LG CNS

SecuXper

ChatGPT와 AI시대의 보안전문가 생존전략 웨비나

해킹에 대응하는 AI,
AI Assistant를 통한 24시간 관제방안

LG CNS 보안서비스 Innovation팀
김상화 책임

LG CNS

목 차

1 관제 모니터링의 중요성

실무적으로 확인된 모니터링 커버리지와 인력베이스 관제 현황

홈 > 산업 > IT

[中 해커 놀이터 된 한국] "10% 뚫려도 서버 100만대 노출…보안 투자 급선무"

입력 2023-02-15 17:56:21 수정 2023.02.15 18:50:03 강도림 기자

실제 확인된 모니터링 커버리지

보안 장비 WAF / IPS	0 ~ 5 %
메일 유출 모니터링	0.7 ~ 10 %

(+ 종합적 관제 부재)

인력 베이스 관제 현황

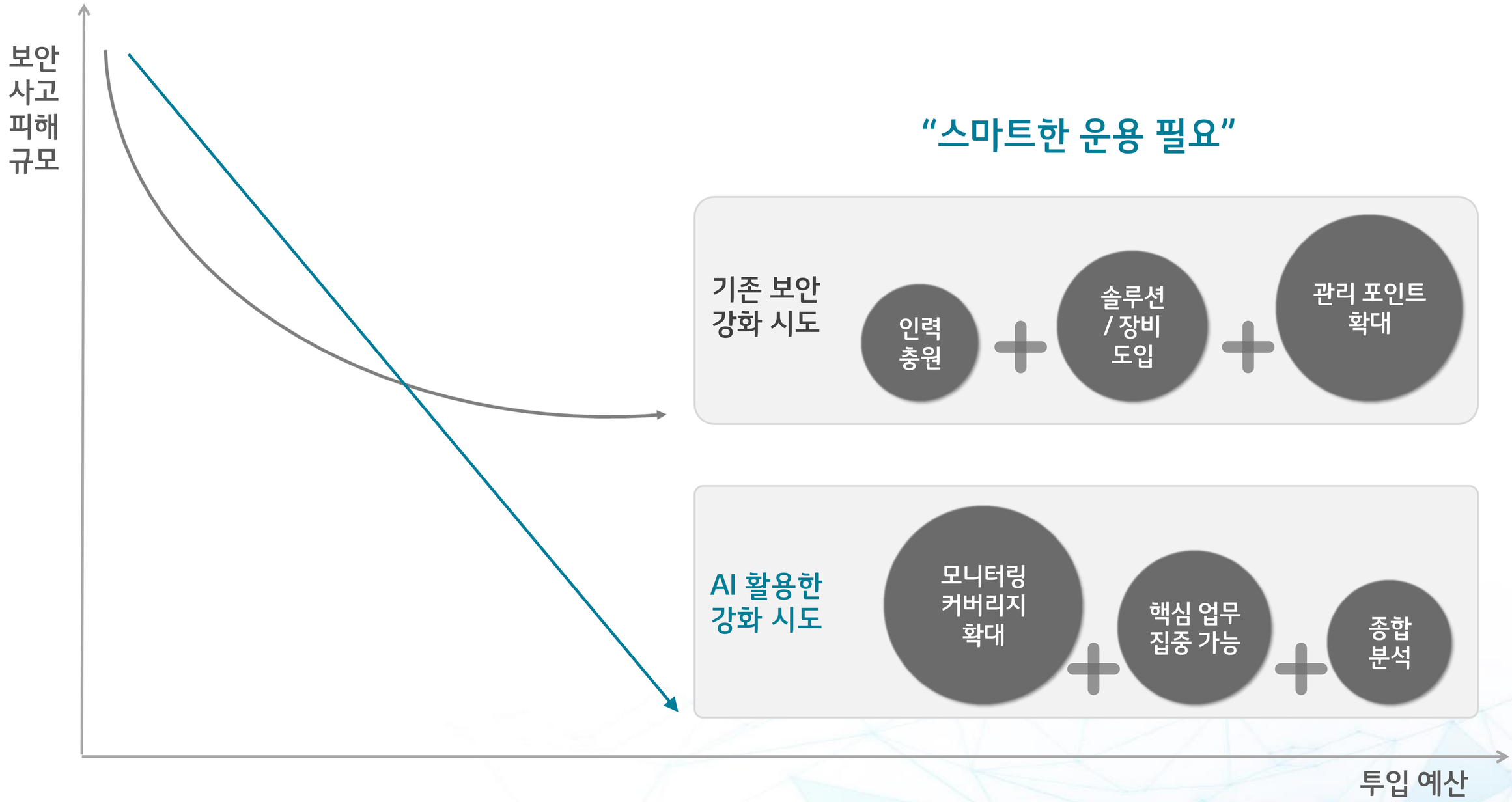
케이스 처리 건수 (1인/1일)	5~10 건
일 발생 케이스 수	1~200 건

