

ChatGPT와 AI시대의 보안전문가 생존전략 웨비나

“보안모니터링 업무는 AI에게 맡겨주세요”
정보유출 AI 운영경험과 사례소개

LG CNS 보안서비스 Innovation팀
정좌연 책임

목 차


- 1 ChatGPT와 보안전문가 생존전략
- 2 AI 보안 적용의 현실적인 어려움
- 3 정보유출 분야의 AI의 도입성과
- 4 SecuXper AI 소개

1


ChatGPT와 보안전문가 생존전략

> ChatGPT에게 보안위협에 대해 물어보았다.

Q) `https://insecure-website.com/products?category=Gifts'--` 구문의 위협요소를 알려주세요.

 URL "`https://insecure-website.com/products?category=Gifts'--`"은 SQL Injection 공격을 포함할 가능성이 있어 보안 위협이 될 수 있습니다. "--"는 원래 SQL 쿼리를 종료하는 주석으로 작동하며, "Gifts" 다음의 아포스트로피는 구문오류를 발생시키거나 의도하지 않은 명령을 일으켜 SQL 쿼리를 조작하여 민감한 데이터를 검색하거나 데이터베이스를 수정하는 것이 가능하게 합니다.



Q) "`_xm_webid_1_=-1" OR +716-716-1=0+0+0+1 --`"의 위협요소를 알려주세요.

 이 문장은 잠재적으로 블라인드 SQL Injection 공격의 일부일 수 있습니다. 이 유형의 공격에서 공격자는 검색상자나 로그인 양식과 같은 사용자 입력 필드를 조작하여 취약한 애플리케이션 악성 SQL 코드를 삽입하려고 합니다.

1

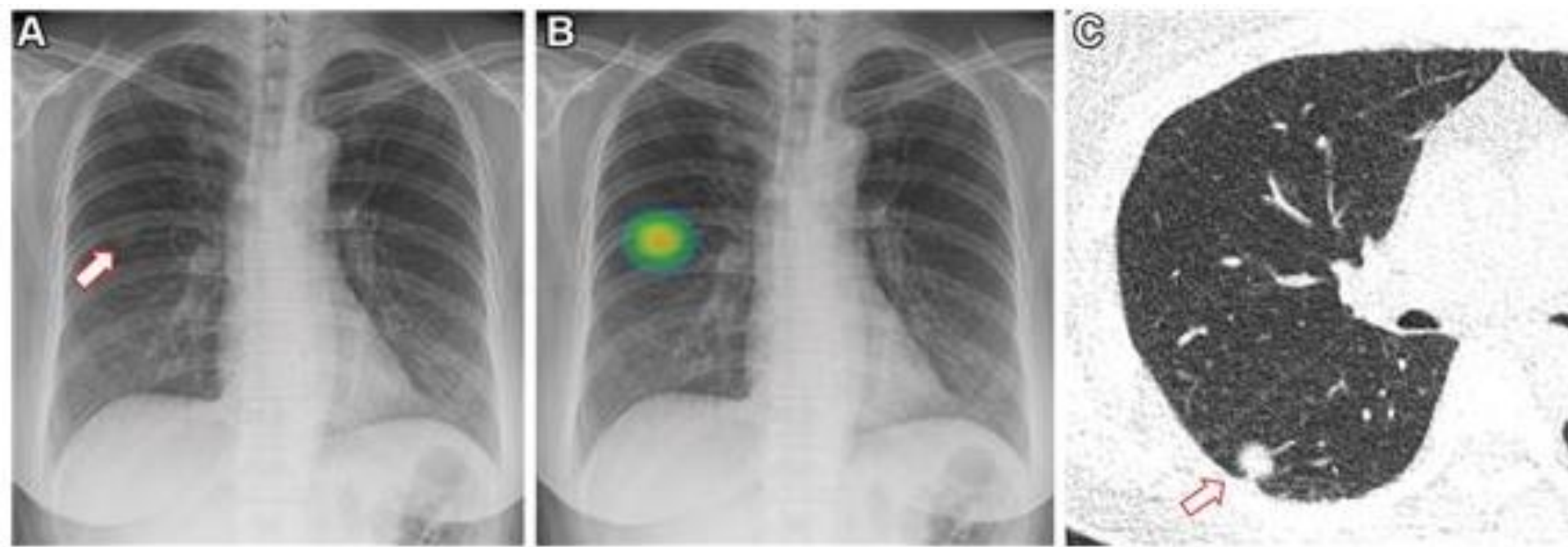
ChatGPT와 보안전문가 생존전략

> AI가 전문가의 업무를 대체할 수 있을까?

유형	Chat GPT 답변 예시	대체 가능 여부
1. 문자열 관련 공격 및 자연어 처리	 "OR 3+318-318-1=0+0+0+1 --"는 SQL Injection 공격의 전형적인 예시로, 악성 요소가 웹 애플리케이션의 취약점을 이용하여 공격할 수 있습니다.	→ 학습 데이터가 충분히 있으면 대체 가능 ● SIEM 적용 가능
2. 상황에 따른 위협수준 판단	 IP 주소 192.168.91.42는 사설 IP 주소 중 하나이며, 일반적으로 공개된 인터넷에서 직접 접근할 수 없습니다. 따라서 이 IP 주소가 공격자인지 여부는 그 사용 목적과 상황에 따라 다릅니다.	→ 정보 부재 상황, 정책 오류는 판단하기 어려움 약 90% 정확도를 보장 ● 전문가의 확인 필요

의료분야에서의 AI활용

AI기반 흉부 X-Ray 보조진단 시스템



AI 사용군 환자의 흉부 X-ray 폐결절 검출 사진. 이 환자는 실제 조직검사에서 폐암 진단을 받았다(사진 제공: 서울대병원).

