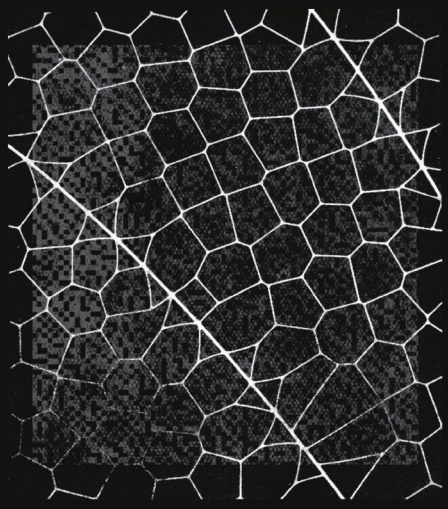
hackerone

Project Glasswing

Securing critical software for the AI era

ANTHROP\C 엔트로픽



CTEM:

(Continuous Threat Exposure Management)

CTEM은 2022년 **가트너(Gartner)**에서 기존 사후 반응적인 취약점 관리의 한계를 지적하며 정립한 개념으로 **지속적인 위험도 순위 적용 노출관리**를 적용한 보안 서비스를 뜻합니다.

2026년까지 CTEM 프로그램을 통해 보안 투자 우선순위를 정하는 기업은 **가시적 보안 침해 사고를 2/3(약 67%)가량 감소** 시킬 수 있을 것이라는 예측을 내놓으며 전 세계적인 트랜드로 유행시켰습니다.

다양한 글로벌 보안 기업들이 CTEM 서비스를 제공 중이지만, **여러 보안 기술**(외부 공격 표면 관리, 공격 경로 분석, 취약점 관리 등)이 **융합된 플랫폼** 형태로 제공하는 곳은 **해커원**뿐입니다.

해커원은 CTEM의 5단계 전체에 대한 서비스를 제공해드리며 **'인간 공격자 기반의 위협 노출 검증(Crowdsourced Security Validation)'** 영역에서는 전 **세계 1위**로 손꼽히고 있으며, CTEM 개념을 온전히 시스템으로 구현한 곳은 **해커원**이 **유일**합니다.

超 AI 공격 대응을 위해

글로벌 기업이 선택한 서비스

Anthropic · Cloudflare · Malwarebytes · Qualcomm · aws · KRAFTON

미국국방부 · 미 연방준비위원회 · 영국국방부 (Ministry of Defence)

Goldman Sachs · PayPal · coinbase

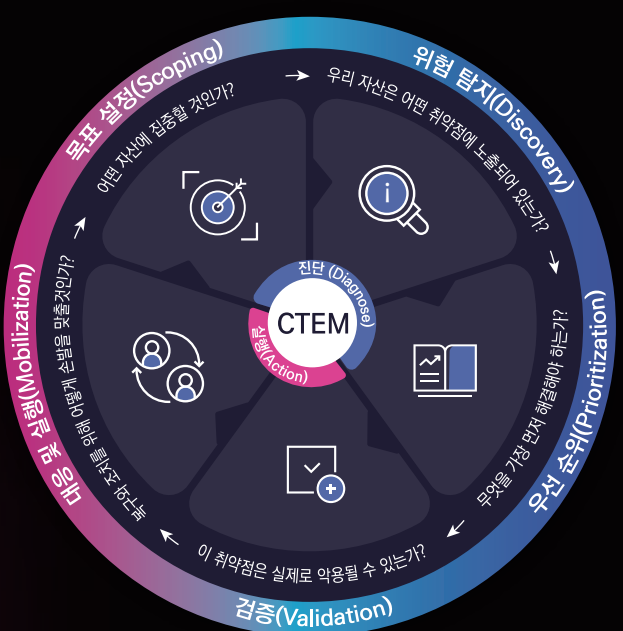
Lufthansa Nonstop you · IKEA · TOYOTA

CTEM (Continuous Threat Exposure Management)

지속적인 위험도 순위 적용 노출관리를 통한 고객의 보안 프로그램 강화

CTEM:

- 목표 설정(Scoping)
- 위험 탐지(Discovery)
- 우선 순위(Prioritization)
- 검증(Validation)
- 대응 및 실행(Mobilization)



H1 플랫폼: 지속적 위협 노출 관리(CTEM)

제품군

H1 지속적 보안 테스트 | H1 바운티 | H1 코드 | H1 에이전틱 모의해킹 | H1 AI 레드팀 | H1 검증 | H1 취약점 조치

H1 플랫폼 — 에이전틱 오케스트레이션

CTEM 운영 사이클

공격 표면 식별

- 지속적인 공격 표면 범위 확보
- 지속적인 모의 공격 테스트
- 필요 시 수행하는 표적형 보안 테스트
- 취약점 신고 및 공개 관리

검증 및 우선순위 지정

- 실재 악용 가능성 검증
- AI 기반 위험도 평가 및 우선순위 산정
- 중복 취약점 제거 및 오탐 감소
- 위협 정보 강화 및 보안 맥락 분석

취약점 조치

- 상황 인지 기반 담당자 자동 할당
- 소스코드 기반 수정 가이드 제공
- 조치 결과 검증
- 재발 여부 지속 모니터링

핵심 플랫폼 기능

H1 게이트웨이 | H1 연동 및 통합 | H1 자동화 | H1 분석 및 위협 인텔리전스

커뮤니티

보안 연구원 (Security Researchers) | 레드팀 (Red Teamers) | 침투 테스트 전문가 (Penetration Testers) | 보안 엔지니어 (Security Engineers)

관리형 및 전문 서비스

Hai 트리아지 | 보안 자문 서비스 | 라이브 해킹 이벤트 | 기술 계정 관리

가장 중요한 영역부터 시작하십시오

각 단계별 최적의 솔루션을 활용하여 취약점을 발견하고 검증하며, 조치할 수 있습니다.

가장 어려움이 많은 부분부터 시작하십시오. 각 제품은 H1 플랫폼 전체로 연결되는 관문이며, 고객의 요구에 맞게 설계되었을 뿐만 아니라 향후 요구사항이 변화함에 따라 확장할 수 있도록 구축되어 있습니다.

Hai

해커원의 에이전트 기반 AI 오케스트레이터 'Hai'는 모든 단계에서 에이전트들을 조율하고, 결과를 지속적으로 평가 및 검증하며, 우선순위 결정 시간을 기존의 몇 시간에서 몇 초로 단축합니다.

H1 상시 테스트

상시 운영되는 AI 에이전트 기반 테스트를 통해 애플리케이션 전반에서 취약점을 지속적으로 발견하고 검증하며, 실제 악용 가능성까지 입증합니다.

H1 코드

AI 기반 코드 보안 분석과 보안 전문가의 검증을 결합하여 개발 단계에서 취약점을 조기에 식별하고, 수정 완료된 결과를 기존 워크플로우에 제공합니다.

H1 검증

불필요한 경고와 오탐(Noise)을 제거하고, 95% 수준의 정확도로 검증합니다. 이를 통해 보안팀이 처리해야 하는 유효 보안 신호(Signal)의 품질을 40% 향상시킵니다.

H1 에이전틱 모의해킹

AI 기반 침투 테스트를 통해 공격 표면 규모에 맞춰 테스트 범위를 유연하게 확장할 수 있으며, 기존의 제한된 기간 중심 침투 테스트에 비해 깊이 있는 분석과 빠른 검증을 제공합니다.

H1 바운티

세계 최고 수준의 보안 연구자들이 자동화 도구로는 발견하기 어려운 핵심 취약점 (새로운 공격 체인, 비즈니스 로직 취약점 등)을 식별합니다.

H1 AI 레드팀 테스트

OWASP LLM Top 10, MITRE ATLAS 및 NIST AI RMF에 맞춰 설계된 다양한 AI 기반 서비스에 대해 적대적 공격 관점의 보안 검증을 수행합니다.

hackerone

UNET × SCK
www.unet.kr
02-2088-3030
www.sckcorp.co.kr
02-2187-0114