*케이스: 사고 분석을 위한 로그 모음

출처: https://sedaily.com/NewsView/29LRFD25I6

2 보안 강화 노력과 사고규모의 관계

기존 보안강화 시도와 AI 활용 강화 시도에 따른 보안 사고 피해 규모 비교



3 기존 침해관제 현황 및 AI 활용방안

변화하는 보안 관리 환경에서의 AI 적용 가능성

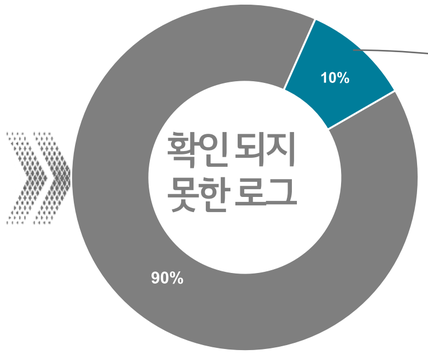
기존 침해 현황	어려운 점	AI를 이용한 방안
단순 키워드 / 패턴/시그니처 기반 탐지	패턴 우회 공격에 취약	패턴개선 AI모델
새로운 공격 패턴이 추가될 때마다 규칙을 생성하고 관리 필요	규칙을 생성하기 전에 대응이 어려움	프로파일링 AI모델
늘어만 가는 룰	관리 공수 증가 룰 관리를 위한 별도 인력 필요	학습데이터 활용
다수의 관제 요원 존재	관제 실력 / 의견 차이 존재	AI Assistant 사용한 업무 상향 평준화
새로운 취약점 / 공격 지속 발생	장비 업데이트 전까지 기록도 안됨	AI모델에 의한 식별 가능