출처: 청년의사 신문

의사 보조하는 AI 실제 성능은?...폐 결절 검출률 2배 '깡충'

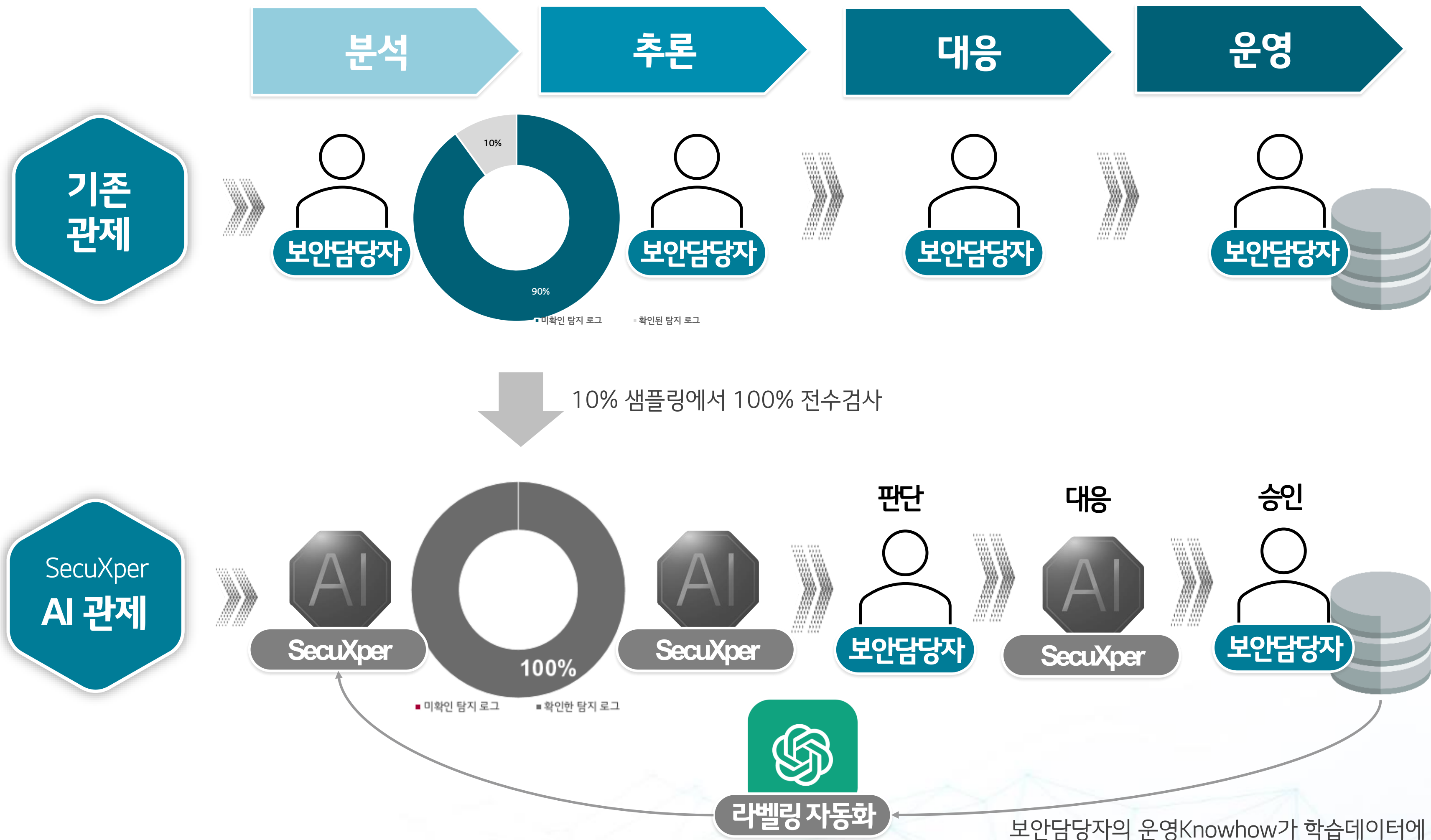
청년의사 & 고정민 기자 | © 입력 2023.02.17 16:07 | 댓글 0

그 결과, AI 사용군 폐 결절 검출률이 0.59%로 0.25%인 비사용군보다 2.4배 높았다. 검출 정확도도 엇비슷했다. 양성 환자 가운데 추가 컴퓨터단층촬영(CT) 검사에서는 결절이 발견되지 않는 가의뢰율은 AI 사용군 45.9%, 비사용군 56.0%였다.

연구팀은 AI를 활용하면 불필요한 추가 검사를 억제하면서 결절 검출률을 개선할 수 있다고 설명했다. 다만 이런 결과는 AI 분석을 참고해 영상의학과 전문의가 최종 판독했을 경우로 한정됐다. AI가 단독 판독하면 결절이 없는데도 양성으로 판단하는 가양성이 늘어 불필요한 추가 검사로 이어졌기 때문이다.

