</p> <p>“페이로드 분석 요청!”</p> <p>AI “분석 결과, 공격 시도 발견됨...”</p> <p>다양한 표현의 질의도 정확히 이해하고 응답</p>	<p><b>공격 대응 속도 향상</b></p> <p>“CAPEC-96 공격 기법 설명해줘”</p> <p>AI “이 기법은 ... (간략 설명)”</p> <p>AI가 SIEM 데이터 속에서 즉시 필요한 정보 추출</p>
--	--	---

## eyeCloudAI 어시스턴트 핵심기술

<p><b>보안 전문 학습 데이터 구축</b></p> <p>일반 시와 다른 특별한 교육 자료 사용</p>	<p>실제 보안 업무를 해본 전문가들이 직접 만든 학습 자료를 활용하고, 전 세계적으로 공인받은 사이버 위협 정보(MITRE ATT&amp;CK, CVE, CAPEC)를 학습하며, 실제 보안 관제 현장에서 발생한 사례들을 바탕으로 한 실전 데이터를 종합적으로 활용하여 보안 업무에 특화된 교육을 받음</p>
<p><b>맞춤형 추가 교육 (Fine-Tuning)</b></p> <p>우리 조직에 딱 맞는 시로 재 교육</p>	<p>이미 똑똑한 AI를 우리 회사의 보안 업무 방식에 맞게 다시 한 번 교육시키는 과정을 거쳐, 실제 보안 관제센터(SOC)의 업무 처리 방식과 우리 회사 데이터를 학습함으로써 더욱 정확한 대응이 가능하도록 최적화</p>
<p><b>똑똑한 정보 검색 시스템 (LangChain + RAG)</b></p> <p>필요한 정보를 정확히 찾아서 최적의 답변 제공</p>	<p>여러 개의 AI 기능을 마치 사슬처럼 연결해서 더 강력한 성능을 만드는 LangChain 기술과 질문을 받으면 관련 자료를 먼저 찾아보고 그 정보를 바탕으로 정확하고 맞춤형 답변을 생성하는 RAG 시스템을 결합하여, 마치 경험 많은 보안 전문가가 방대한 자료실에서 필요한 정보를 순식간에 찾아 정확한 조언을 해주는 것과 같은 서비스를 제공</p>

## 도입효과

<p><b>정탐률 개선 (정확한 탐지율)</b></p> <p>CNN(2만건 학습) → LM(700건 학습), 동일조건 정탐률 상승</p> <p>데이터 효율성이 '약 29배' 증가, 성능 향상</p> <p>49.4% Before → 94.8% After</p> <p>Less Data, Better Positive</p>	<p><b>오탐률 감소 (불필요한 알람)</b></p> <p>feature space를 더 효과적으로 이해, 동일조건 오탐률 감소</p> <p>모델이 공격/비공격 구분을 더 명확하게 학습</p> <p>50.6% Before → 5.2% After</p> <p>불필요한 알람 감소</p>
<p><b>정·오탐 분석/분류 자동화</b></p> <p>단순 반복 업무의 기계적 처리 가능</p> <p>하루 2만건 분석에 필요한 인력을 시로 대체</p> <p>1명이 30건 업무 처리 시 → 실제 650명의 인력소요</p>	<p><b>이상행위 탐지</b></p> <p>알려지지 않은 위협도 탐지</p> <p>비지도 · 강화 학습을 통한 신종 위협 탐지</p> <p>숙련된 분석가가 장기간 분석해야 할 위협을 기계적으로 처리</p>
<p><b>인력 부담 감소</b></p> <p>전체적 모델 효율화</p> <p>고품질 데이터셋 구축 및 신규 모델 학습 · 배포 가능</p> <p>평균 분석 시간 97% 이상 단축</p> <p>데이터 분석 약 1/29</p>	<p><b>리포트 자동 생성</b></p> <p>보고 및 의사결정 지원</p> <p>리포트를 자동 생성하여 관리자의 의사결정 지원</p> <p>보안 관제를 위한 세분화된 질의 응답 수행</p>
<p><b>운영비용 절감</b></p> <p>모델 효율화</p> <p>대량 이벤트 대응 자동화 될수록, 한 번에 더 많은 위협 이벤트 처리 가능(리소스 분배 효율 ↑)</p> <p>초과근무 감소, 분석가 번아웃 예방</p>	<p><b>재학습 주기 완화</b></p> <p>소량 데이터로도 업데이트가 가능해, 주기적 재학습 부담 감소</p> <p>학습 데이터, 학습 시간 대폭 감소</p> <p>많음 → 적음</p>