4 AI 침해관제 프로세스

AI보안 도입 전후의 프로세스 비교

01 분석 → 02 추론 → 03 대응 → 04 운영

기존 관제



분석 > 추론 > 대응 > 운영

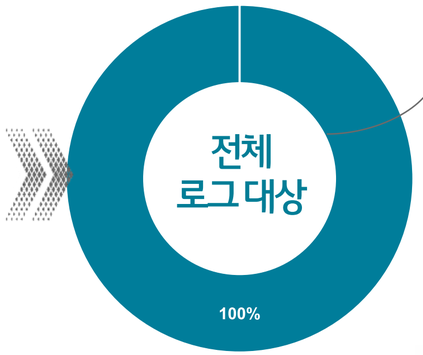
담당자 지식 기반 일부 선택 필터링

보안담당자

저장

SIEM

SecuXper AI 관제



분석 > 추론

AI

SecuXper AI

판단

보안담당자

대응

AI

SecuXper AI

승인

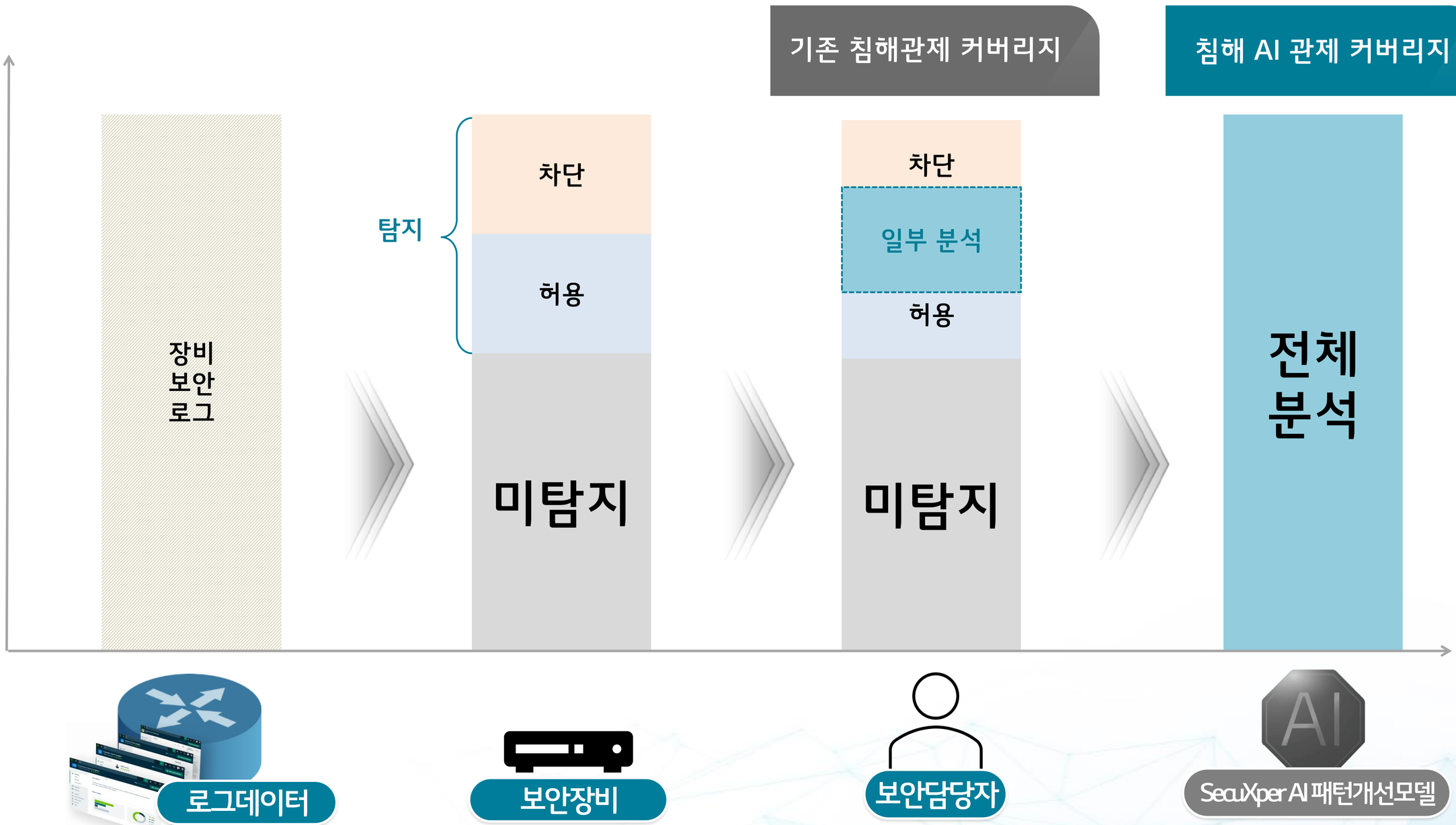
보안담당자

저장

SIEM

학습에 활용 > 모델 성능 지속적 개선

기존 침해관제 커버리지 대비 확대된 AI 관제 커버리지 비교



AI 분류모델을 이용한 변형된 공격 탐지 예시

학습 데이터

기존 키워드	/etc/local.xml
변형된 키워드 학습	/etc/local_bak.xml
	/etc/local_dev.xml
	/etc/local_debug.xml

