Case Study

AI는 보안관제를 어떻게 바꾸고 있을까요?

Datadog Security와 AI 관제로 위협을 탐지 · 대응한 3가지 사례

DATADOG PARTNER

MetanetX

탐지도 AI로, 대응도 AI로

Datadog은 인프라, App, 보안 등 흩어진 로그를 한곳에 모으고, AI가 이상징후를 탐지하는 All-in-one 플랫폼입니다.
이 플랫폼과 연계된 **메타넷엑스 AI 보안관제센터**의 AI 에이전트가 위협을 자동으로 분석·대응합니다.

메타넷엑스 차세대 보안관제 서비스
: MSSP with Datadog

End-to-End 모니터링

DATADOG

인프라, 로그, APM, RUM, 보안을 하나의 스택으로 연결합니다

Security

클라우드 에러부터 런타임 위협까지 실시간 탐지하고,
운영 데이터와 연계 분석해 맥락까지 파악합니다.

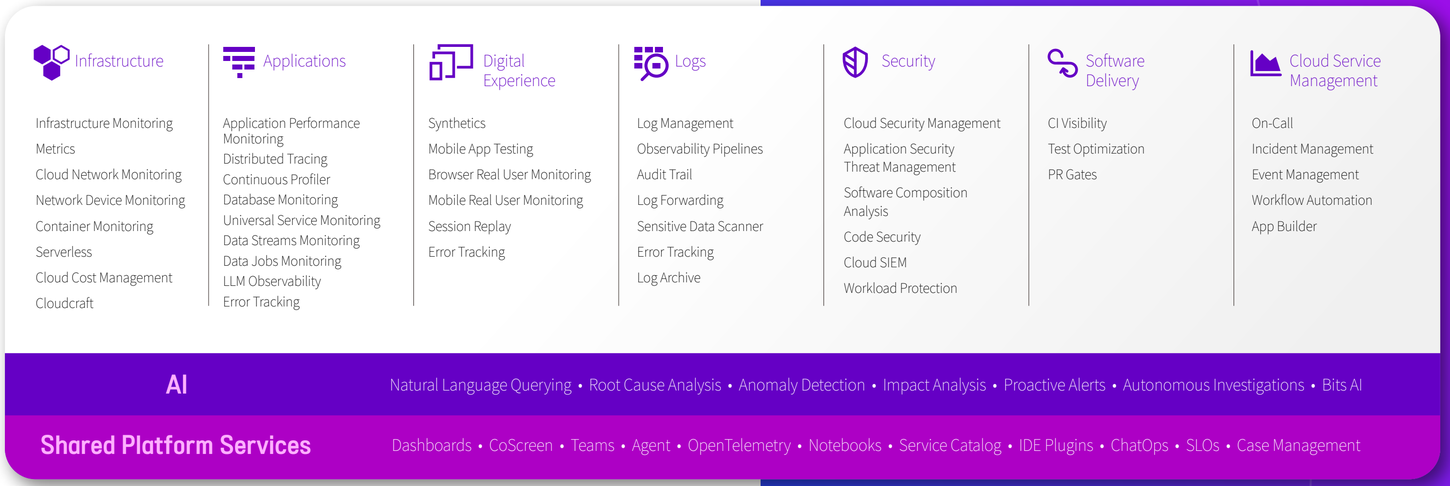
Bits AI

AI 에이전트가 이상 징후를 자동 탐지하고 원인 조사까지 수행합니다.
보안 경보 분석을 단축하고, 신규 위협도 선제적으로 찾아냅니다.

AI 보안관제센터 (AI SOC)

MetanetX

AI Agent가 1차 조사 · 검증을 자동 수행하고, 메타넷엑스의
보안 전문가가 최종 판단 · 조치합니다. 24x 365 자동화
기반으로 운영되는 관리형 보안관제 서비스입니다.



