Zeclue
AI-Driven DFIR & Audit Copilot

AI 기반 디지털 포렌식 · 하이브리드 RAG · Agent · SIEM 연계

Zeclue — 증거로 답하는 AI 기반 디지털 포렌식

경보에서 증거로, 증거에서 보고서로
AI 자동화 사고대응 포렌식

보안장비와 관제 시스템의 경보를 받아 필요한 증거를 수집하고, 원본을 보존한 채 분석해 근거가 달린 조사·감사 보고서를 만듭니다. 기존 EDR·방화벽은 그대로 두고 옆에서 연계합니다.

Zeclue Desk
현장 조사관용 포터블 패키지

Zeclue Server
중앙 통합 · 협업 분석 플랫폼

왜 필요한가

지금의 사고 조사

- ✕ 경보가 와도 장비마다 따로 확인하고, 증거는 현장에 가서 수동으로 복사
- ✕ 모바일 · PC · 서버 기록이 흩어져 공격 경로를 잇기 어려움
- ✕ 출처가 불분명한 AI 답변은 감사·법정 자료로 쓰기 어려움

Zeclue와 함께

- ✓ 경보를 모아 조사 우선순위를 정리하고, 원격 Agent 또는 현장 USB로 필요한 증거만 수집
- ✓ 여러 기기와 장비 로그를 하나의 사건 타임라인에서 분석
- ✓ AI가 쓴 문장마다 원본 증거를 표시해 누구나 근거를 다시 확인

사고대응 흐름

1. **경보 수신** — SIEM · 방화벽 · WAF 등 기존 장비
2. **AI 트리아지** — 경보 정리 · 조사 우선순위
3. **증거 수집** — 원격 Agent 또는 현장 USB
4. **봉인 · 분석** — 원본 보존 · 통합 타임라인
5. **차단 권고** — 사람 승인 · 2단계 인증 후 연동
6. **보고서** — 경영진용 · 분석가용

이런 조직에 맞습니다

공공 · 국방 감사실
내부 감사, 정보 유출 조사

수사기관
디지털 증거 선별 수집 · 분석

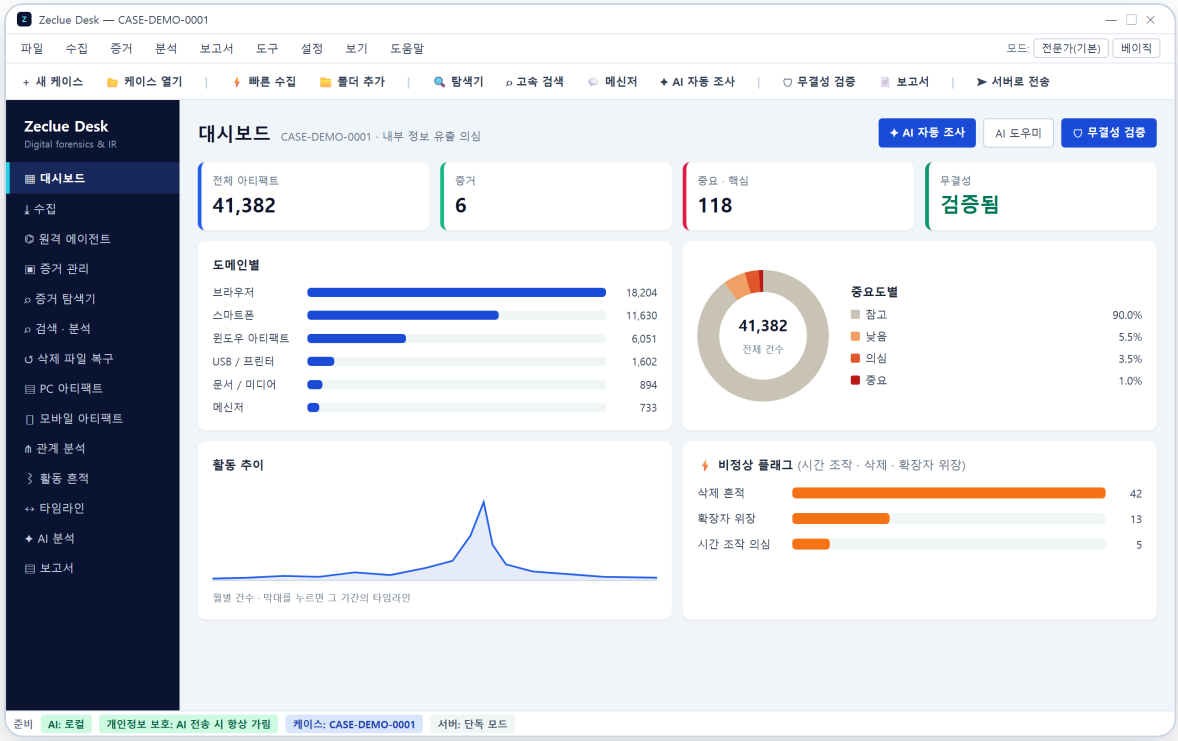
CERT · SOC
침해사고 원인 규명 · 대응

기업 보안 · 감사팀
사고 보고서 · 재발 방지

Zeclue는 사후 증거 분석 · 차단 권고 · 감사 보고서 작성을 돕는 소프트웨어입니다. 실시간 차단 장비나 EDR 대체 제품이 아닙니다.