1 ChatGPT와 보안전문가 생존전략

보안분야에서의 AI활용, 90%의 생산성 향상과 보안담당 전문지식으로 학습데이터에 내재화



2

AI 보안 적용의 현실적인 어려움

실무 적용관점의 주요 문제점

Data



- 학습용 데이터 부족
 - 고품질 데이터 부족
 - 분석용 로그 Vs 이벤트 로그

- 정보보안 담당자간 판정 기준 상이



부족한 데이터

Quality



- 상용 수준 품질을 제시하기 어려움
 - 적정 비용과 정량적 성능제시 미흡

- 데이터 분석 기능에 한정
 - ChatGPT와 같은 이상판정 부족
 - 차트 위주의 분석도구만 제공



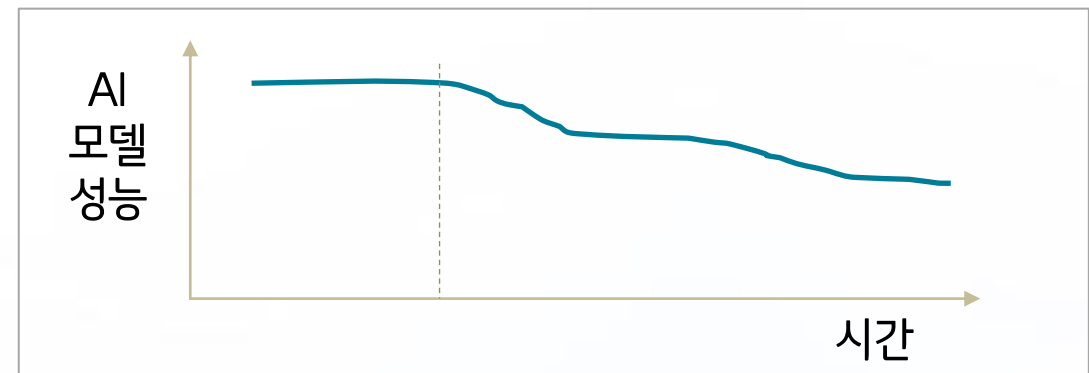
AI서포트 미흡

Operation



- AI의 성능 문제
 - 패턴 변화에 따른 성능저하 발생
 - 스스로 학습하는 AI부재

- 운영과 유지보수의 비용증가
 - 인력채용 및 운영의 어려움
 - AI투자에 대한 ROI 확보 어려움



낮은 성능, 고비용

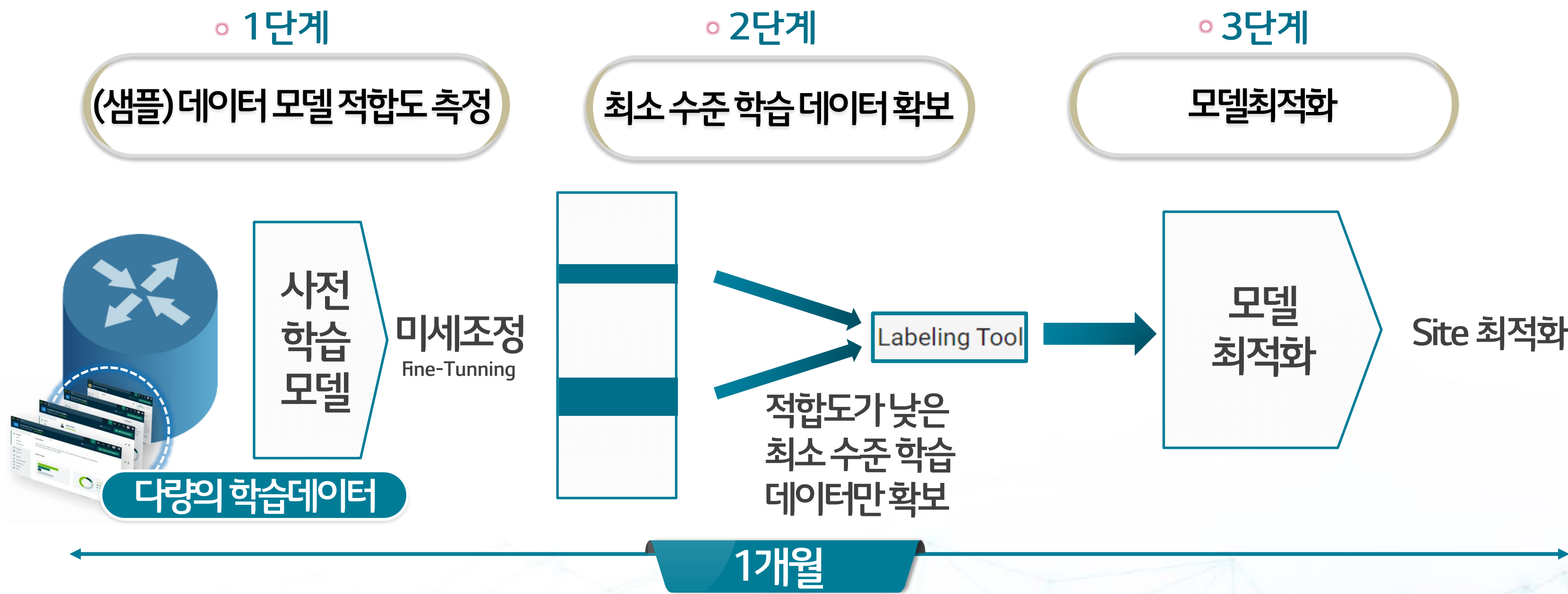