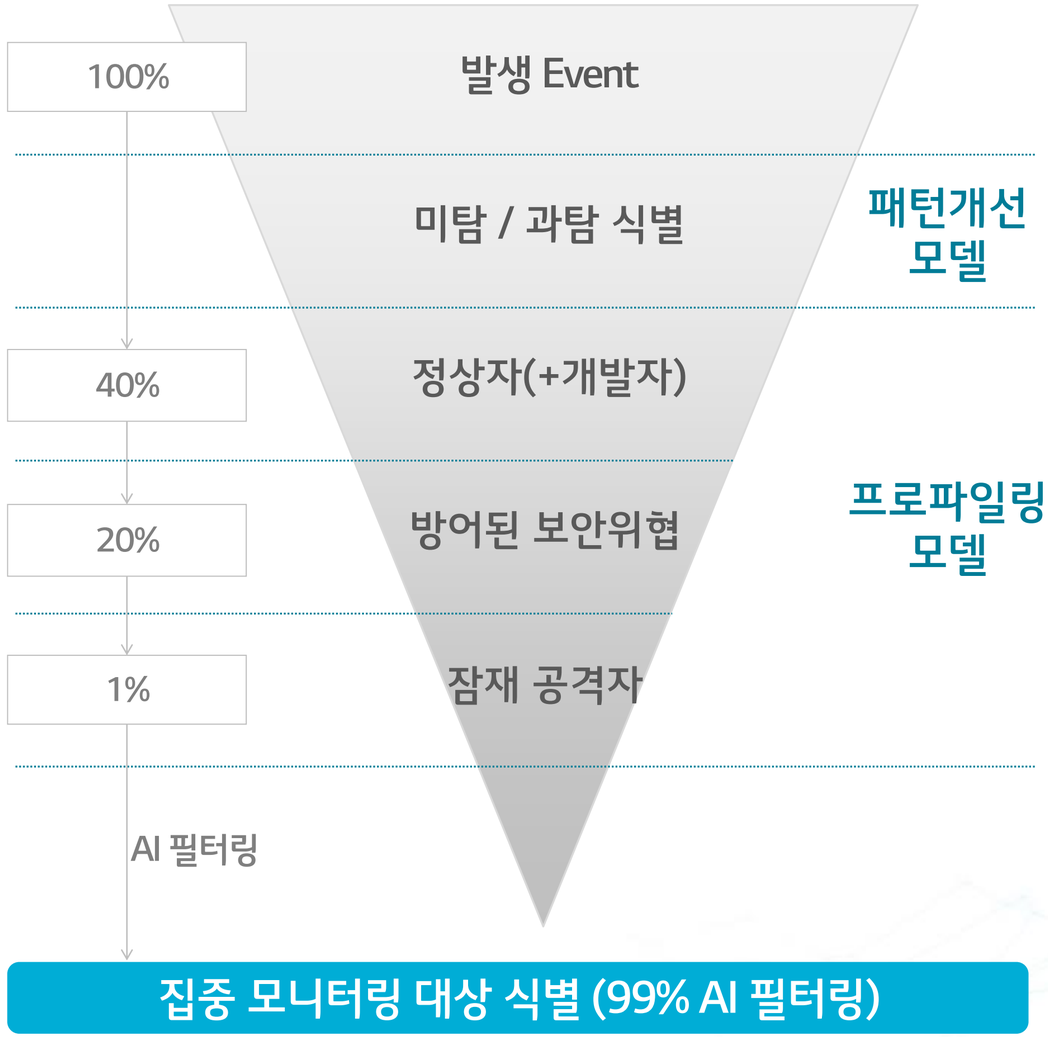
단순 키워드 기반으로 탐지할 수 없는 변형된 공격 시도 탐지 가능

모델 결과

구분	URI	키워드 탐지 여부	AI 분류 모델 탐지 여부
의심 URI	/+CSCOE+/files/file_list.json	N	Y
	/mgmt/tm/util/bash	N	Y
	autodiscover/autodiscover.json	N	Y
정상 URI	mngt/insa.jsp	N	Y

