CipherData

보안 운영의 패러다임 전환

AI-Native Detection and Response (AIDR)

사람을 대신해 탐지·조사·대응까지 자율 수행하는 AI SOC 플랫폼

스마트한 보안 | 즉각 사고대응 | 운영비용 절감

#AIDR #AI_SOC #SecOps

www.cipherdata.ai
sales@cipherdata.ai

THE PROBLEM · 보안관제 현안

보안 전문가 부족이 $10.22M 데이터 유출로 이어집니다

데이터 유출 사고 1건당 피해액 — 미국 평균 $10.22M · 글로벌 평균 $4.44M

초당 수천 건에 달하는 AI 기반 '바이브 해킹(Vibe Hacking)' 위협이 쏟아지지만, 이를 막아야 할 보안 조직은 만성적인 인력난과 경보 과부하에 직면해 있습니다.

480 만명

보안 전문가 부족

만성 번아웃 · 높은 이직률 · 실효성 없는 SOC

3,832 건

매일 발생하는 보안 경고

62% 무시 · 84% 오탐 · 대응 4시간 이상

276 일

대처까지 걸리는 시간

90% 반복 수동 업무 · 비효율 SOC

16 %

AI를 사용한 공격

데이터 유출의 6분의 1 · 정교한 공격

핵심 원인은 "예산 부족"

전 세계 보안 인력 추정치는 545만 명이지만, 추가로 필요한 인력은 480만 명에 달합니다.
아시아·태평양 지역의 인력 격차는 전년 대비 +26.4% 증가하며 가장 빠르게 벌어지고 있습니다.

출처: IBM Cost of a Data Breach Report 2025 · ISC2 2024 Cybersecurity Workforce Study · Vectra 2024 State of Threat Detection

WHY NOW · 지금 도입해야 하는 이유

기다리는 비용이, 도입 비용보다 큽니다

공격은 기다려주지 않습니다

AI 기반 공격이 초당 수천 건씩 쏟아지고, 유출의 6분의 1은 이미 AI를 악용합니다. 미룰수록 노출과 피해가 누적됩니다.

미루는 한 분기마다 비용

인력난·번아웃·놓친 알람·느린 대응(MTTR)이 지금도 매일 비용으로 발생합니다. 다음 예산을 기다리는 손실은 회수되지 않습니다.

지금 가진 도구로 바로 시작

이미 구축된 SIEM·XDR 위에 얹어 즉시 가동 — 신규 구축 없이 이번 예산 주기 안에서 효과를 확인합니다.

THE SOLUTION

AI-Native Detection and Response (AIDR)

인력 부족 상황에서도 100% 사건 커버리지를 보장하는 자율 보안운영 플랫폼

스마트한 보안 | 즉각 사고대응 | 운영비용 절감

200:1

경보 대비 케이스 비율

분류·상관 분석된 경고를 중요한 사건만으로 선별

24×7

자율 운영

인력 부족 상황에서도 100%의 사건 커버리지를 보장

>48×

수일이 아닌, 수분 내 대응

평균 대응(MTTR) 및 사건 해결 시간을 획기적으로 단축

90%

비용 절감

한 명의 전문가 비용으로 최소 10배 이상의 생산성 제공

Agentic Workflow

선제적 위협 탐지

위협이 사건으로 번지기 전 능동적으로 포착

문맥 인식 기반 대응

자산·위협 맥락을 이해해 정확하게 대응

지속적 학습

대응 결과를 학습해 역량을 강화

PROVEN RESULTS · 기술 경쟁력

K-테스트베드 실증으로 기술적 유효성을 입증했습니다

공공기관 보안관제센터에서 2.5개월간 진행된 실증. 5개 기관, 800건의 경보 데이터를 기준으로 인력 중심 SOC(AS-IS)와 AIDR(TO-BE)를 직접 비교했습니다.

구분	AS-IS · 인력 중심 SOC	TO-BE · AIDR 실증 결과	개선
MTTR(건당 대응시간)	35.27분 / 건	**1.53분 / 건**	**23× ↓**
시간당 위협 처리	1.7건 (인력 10명)	**39.21건**	**23× ↑**
위협 판정 방식	100% 수동 판정	**AI 자동 판정**	—
업무 구조	Alert 분류·조사·보고에 인력 대부분 투입	**85% 즉각 판단·조치, 인력은 Suspicious에 집중**	—

23×
MTTR 단축
35.27분 → 1.53분

23×
처리량 증가
시간당 1.7건 → 39.21건

84.67%
AI 자동 판정 비중

사람 10명이 하던 일을, AI가 더 빠르고 정확하게

실증 환경에서 AIDR은 대응 속도와 처리량을 23배 끌어올려, 업무 구조를 효율적으로 혁신합니다.