2 AI 보안 적용의 현실적인 어려움

> Data : 부족한 학습데이터는 사전학습모델을 활용하여 최소수준의 데이터만으로도 최적화 가능

일반적 AI
구축

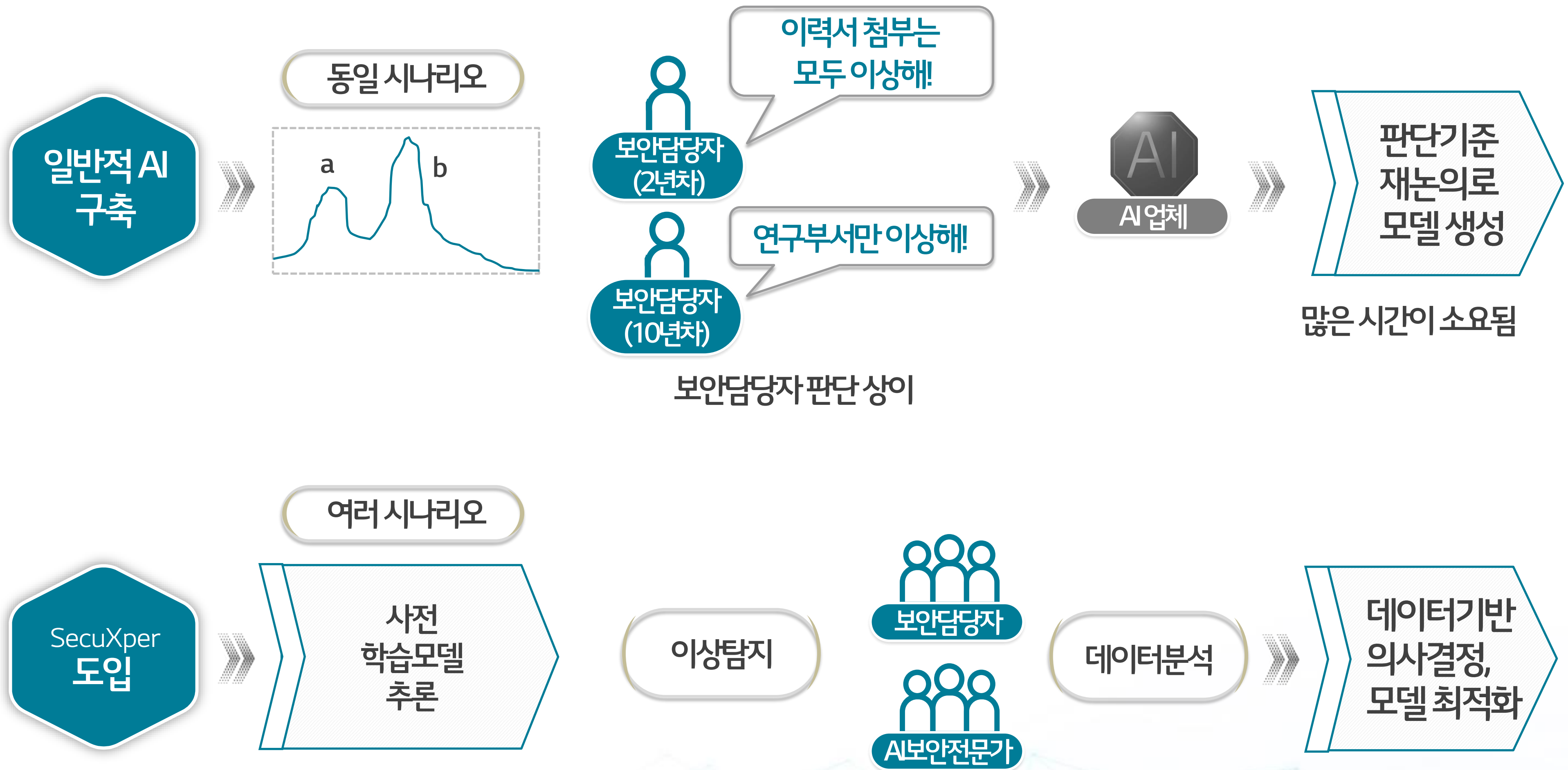


SecuXper
도입



2 AI 보안 적용의 현실적인 어려움

> Data : 상이한 전문가의 판단을 AI전문가의 데이터 분석 Insight를 활용하여 최적화



2

AI 보안 적용의 현실적인 어려움

Quality : 데이터 분석도구가 아닌 AI 활용기반의 정량적 성과 제공 필요



SW 프로젝트

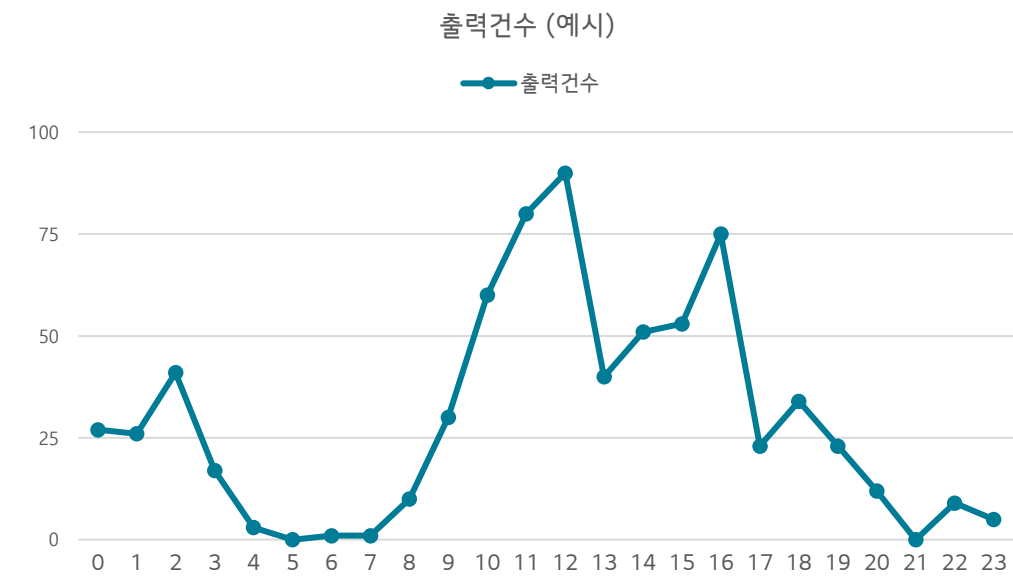
- 기존의 프로젝트 관리 경험
- 업무 리딩 및 데이터 점검 용이
 - UI/UX 테스트 및 검증 가능



- 가시적 결과물
- 정상적인 기능동작으로 점검가능

기존 AI 프로젝트

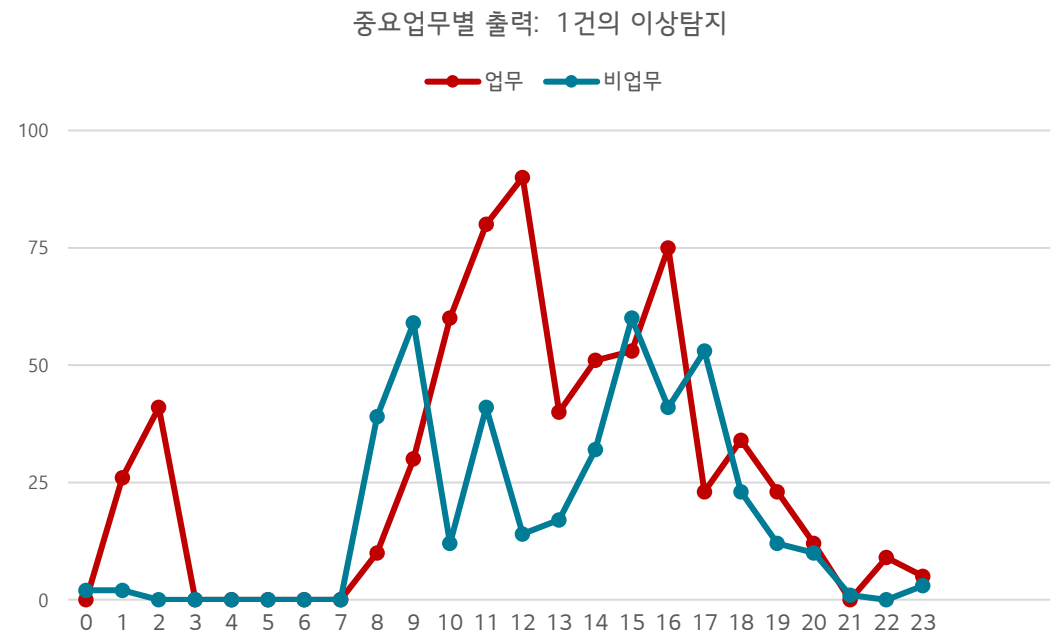
데이터 분석도구로 자체 해석 어려움
단순 수치에 근거한 이상탐지



- 비가시적 결과물
- 기능동작은 정상적이나, 데이터 Insight는?