탐지 · 수집

- 이기종 로그 통합
- Mythos 위협
- 위협 헌팅

AI 자율 조사

- 신호 연관분석
- 근거 기반 검증
- 위험도 우선순위화

대응 · 조치

- 위협 유형별 자동 대응
- 선제 차단·격리
- 계정·세션조치

운영 · 거버넌스

- 침해 사고 소명 추적
- ISMS-P 등 인증 대응
- 정기 분석 리포트

AI Agent

Case. A사 개요 및 배경

M365 계정 탈취, 아무도 몰랐습니다

피싱·세션 탈취에 대응한 보안관제 구축 사례

전사가 Microsoft 365로 업무를 처리하는 글로벌 하이테크기업 A사.
IT 담당부서에서 한정된 인력이 계정 · 권한 · 문의 · 장애 대응을 함께 맡고 있었습니다.

A사 보안 운영의 현실

M365 로그는 계속해서
남고 있었지만,
보는 사람은 없었습니다.

▼

보안에 취약할 수 밖에 없는 상황이었고, 실제 협력업체를 위장한 공격을 받았습니다.



실제 공격 전개 :

정상 활동으로 위장해 침입



① **세션 탈취** (MFA 우회)	협력사 사칭 피싱으로 로그인 세션을 가로챔
② **흔적 은폐**	받은 편지함 규칙을 심어 수신 메일 자동 삭제
③ **2차 피싱 확산**	신뢰받는 내부 계정으로 내외부에 재발송

▼

비밀번호 재설정 만으로는 차단 불가능한 상황

“ 침해인지 아닌지, 어떻게 구분할 수 있었을까요? ”

Case. A사 해결 방안 및 효과

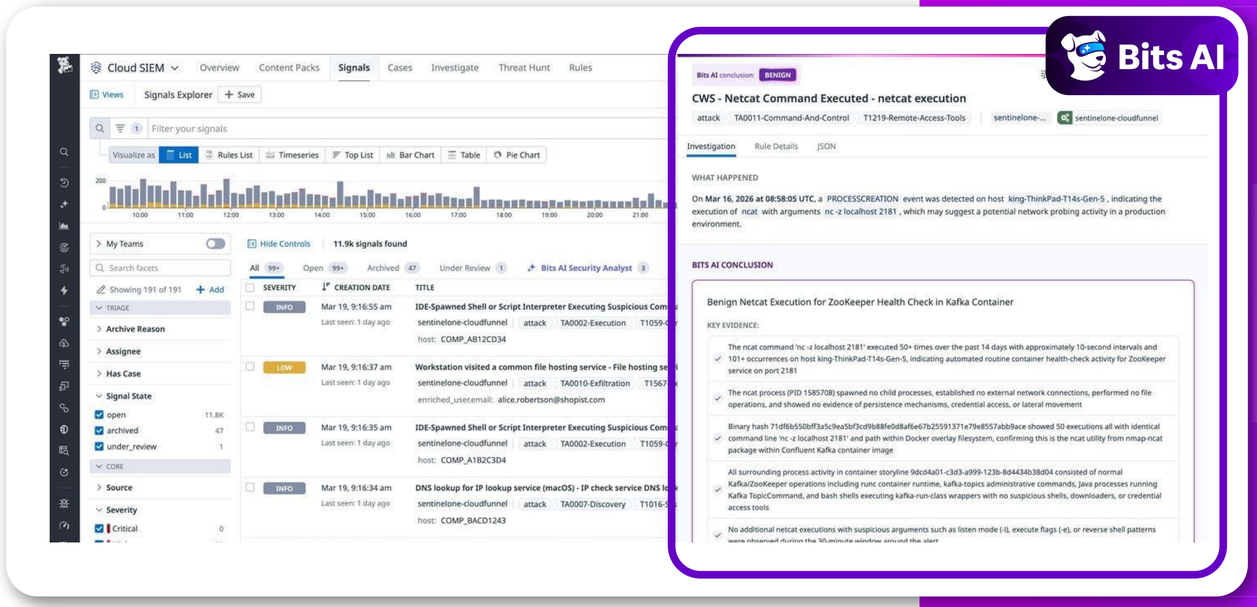
수집 → 조사 → 검증까지 모두AI Agent가

AS-IS	TO-BE
로그를 하나씩 확인	AI 에이전트가 연관 신호 자동 조사
개별 경보 단위로 판단	침해 흐름 단위로 자동 판단
비밀번호 재설정 수준의 대응	세션 · 규칙 · 인증까지 완전 조치