HOW IT WORKS

보안 플라이휠로 비즈니스 리스크를 감소

방대한 이벤트를 '실행 가능한 소수의 과제'로 압축하는 AIDR 파이프라인

600K Events › **200** Alerts › **20** Incidents › **1** Attack Chain › **Action** Actionable Task

Alert Detection

EDR·NDR·SIEM·IAM
전 영역 이벤트에서 유의미한 경보를 탐지

Incident Detection

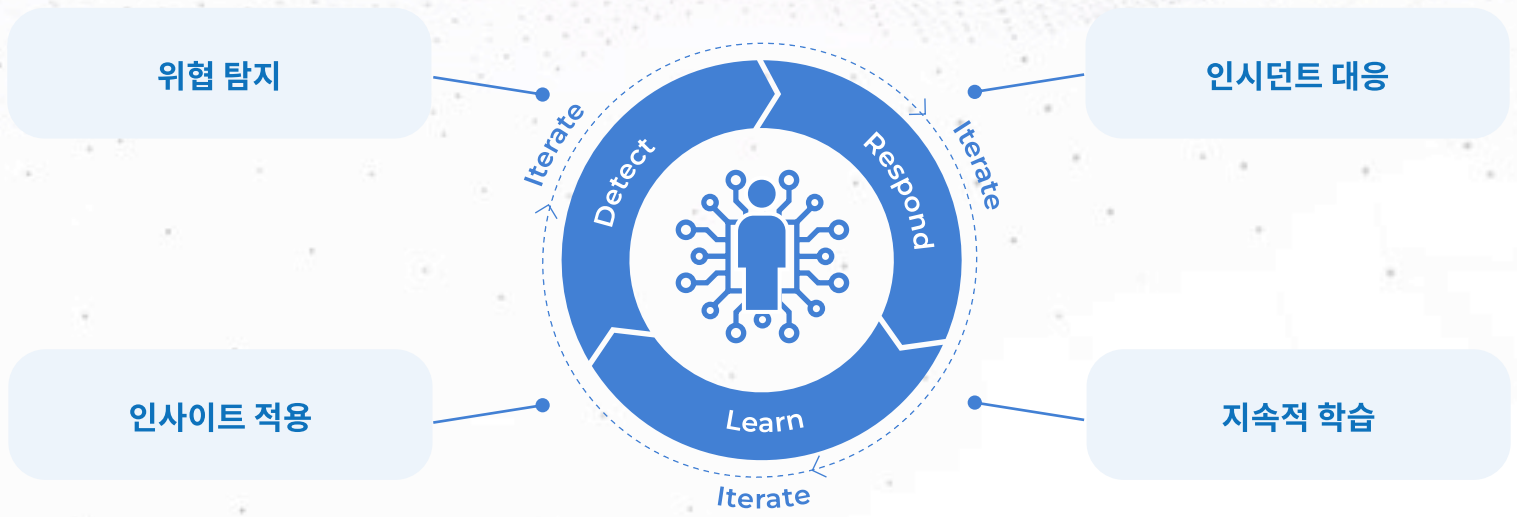
상관 분석으로 흩어진 경보를 실제 인시던트로 묶음

Attack Chain

공격 체인 단위로 위협의 전체 흐름을 재구성

AI-Powered Response

실행 가능한 과제로 변환해 자율 대응 및 조치



플라이휠 효과

위협 탐지 → 인시던트 대응 → 인사이트 적용 → 지속적 학습의 선순환. 대응을 거듭할수록 정확도와 자동화 범위가 함께 커집니다.

전 영역 커버리지

Network · Endpoint · Cloud · Apps에 걸친 데이터 소스를 통합해 단일 화면에서 위협을 탐지하고 대응합니다.