SecuXper AI

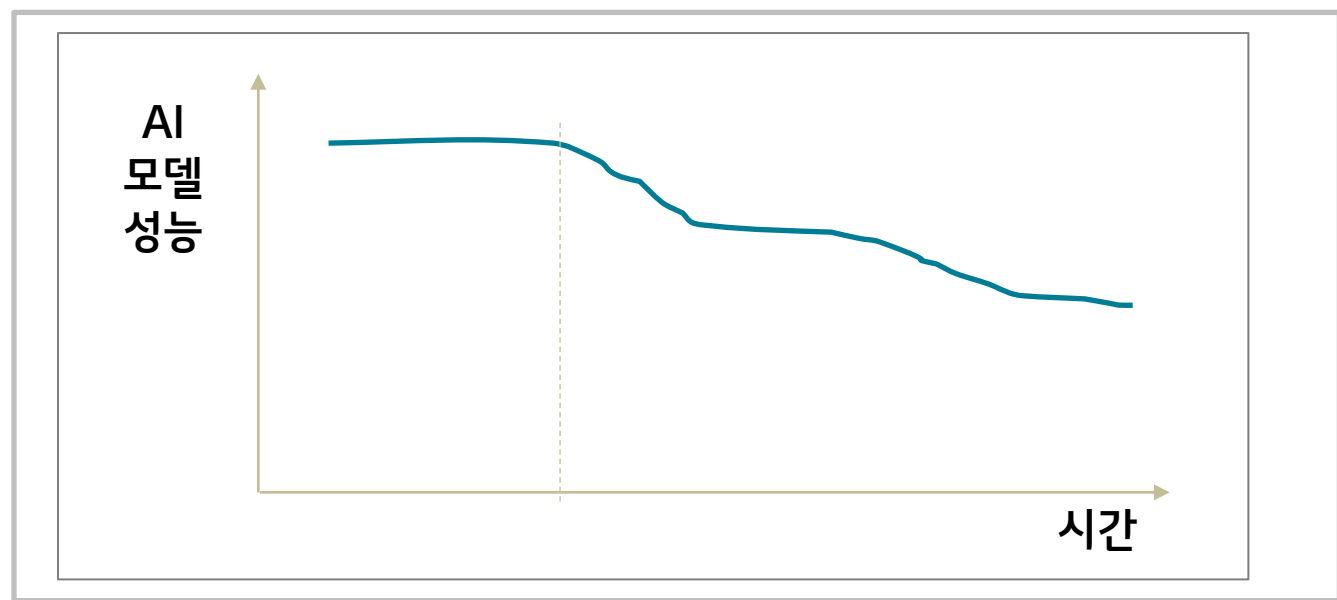
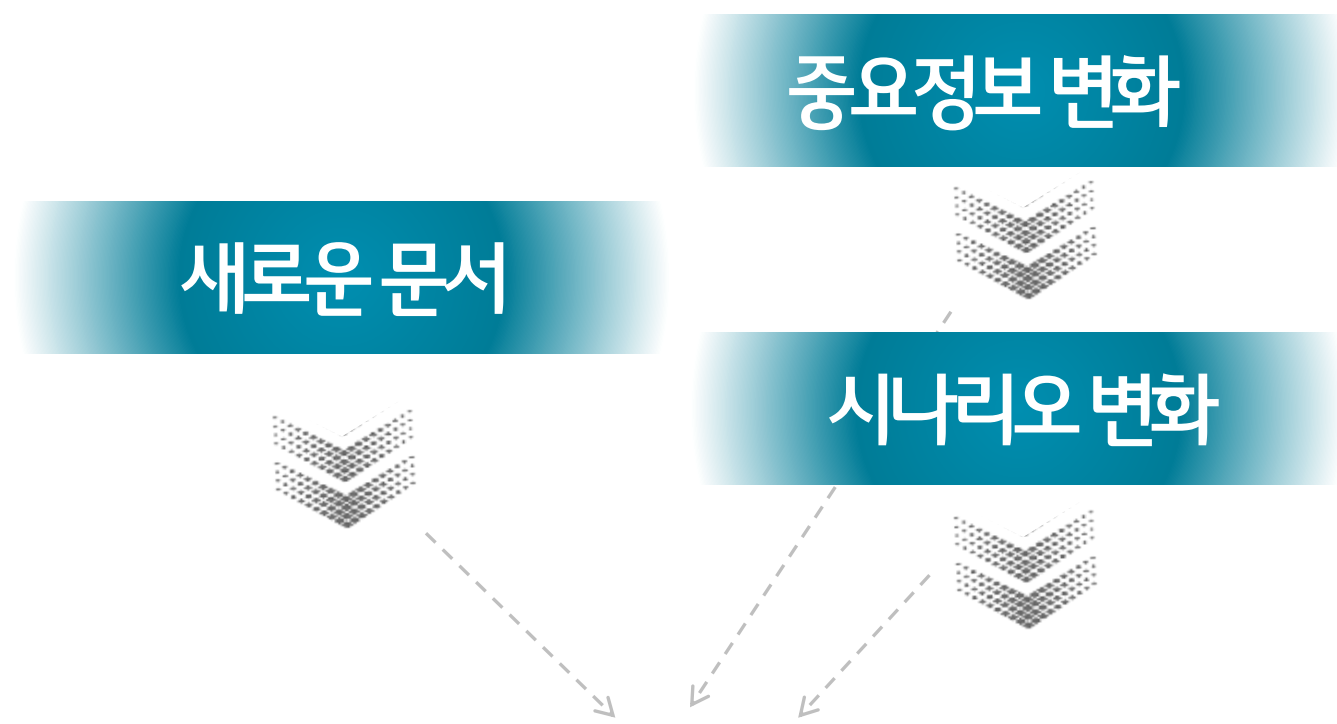
AI의 분류결과를 반영한 이상탐지
(자연어 처리 결과)