“ 비밀번호로 못 막는 공격을, 초기에 차단했습니다.”

① Datadog Cloud SIEM

Datadog 플랫폼에서 AI가 흩어져 있던 신호의 판별 결과를 만들어 냈고,



② AI 보안관제센터

AI SOC의 AI Agent가 조사 · 검증해 계정 탈취 공격에 대응했습니다.



Case. B사 개요 및 배경

공격자와 고객이 같은 문으로 들어온다면?

크리덴셜 스터핑에 대응한 자동화 관제 구축 사례

온·오프라인 채널을 함께 운영하는 글로벌 리테일 기업 B사.
DevOps팀이 배포·인프라 운영에 App·API 보안까지 맡고 있었습니다.

B사 보안 운영의 현실

로그인 실패는 늘어났지만,
DevOps 팀에서는 원인을
알수 없었습니다.

▼

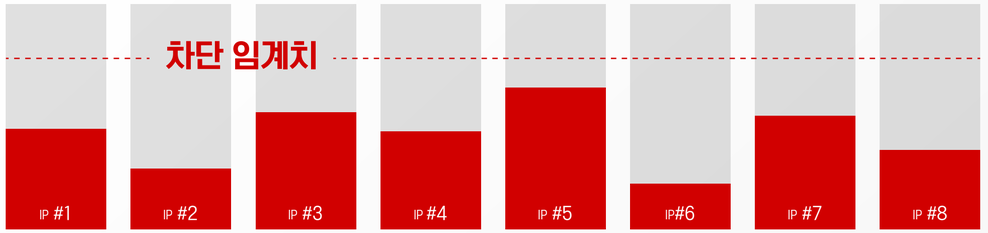
**가장 어려운건 판단.
차단은 언제든 가능했지만,
무엇을 차단할지가
문제였습니다.**



"어떻게 공격만 판별해 차단했을까요?"

실제 공격 전개 패턴 :
임계치 아래로 나눠 분산 침입





분산된 다수 IP로 공격: 개별 요청량은 모두 임계치 미만

▼

※ 일부 계정은 로그인 성공해 정상 트래픽에 묻힘
※ IP를 일괄 차단하면 실제 고객까지 막힐 수 있음

Case. B사 해결 방안 및 효과

고객은 통과 시키고,
공격만 골라 막는 AI

AS-IS	TO-BE
IP 목록을 수기로 정리해 차단	AI가 캠페인 단위로 자동 판별
오류율만으로 공격 여부 판단	오차단 위험까지 계산해 자동 판정
대응까지 수십분 소요	담당자는 승인 여부만

“ AI가 스스로 판단하게 하고, 자동으로 차단했습니다.”