제품 라인업 · 화면

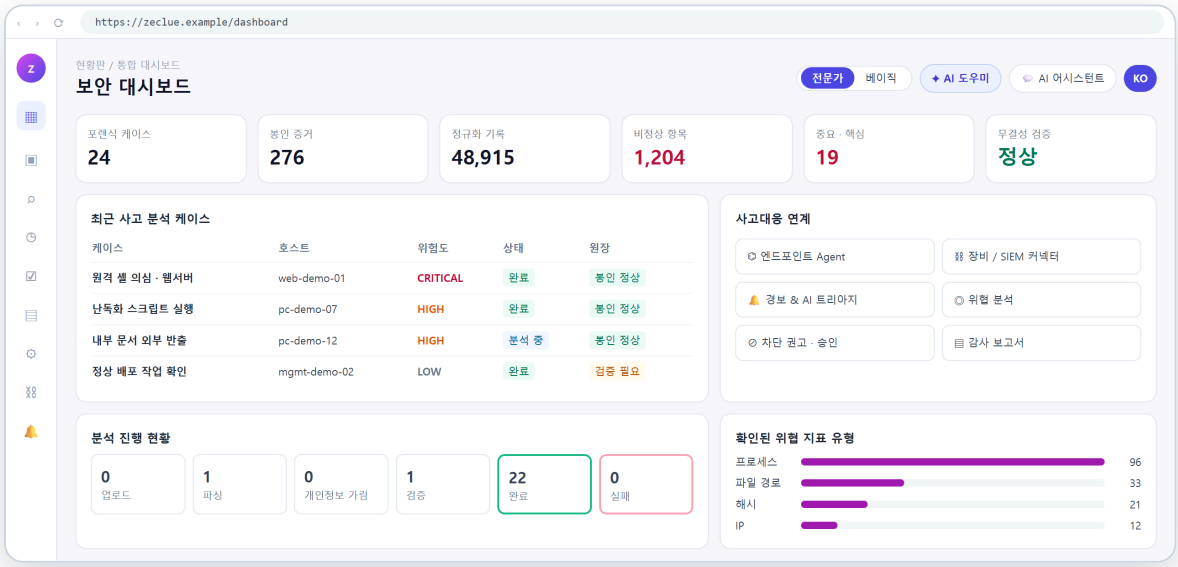
Zeclue Desk 현장 조사관용 포터블 패키지



Zeclue Desk · 케이스 대시보드 (화면 예시 · 합성 데이터 · 실제 화면은 상담 시 시연)

- 설치 없이 USB · 외장 SSD에서 바로 실행
- 선별 압수 확인서 · 해시 목록 출력
- PC · 모바일 증거 선별 수집과 빠른 검색
- 봉인한 증거 묶음을 Server 케이스로 전달
- 작업 위치를 외장 저장장치로 지정해 흔적 최소화
- 대상 · 현장 수사관, 1인 보안 · 감사 담당자, 출장 조사반

Zeclue Server 중앙 통합 · 협업 분석 플랫폼



Zeclue Server · 보안 대시보드 (화면 예시 · 합성 데이터 · 실제 화면은 상담 시 시연)

- 엔드포인트 Agent · SIEM / 보안장비 연계
- 근거가 표시된 AI 조사 브리핑 (폐쇄망 로컬 AI)
- 모바일 · PC · 서버 · 장비 로그 통합 타임라인
- 차단 권고 → 사람 승인 · 2단계 인증 → 연동 · 되돌리기
- 공격 경로 관계도 시각화
- 대상 · 공공 · 국방 감사실, CERT, 대기업 · 금융 SOC

주요 기능

시간 조작 · 위장 파일 탐지
파일 날짜 조작과 확장자 위장 흔적 표시

하이브리드 RAG AI 분석
사건 기록에서 근거를 찾아 증거 번호와 함께 답변

모바일 이상 징후
초기화 · 앱 삭제 흔적을 PC 기록과 한 타임라인에

금융 · 가상자산 단서
계좌 · 지갑 주소 단서 정리와 흐름 시각화

개인정보 보호
AI 분석 · 외부 전송 시 개인정보 자동 가림

사람 승인 안전장치
장비 변경은 승인 · 인증 후에만, 되돌리기 지원

신뢰 · 보안 원칙

- 원본 증거는 읽기 전용, 분석은 사본에서만
- 누가 · 언제 · 무엇을 했는지 감사 기록
- 인터넷이 끊긴 폐쇄망 · 온프레미스 구축
- 수집 시점에 원본 해시(SHA-256)로 봉인
- AI는 권고만, 장비 변경은 사람이 결정
- 외부 AI는 기관이 허용한 경우에만 사용

도입 방식

- 기관 규모에 맞춘 온프레미스 구축
- 기관 환경 · 기존 장비에 맞춘 PoC(시범 적용)
- 구독형 이용 지원 (별도 협의)
- 16년 수사기관 · 대규모 서비스 보안 실무 경력의 대표가 직접 개발 · 지원

상담 신청 · PoC 문의

환경(폐쇄망 여부), 대상 기기, 사용 중인 보안장비, 희망 일정을 알려 주시면 맞춤 시연을 준비해 드립니다.

이메일 **skyjesus111@gmail.com**
웹사이트 **zeclue.com**

본 자료는 공개용 요약본입니다. 세부 기술 자료는 비밀유지 협약(NDA) 후 별도로 제공합니다. 제품 사양과 연락처는 사전 고지 없이 바뀔 수 있습니다.

Copyright © 2026 Zeclue. All rights reserved.