- 사람의 판정과 같은 결과물
- AI에 의해서 문서의 내용 분류하고, 이상탐지 후보를 제시함
 - AI에 의해서 개인별 업무시간 판정 (해외근무자도 식별)

2 AI 보안 적용의 현실적인 어려움

> Operation : 지속적인 성능 보장과 비용 최적화



시간이 지남에 따라 성능이 떨어지는 AI 모델

일반적 AI 구축

SecuXper 도입

자체인력

외주인력



구독 서비스

고비용
인력 운용 효율 저하

인력 수급 어려움
신속한 성능 저하 파악 및 대처 어려움

정기적 re-training
백오피스 인력 지원
신속한 성능 저하 파악 및 대처 가능

3

정보유출 분야의 AI 도입 성과

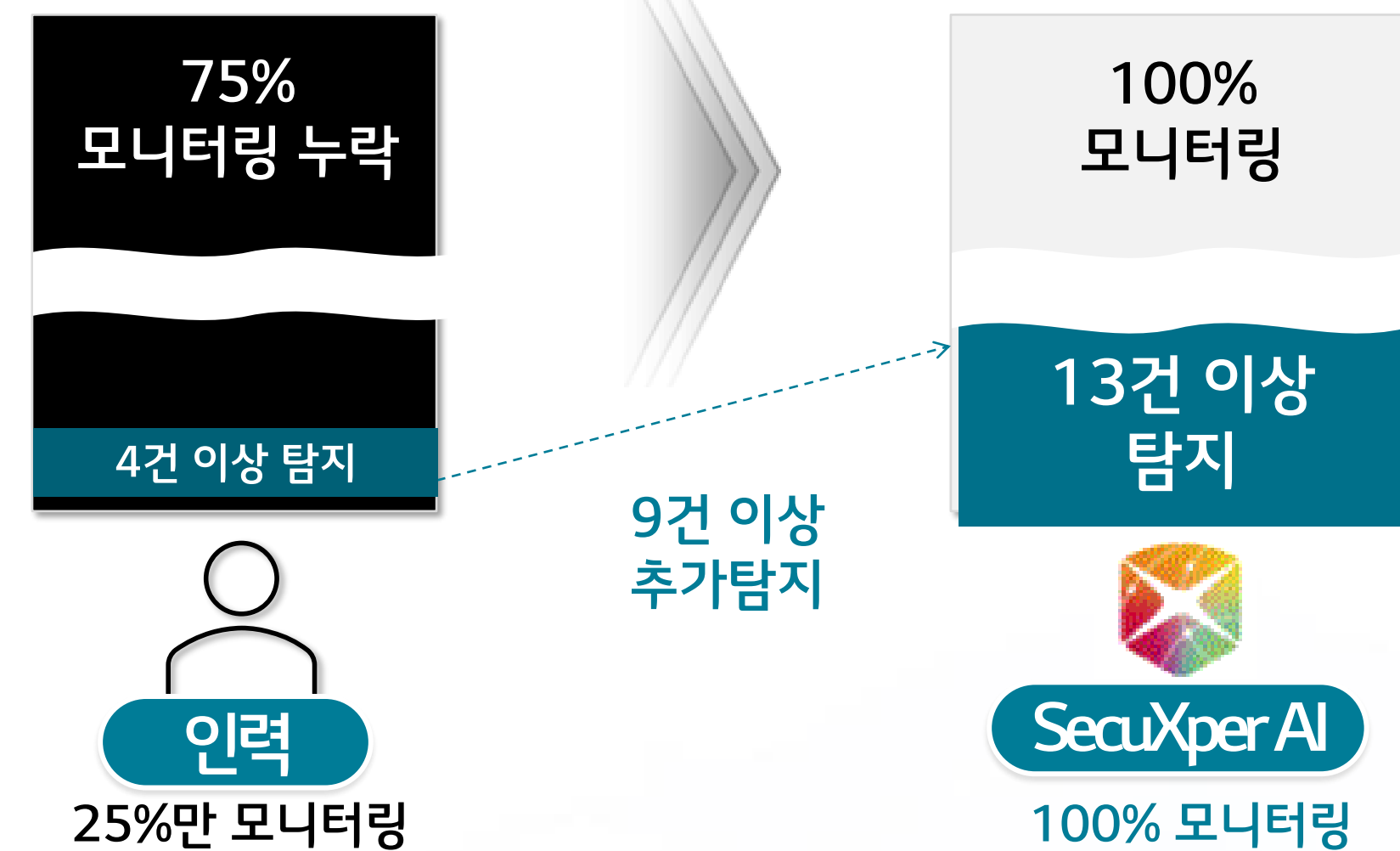
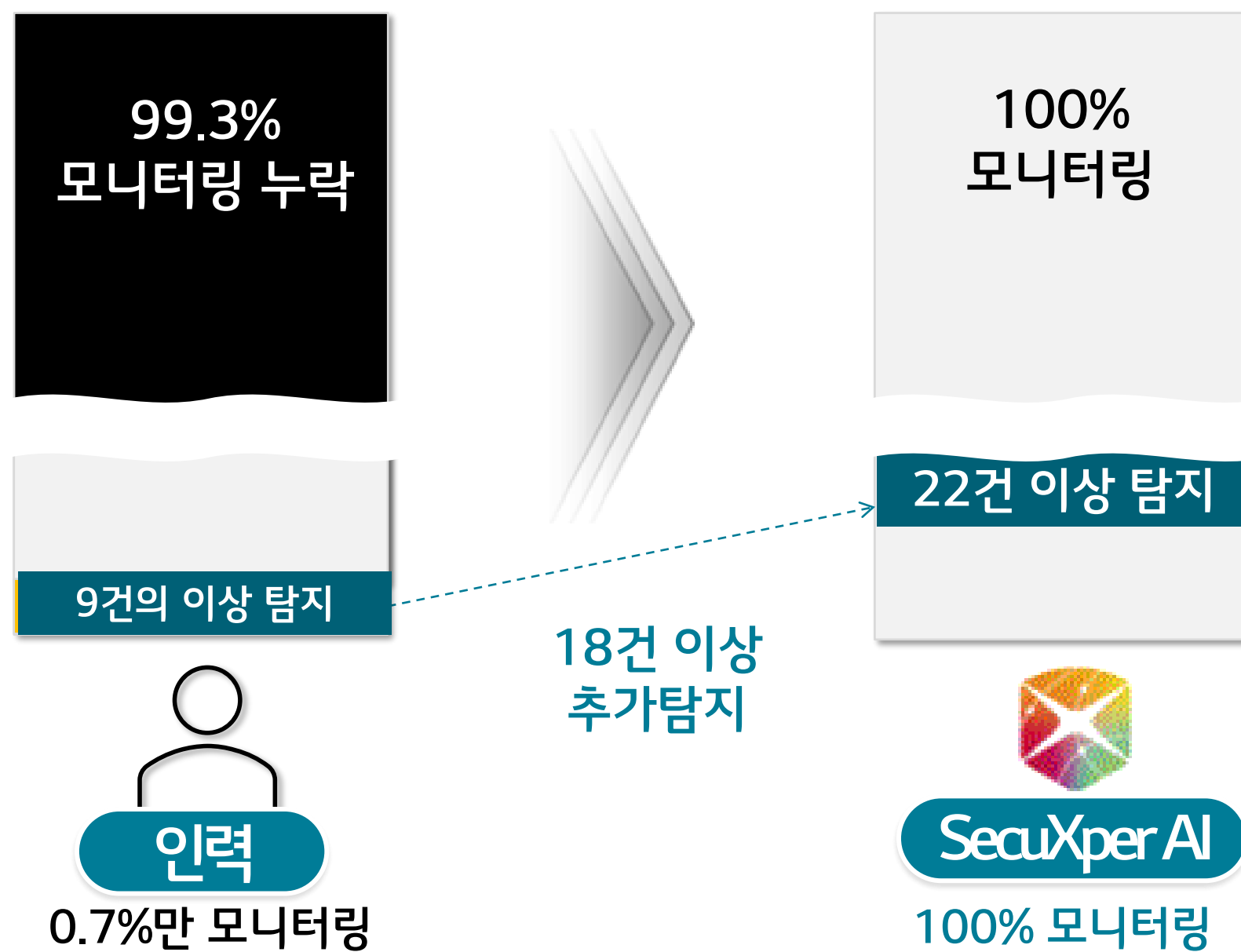
> 기존 대비 전수 모니터링 가능, 미탐 다수 탐지