① Datadog App & API Protection
API 및 요청 패턴 분석

↓

Workflow Automation
자동화 사전 정의

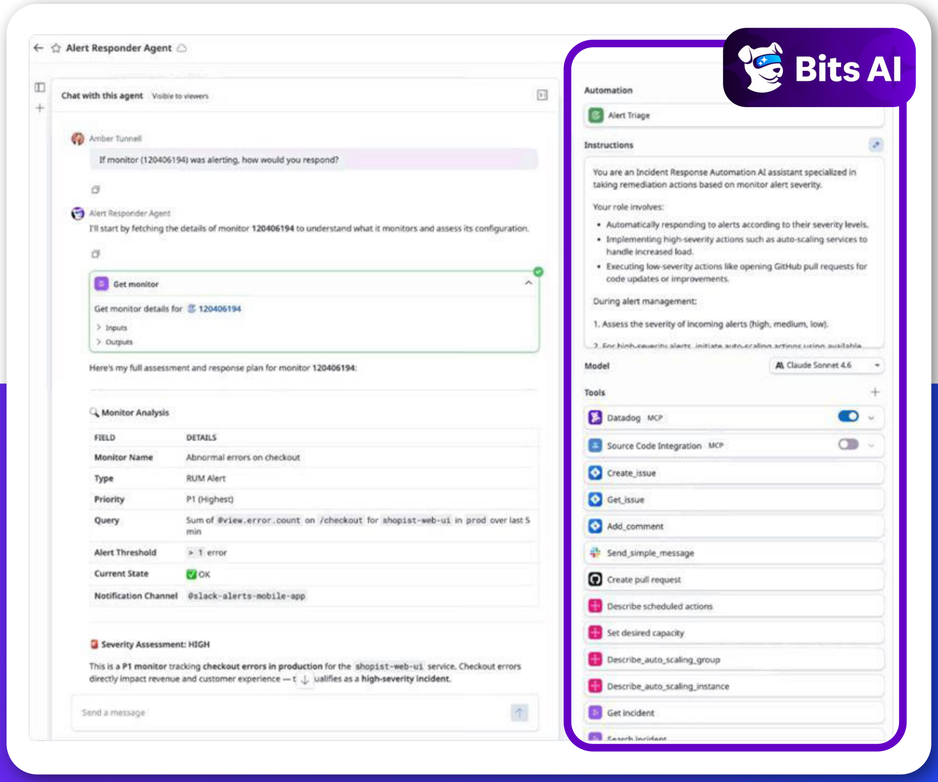
위험 명확 → 자동 차단
사전 승인된 룰이 방어 장비 API를 호출해 즉시 차단

판단 어려움 → 승인 후 차단
Slack·Jira 등 즉시 요청 담당자 승인 후 차단·통보

Ticketing

② AI 보안관제센터 MetanetX

AI Agent 로그인 계정 추가 조사, 추론 → **보안 전문가** 세션 폐기 및 계정 조치



Case. C사 멀티 클라우드 계정 통합 거버넌스 구축

복잡한 계정 보안, 사각지대가 사라졌습니다

흩어진 클라우드 계정을 단일 기준으로 통합한 거버넌스 구축 사례

계열사·사업부가 각자 클라우드를 운영하는 대기업 계열 서비스 기업 C사.
계정이 수백 개로 늘며 생성일·관리 조직·보안 기준이 제각각이었습니다.

C사 보안 운영의 현실

점검 대상을 늘려도,
불안은 줄지 않았습니다.



**위험을 분석할 시간보다,
담당자를 찾는 시간이
더 길었습니다.**

“ 보안 수준을 ‘숫자’로 관리할 수 있게 되었습니다.”

해결 방안

AS-IS 기준 제각각 사각지대 존재



Datadog CSM Bits AI AI 기반 계정 자동 수집 → 단일 기준 적용 및 분류

TO-BE 단일 기준 관리·가시화



전체 계정 중 공통 기준 적용 비율 : 87.5%

Contact Us

더 궁금한 부분이 있으신가요?

사례집에 모두 담지 못한 실제 수치와 상세 적용 과정들,
상담을 통해 직접 안내해 드립니다.

바로 시작해보는 6주 PoC 프로그램

자사 환경에서 탐지 결과와 운영 방식을 직접 검증해보세요!
구축 부담 없이 상시 신청 가능합니다.

→ PoC 신청하기

도움이 필요하신가요?

AI 전환을 위한 클라우드 구축, 운영 및 보안 등
메타넷엑스 전문가에게 상담받아 보실 수 있습니다.

→ 문의하기