추론 단계의 실제 프로젝트 성과 및 활용 예시

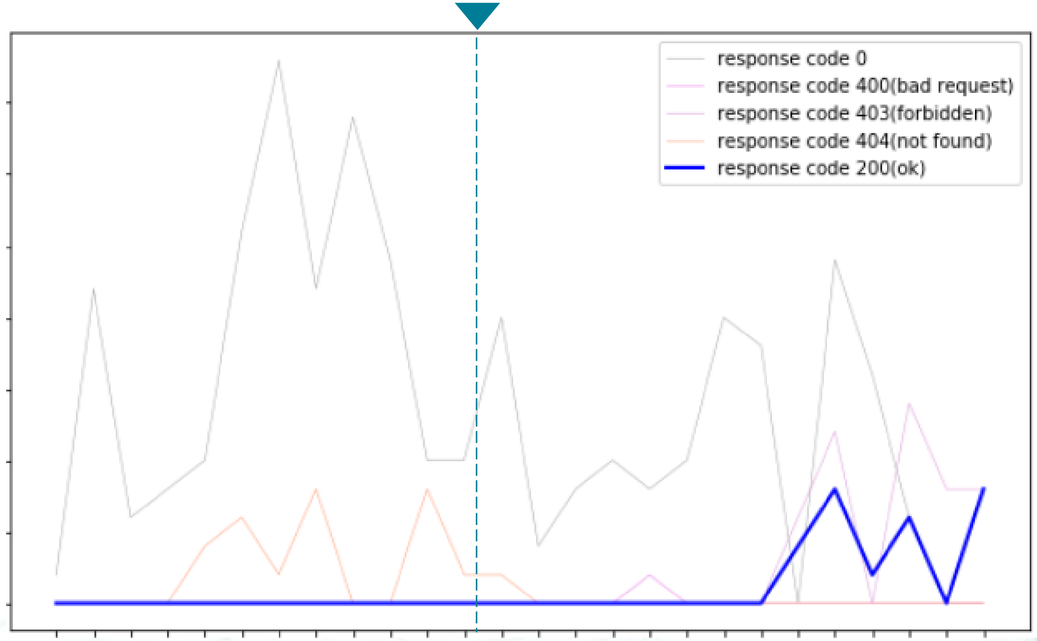
프로젝트 필터링 성과 사례



집중 모니터링 대상 식별 (99% AI 필터링)

추론 결과 활용 예시

공격자 IP가 보안 장비에서
일부는 차단되나
일부는 허용되어
서버 응답 200에 도달한 사례



SecuXper AI 침해 솔루션은 총 23개의 모델을 조합하여 결과를 추론함

예시

패턴개선 AI모델 (판정결과)									이상탐지 AI모델
…	l** 공격징후	패킷 N** 공격징후	s*** 공격징후	User-***** 탐지결과	x_******* 공격징후	패킷 **IP	SQL*** 공격징후	…	추론결과
…	0	0	0	0	1	0	0	…	허용
									차단

예시

프로파일링 AI모델 (판정결과)															이상탐지 AI모델
…	내부망 여부	패킷**	지역**	전역**	에러 rate	패턴 개선 모델 지역**	패턴 개선 모델 전역**	외부 개방 여부	A**	패턴 개선 모델 A**	** IP수	유사도	개발자 *** 분석 결과	…	**추론결과**
…	1	1.389	0.022	0.006	0.254	0.009	0.009	0	0.006	0.000	2	0.267	0.003	…	공격자
															정상자