- 메일 유출의 경우 1명의 인력, 일평균 65건 → AI기반 일평균 8,455건 모니터링 (약 130명의 인력운영효과)

메일 유출 모니터링 결과

파일 유출(출력, 다운로드) 모니터링 결과

※ 15일 모니터링 결과



3

정보유출 분야의 AI 도입 성과

> 변화하는 보안관리 환경에 적합한 지능화된 보안



4 SecuXper AI 소개

> SecuXper AI가 제공하는 Solution

지난 5년 간의 유출, 침해, 오남용 보안 분야에 적용되었던, SecuXper AI서비스를 통해서 사전 학습모델을 제공받고, AI의 서포트를 통해서 생산성 향상과 AI 도입비용을 절감

SHARE
Insight

with Learning Data

SUPPORT
JOB

with AI Assistant

SAVE
MONEY

with subscription

AI Assistant 적용

AI 모델 최적화

Dashboard 커스터마이징

The image displays three main components of the SecuXper AI system:

- AI Assistant 적용 (AI Assistant Application):** A screenshot of a reservation system interface. It shows a reservation confirmation for No. 143741. The AI assistant is integrated into the system, providing automated responses and handling reservation details. The interface includes a sidebar with navigation options like '데이터셋', '라벨', and '모델링'.
- AI 모델 최적화 (AI Model Optimization):** A screenshot of a dashboard showing performance metrics. It features a large numerical display for '이상 메일' (524, 537, 13) and several charts: a pie chart for '요일별 이상 건수' (Daily Abnormal Cases) and a bar chart for '부서별 이상메일 건수' (Abnormal Email Cases by Department). The pie chart shows: Friday (14%), Monday (24%), Thursday (21%), Wednesday (20%), Tuesday (18%), Friday (14%), Saturday (2%), and Sunday (1%).
- Dashboard 커스터마이징 (Dashboard Customization):** A screenshot of a highly customized dashboard. It includes a '부서별 이상메일 건수' bar chart, a '일일 이상 메일 건수' (Daily Abnormal Email Cases) bar chart, and a table of '이상 메일' (Abnormal Emails) with columns for sender, recipient, and subject. The dashboard also features a '주말/야간 이상 건수' (Weekend/Night Abnormal Cases) gauge chart showing 2.82%.