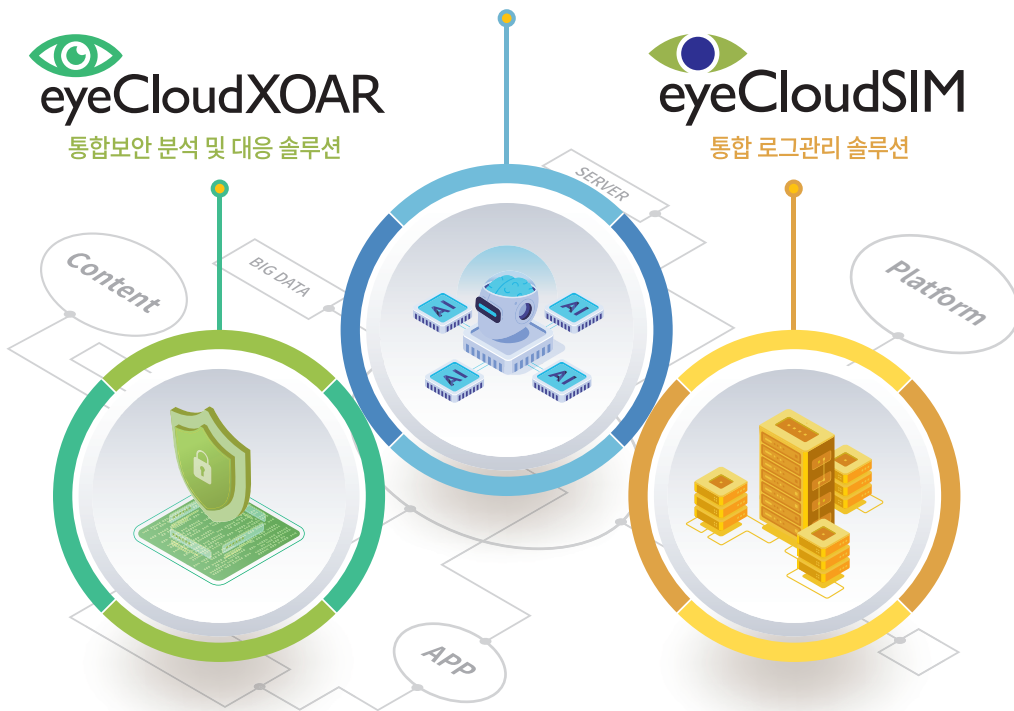
인공지능 분석 및 지원 솔루션



통합보안 분석 및 대응 솔루션



통합 로그관리 솔루션



● **본사** 서울시 성동구 성수일로 4길 25 서울숲코오롱디지털타워 14F

● **대전지사** 대전광역시 유성구 죽동로297번길 83, 대울빌딩 3층

● **대구지사** 대구광역시 동구 팔공로 241 태왕아너스타워 104호(봉무동)

● **광주지사** 광주광역시 북구 첨단과기로208번길 43-22, 첨단와이어스파크 A동 1012호

● **TEL.** 1800-6713

● **FAX.** 02-499-7605

● **구매문의.** [contact@seculayer.com](mailto:contact@seculayer.com)

● **기술문의.** [tech@seculayer.com](mailto:tech@seculayer.com)