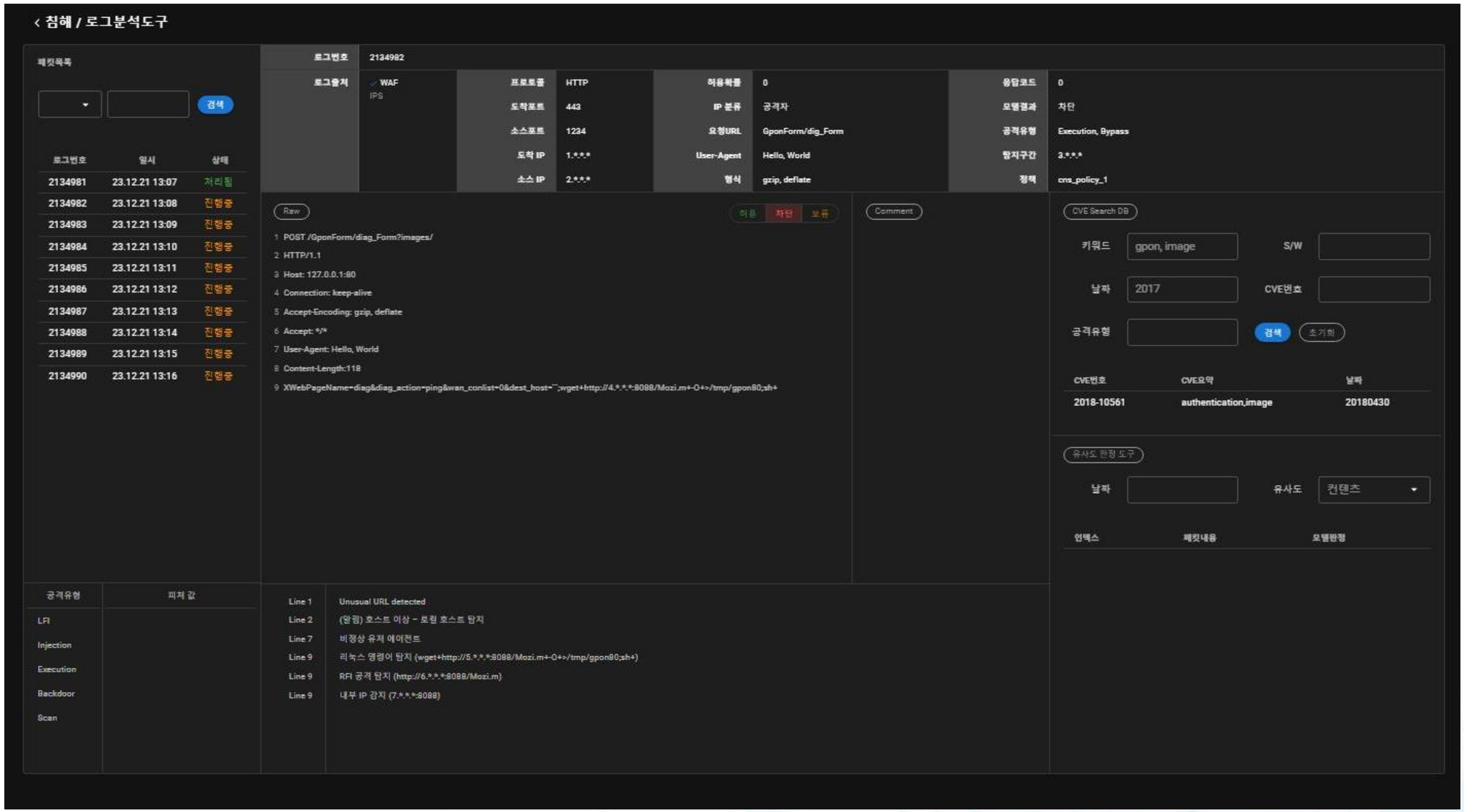
기존 인력베이스 24시간 관제 운영과 AI 기반 운영 비교

	기존 24시간 관제 운영	SecuXper AI 침해관제
1차 모니터링 및 탐지	3교대 근무 관제요원A 관제요원B 관제요원C	
2차 사고 대응 및 분석	보안담당자	SecuXper AI Assistant 보안담당자