PLATFORM IN ACTION

워크플로우의 90%를 AI가 자동 완료합니다

기존 인력 기반(SIEM/XDR) 보안관제 vs. AIDR 자율 보안관제

기존 인력 기반 SOC

- **Triage**: 경보 피로 · 오탐 · 맥락 정보 부족
- **Investigate**: 수동 로그 검색 · 이벤트 분석
- **Mitigate**: 수동 대응 조치 · 대응 지연 리스크
- **Remediate**: 복잡하고 오래 걸리는 근본 원인 분석
- **Comply**: 개인정보 보호 규정 · 법적 검토 필요
- **Report**: 번거로운 수동 보고서 작성

CipherData AIDR

90% 워크플로우 자동화 완료

- Triage·Investigate·Mitigate·Remediate를 AI가 자율 수행
- 잔여 10%의 업무만 전문가 검토 과제로 전환
- 전문가는 고난도 의사결정·승인에만 집중

분석가의 역할이 '수동 처리'에서 '검토·승인'으로 바뀝니다

반복적이고 소모적인 90%의 관제 업무를 AI에 위임하고, 사람은 판단이 필요한 핵심 과제에만 집중함으로써 SOC의 생산성과 만족도를 동시에 끌어올립니다.

전체 공격 체인을 꿰뚫는 하나의 보안 플랫폼

자격 증명 악용부터 횡적 이동까지 — 탐지·조사·대응을 한 곳에서

전체 공격 체인 가시성

Initial Access · Discovery · Lateral Movement · C&C까지 공격의 전 단계를 하나의 타임라인으로 시각화합니다.

Incident Details

Overview · Investigation · Assessment로 구성된 사건 상세 화면에서 위협의 맥락을 즉시 파악합니다.

Playbook · Mitigation

상황에 맞는 완화 조치를 플레이북으로 자동 생성하고 실행 가능한 과제 형태로 제시합니다.

Chat-bot & Dynamic Query

자연어 요청만으로 위협 분석용 쿼리를 자동 생성해 추가 조사를 손쉽게 수행합니다.

BUSINESS MODEL

연간 구독형 플랫폼

AIDR Core · AIDR 360 · 사용량 기반 Add-ons

AIDR Core

$120K / 연

40K Investigations

- ✔ Alert Collection
- ✔ Incident Detection
- ✔ Context Discovery
- ✔ Dynamic Response Plan
- ✔ Essential Support

AIDR 360

$240K / 연

40K Detections + 40K Investigations

- ✔ Event / Log Collection
- ✔ Alert Detection
- ✔ Attack Chain Detection
- ✔ Proactive Investigation
- ✔ Continuous Learning
- ✔ AIDR Core 전 기능 포함

Add-ons

Usage-based

필요에 따라 유연하게 확장

- + 10K Investigations — $30K
- + 10K Detections — $30K
- + Single-Tenancy (Ent/Premium)
- + Premium Tech Support

40,000 Investigations
= Tier 1 분석가 10명의 평균 처리량

동일한 업무량을 처리하는 경쟁사 솔루션 가격은 **$360K**. AIDR Core는 그 ⅓ 수준인 $120K로 동등 이상의 성능을 제공합니다.

TEAM & CONTACT

현장의 문제를 20년간 겪은 당사자가 만듭니다

압도적인 창업자의 시장 적합성

Kevin Ha · Founder & CEO

- **Meta** (Head of Privacy Incident Response Eng)
- **Amazon** (Head of Security Eng, Alexa AI)
- **Poshmark** (VP, Security)
- **Symantec** (Principal Software Engineer)

세계적 수준의 R&D 팀

가장 신뢰하는 전 동료와 전문가들

AI	Google DeepMind	amazon alexa
Detection	Microsoft	Symantec
Engineering	SAMSUNG	NAVER

글로벌 R&D, 국내 밀착 지원

시애틀과 실리콘밸리에서 세계 최고 수준의 보안과 AI를 다뤄온 팀이 미국 본사를 두고, 서울 지사를 통해 국내 보안 현장 바로 곁에서 함께합니다.
글로벌 수준의 자율 보안운영을, 한국 환경과 규제에 맞춰 가장 가까운 거리에서 전달합니다.

US Headquarters — Bellevue, WA, USA

KR Seoul Office — 서울 강남구 삼성동

CipherData

AIDR을 데모로 직접 확인해 보세요

데모부터 PoV까지, 현재 보안 환경에 맞는 도입 방안을 검토해 드립니다.

라이브 데모 | PoV | 도입 상담

www.cipherdata.ai

sales@cipherdata.ai