> 솔루션 특징점 및 주요 기능

정보유출 이상탐지 AI 특징점

95% 성능보증 • AI의 분류 정확도 95% 보장

AI기반의 탐지시나리오 • 패턴대비 80% 적은 시나리오로 보다 높은 정확도로 이상탐지

전문가의 기술지원 • AI 전문 PMO, 보안 전문가, AI 컨설턴트, 데이터 엔지니어, 대용량 서비스 아키텍트

정보유출 이상탐지 AI주요 기능

문서분류 • 대용량 처리가 가능한 OCR
• 47종 문서분류
• 외국어-한국어 번역 모델

행위 기반 프로파일링 • 중요 문서 식별
메일, 메신저, 파일 다운로드 첨부파일, 이미지 문맥 분류
• 과거/동료 대비 유출 행위
부서별/개인별 업무시간, 출력 행위, 문서열람 행위, 물리 출입 여부

자동 라벨링 • 비지도 기반 클러스터링 유사도 활용
데이터 라벨링 one-stop 서비스

> 적용고객의 VOC

문서분류 및 AI 정확도가
높아 보안홀이 없어지고
단순업무의 90%
개선되었어요

제조 분야

유출에서의 사고위험이
대폭 줄어들었네요

서비스 분야

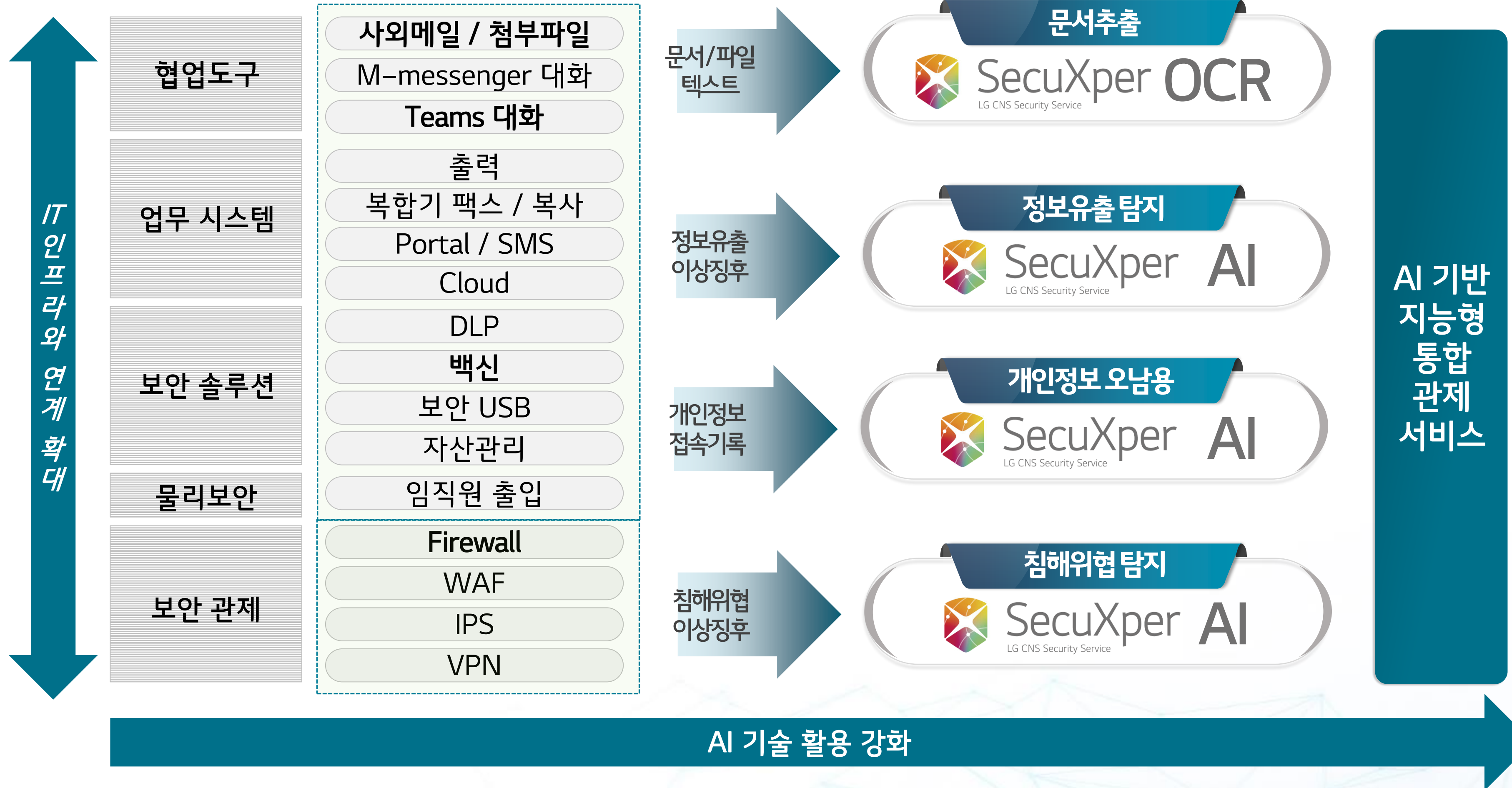
개인정보 오남용
AI 시나리오 덕분에
이제는 짚은 시나리오
변경없이
운영 가능합니다

공공사업분야

4 SecuXper AI 소개

> SecuXper AI 적용 분야

SecuXper 보안AI 솔루션 활용 범위



4

SecuXper AI 소개

1명의 AI전문가 채용비용으로 아래의 구독 서비스를 제공합니다. <https://abba.oopy.io/>

AI 교육 (무상)

AI보안 도입을 위한 기술교육 (2hr)

- 최신 AI보안 Trend
- AI보안에 활용되는 주요 기술과 도입로드맵 가이드

SecuXper AI기반의 데이터분석 (1일)

- SecuXper AI 이해
- API서비스, 자동 라벨링 도구 활용
- 데이터 리터러시 이해

AI운영 지원

운영서비스

- SecuXper AI모델 업그레이드
- AI모델 최적화 서비스(주기적)

유지보수서비스

- 장애 및 서비스 복구 지원

AI보안 컨설팅

도입컨설팅

- AI보안 도입 로드맵 수립 가이드
- AI보안 ISP, 마스터플랜 수립 컨설팅

AI검증컨설팅

- AI성능 검증 컨설팅 (모델 / 시스템처리성능)
- 유출, 침해 AI 데이터 검증 컨설팅

AI보안 솔루션 구축

로그통합

- 로그통합 솔루션 구축 (Splunk 등)
- 솔루션 통합 및 연계 개발

AI활용 솔루션 구축

- 보안에 특화된 OCR, 문서추출, 문서자동분류
- 메일유출탐지, 출력이상, 파일유출탐지 AI
- 개인정보 오남용 탐지 AI, 침해탐지 AI

“보안모니터링 업무는 AI에게 맡겨주세요”
정보유출 AI 운영경험과 사례소개

Thank you