4 AI 침해관제 프로세스

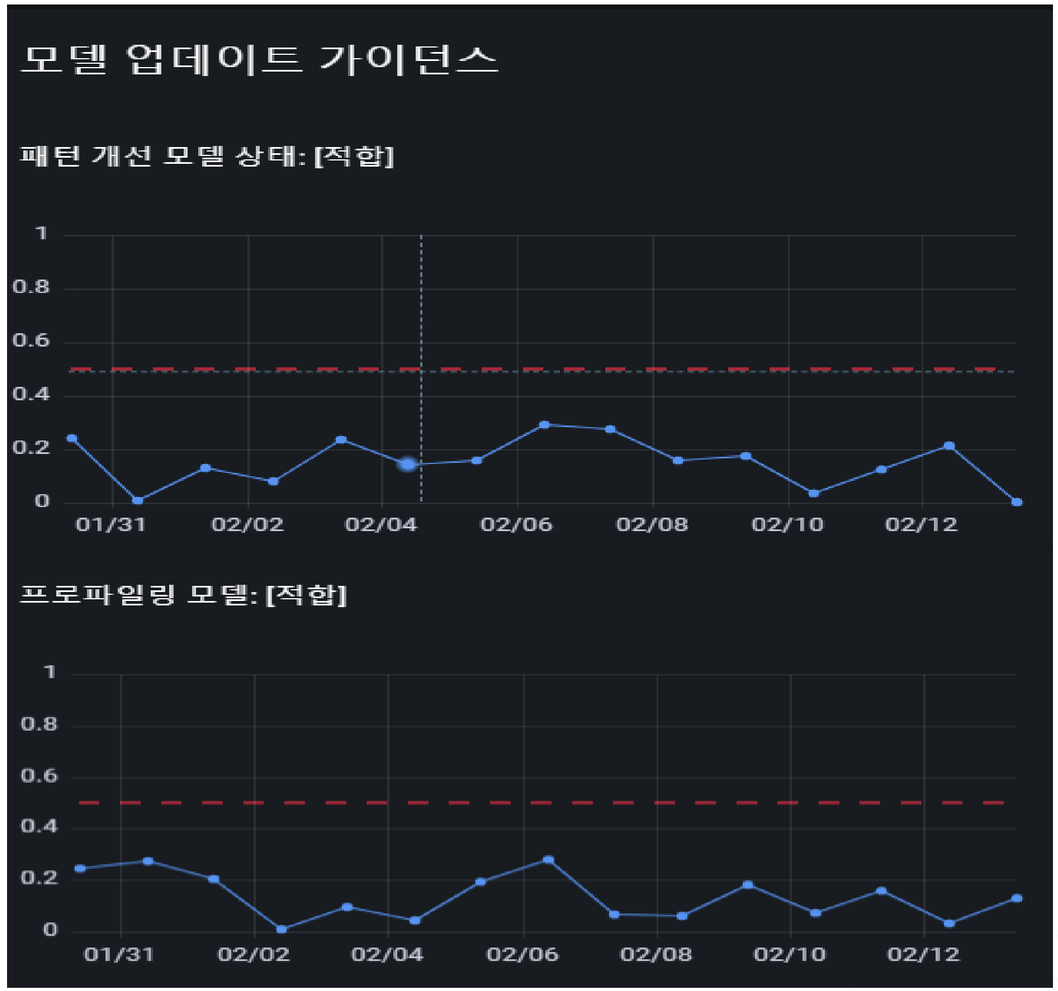
1) 분석 | 2) 추론 | **3) 대응** | 4) 운영

침해 로그에 대한 분석 도구 플랫폼 제공



주기적인 모델 업데이트를 통한 성능유지를 통하여 안정적인 새로운 공격을 탐지하여 제공함

모델 성능 유지



* 산출 방식: 대외비

결과 안정성(새로운 공격 탐지)

구분	패킷 로그	모델결과	
		공격	정상
학습	1") where 3122 = 3122 and sleep(5)	Y	N
	1") where 3122 = 3122 and sleep(50)	Y	N
예측	1") where 3122 = 3122 and sleep(--5)	Y	N
	1") where 3122 = 3122 and sleep(~~5)	Y	N
	" or pg_sleep(__TIME__) --	Unknown	Unknown
	1 and 3824 = benchmark(5000000,md5 (...	Unknown	Unknown

확률기반 결과 분석으로
학습되지 않은 zero-day attack과 같은 신규 공격 탐지

4 AI 침해관제 프로세스

1) 분석 | 2) 추론 | 3) 대응 | **4) 운영**

한눈에 침해 상황을 확인 가능한 대시보드를 제공하며 해당 건에 따른 상세정보 파악 가능

5 SecuXper AI 침해관제 솔루션 특장점

SecuXper AI은 높은 정확도를 기반하며, 침해 특화 모델이 반영 된 대시보드 제공

AI 침해관제 솔루션 특장점

95% 정확도 보장	• 모델 정확도 95% 보장 • 보안 장비 대비 과·오탐 90% 이상 개선
공격자 IP 차단시점 판정	• 보안 장비와 Network Layer간의 정보연계를 통한 공격자 IP 차단시점 판정모델 (사전예방모델)
상세분석 대상 자동 식별	• Daily 잠재 보안 위협자에 대한 케이스 자동 등록 및 분석 결과 제시

AI 침해관제 솔루션 주요기능

침해 특화 모델	• 공격 유형별 특화된 학습 데이터를 이용한 모델 확보 • Network Layer간의 정보공유 모델
대시보드	• 모니터링을 위한 웹 기반 대시보드 제공 • 전체 / 자산 / Client IP 레벨 관점의 대시보드
케이스 분석 도구 with AI	• 패킷 레벨의 모델 분석 및 판정 결과를 종합적으로 판단할 수 있는 도구 • XAI 기반의 사고 대응 Assistant 역할

LG CNS

해킹에 대응하는 AI,
AI Assistant를 통한 24시간 관제방안

Thank you