Sparrow MCP

AI 생성 코드 보안 어시스턴트

이미 개발 환경은 AI 중심으로 재편되고 있습니다.

Claude Code, Codex와 같은 AI 코딩 에이전트는 많은 개발 조직에서 코드 작성과 리뷰 과정에 적극 활용되고 있습니다. 특히 바이브 코딩(Vibe Coding)이 확산되면서 비개발자도 요구사항을 자연어로 전달하며 개발에 참여할 수 있게 되었고, 이에 따라 개발 진입 장벽은 낮아지고 개발 생산성은 더욱 향상되고 있습니다.

개발 방식은 변화했고, 보안 역시 변화가 필요합니다.

기존 애플리케이션 보안은 '시프트 레프트(Shift-Left)'를 통해 점검 시점을 앞당겨왔지만, 주로 코드 저장·빌드 시점에 점검이 이뤄졌습니다. 하지만 AI 기반 개발 환경에서는 코드 생성과 수정이 빠르게 반복되면서, 특정 시점의 점검만으로는 생성되는 코드를 충분히 검증하기 어려워졌습니다. AI가 생성한 코드를 효과적으로 검증하려면 보안 역시 AI 기반 개발 환경 전반에 통합되어야 합니다.

AI 기반 개발로 공격 표면도 확대되고 있습니다.

AI를 활용한 개발이 보편화되면서 코드 생산량이 급증하고 점검해야 할 보안 범위도 함께 확대되고 있습니다. 특히 LLM은 학습 데이터를 기반으로 코드를 생성하기 때문에, 검증되지 않은 패턴이나 보안 약점이 코드에 그대로 반영될 가능성이 있습니다. 또한 AI가 취약한 오픈소스 라이브러리나 검증되지 않은 구성요소를 제안할 경우, 소프트웨어 공급망 리스크가 커져 공격 표면을 넓힙니다.

AI 코딩 에이전트가 코드를 실시간으로 생성하는 환경에서는 전통적인
애플리케이션 보안 방식만으로 개발 속도와 보안성을 동시에 만족시키기 어렵습니다.

따라서 AI 코딩 에이전트와 보안 취약점 분석 도구를 MCP로 연동해,
코드가 생성되는 즉시 소스 코드 및 오픈소스를 분석 및 검증함으로써 코드의 안전성을 확보해야 합니다.

SPARROW

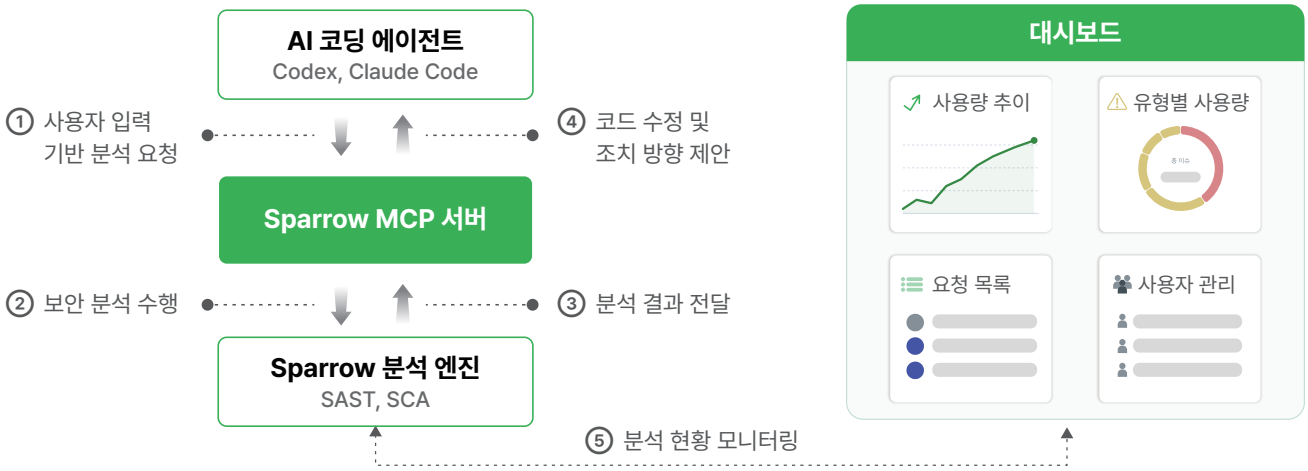
서울특별시 마포구 월드컵북로 396 (상암동 1605), 누리꿈스퀘어 비즈니스타워 13층 주식회사 스패로우

Tel 02-6263-7400 **Fax** 02-6263-7410 **E-mail** marketing@sparrow.im

www.sparrow.im

Sparrow MCP 란?

Sparrow MCP 는 AI 개발 환경에서 대화하듯 소스코드 보안약점 분석과 오픈소스 분석을 수행할 수 있는 AI 생성 코드 보안 어시스턴트입니다. AI 모델이 안전한 코드를 생성할 수 있도록 지원하며 대시보드를 통해 사용자별 분석 현황과 사용량 추이 등을 확인할 수 있습니다.



주요 기능

- 자연어 요청으로 AI 생성 코드 및 파일 분석
- 코드 생성과 동시에 보안 분석 자동 실행
- 분석 결과 기반 안전한 코드 생성 및 자동 수정
- 오픈소스 라이선스/취약점 정보 제공 및 SBOM 생성
- 실시간 분석 상태, 사용자별 요청 목록 등 대시보드 제공

기대 효과

개발 흐름 중단 없는 실시간 코드 검증

취약점 분석을 위한 도구 사용법 학습이나 화면 전환 없이 AI 개발 워크플로우 내에 보안을 내재화합니다. 코드 작성 시 보안 검증부터 결과 요약까지 실시간으로 수행하여 개발 흐름을 유지하면서 코드의 안전을 확보할 수 있습니다.

보안 검증 자동화로 개발 생산성 향상

AI 생성 코드에 대한 보안 검증을 자동화하고 안전한 코드를 파일에 바로 적용할 수 있어 개발자는 분석 결과를 확인하고 취약점을 조치하는데 소요되는 시간을 줄이고 핵심 개발 업무에 집중할 수 있습니다.

오픈소스 사용에 따른 리스크 사전 예방

분석 파일 또는 AI 생성 코드에서 사용된 오픈소스 소프트웨어를 식별하고 SBOM을 생성해 구성 요소를 가시화합니다. 라이선스 정보를 확인해 오픈소스 라이선스 정책을 준수하고, 취약점 정보를 실시간으로 확인해 안전한 컴포넌트를 사용할 수 있습니다.

자세한 상담이 필요하다면,

지금 바로 문의주세요!

E. marketing@sparrow.im

T. 02-6263-7400

스패로우 홈페이지