Sparrow MCP

AI 생성 코드 보안 어시스턴트

제품 화이트 페이퍼

주식회사 스패로우

SPARROW

CONTENTS

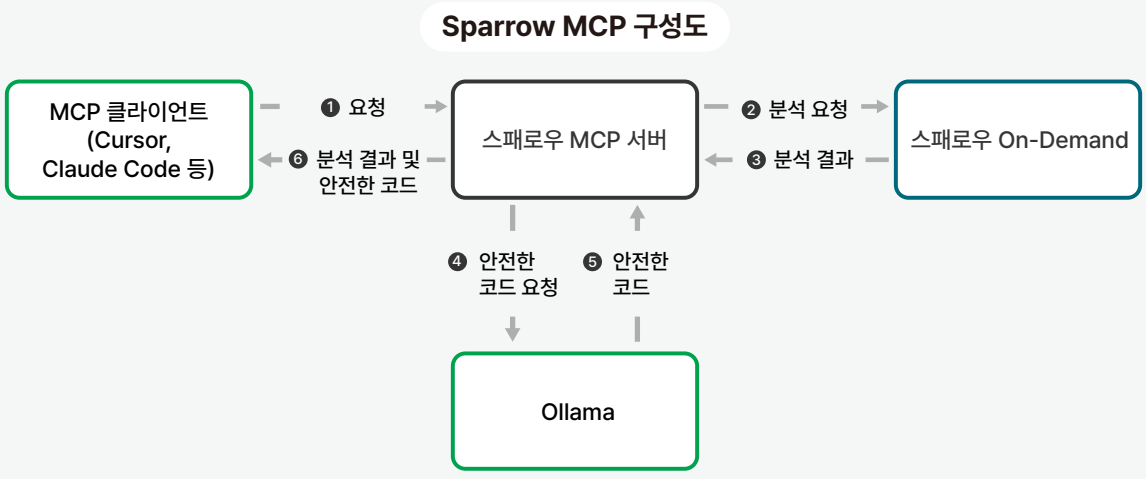
Sparrow MCP
AI 생성 코드 보안 어시스턴트
제품 화이트 페이퍼

Sparrow MCP는 스패로우의 소스 코드 분석 및 오픈소스 분석 제품인 Sparrow On-Demand의 분석 서비스를 AI 모델에 연결하고 IDE 플러그인을 통해 손쉽게 기능을 활용할 수 있는 제품입니다.

Sparrow MCP가 동작하기 위해서는 별도로 두 개의 서버가 필요합니다. 하나는 분석을 수행하는 Sparrow On-Demand 서버입니다. Sparrow On-Demand 서버의 분석 서비스는 MCP 클라이언트에서 MCP 서버를 거쳐 요청된 분석을 수행합니다. 해당 서비스는 일반적인 Sparrow On-Demand 서버와 동일하게 AWS에서 운영되며 소스 코드 분석, 오픈소스 분석, 웹취약점 분석을 수행합니다. 다른 하나는 분석 결과를 기반으로 새로운 코드를 생성하기 위해 사용되는 LLM(Large Language Model) 서버입니다. 여기에 사용되는 LLM 서버는 로컬 환경에 직접 설치하거나, 상용 클라우드 서비스로 제공되는 LLM 서비스를 사용할 수 있습니다. LLM 서버는 분석 서비스의 분석 결과를 수신하고 이를 바탕으로 안전한 코드를 생성하게 됩니다.

Sparrow MCP는 MCP 클라이언트를 통해 로컬 IDE를 MCP 서버에 연결합니다. MCP 클라이언트는 사용자가 로컬 IDE의 LLM 채팅 패널에서 명령을 입력할 때 Sparrow MCP를 명시함으로써 호출할 수 있습니다. MCP 서버는 Sparrow On-Demand에서 제공하는 NPM 기반의 MCP 서버이며 로컬 IDE와 LLM 서버, Sparrow On-Demand 서버 사이에서 요청을 전달하고 응답을 수신할 수 있습니다.

아래는 Ollama에 연결된 Sparrow MCP의 구성도입니다.



즉각적이고 체계적인 소스 코드 및 오픈소스 검증

코드 작성 후 즉각적인 검증

Sparrow MCP는 단일 파일 및 폴더 단위의 소스 코드 및 오픈소스 분석을 지원합니다. 특히, IDE와 직접 연동되기 때문에 개발자가 필요한 시점에 즉각적으로 보안 검증을 수행할 수 있습니다. 이를 통해 개발 초기 단계부터 보안 이슈를 사전에 식별함으로써 전체 개발 주기의 보안 품질을 효과적으로 향상시킬 수 있습니다. 또한 분석 결과를 프롬프트에 표시하는 데 그치지 않고 문제가 검출된 파일을 바로 수정하도록 지시한다면, 개발 중인 소스 코드에서 발견된 보안 약점을 효율적으로 제거할 수 있습니다.

컴플라이언스에 따른 체계적 검증

Sparrow On-Demand 분석 서비스의 소스 코드 분석 검출 규칙은 개발 언어와 컴플라이언스 요구사항에 따라 체계적으로 구성되어 있으므로 다양한 관점에서 종합적인 분석 결과를 제공하게 됩니다. 따라서 Sparrow On-Demand 분석 서비스를 거치지 않고 LLM 서비스에서 직접 소스 코드를 모니터링하여 보안 약점을 확인하는 것보다 더 정밀한 분석을 수행할 수 있습니다. 이러한 분석 결과의 신뢰성으로 인해 Sparrow MCP를 통한 소스 코드 분석은 개발 과정에서 보안 품질을 확보하는 효과적인 방법이 됩니다.

오픈소스 취약점 및 라이선스 문제 확인

Sparrow On-Demand 분석 서비스의 오픈소스 분석을 통해 오픈소스 소프트웨어 컴포넌트에 포함된 취약점이 있거나 오픈소스 라이선스 문제가 있는지 확인할 수 있습니다. 예를 들어, 개발자가 프로젝트에서 오픈소스 라이브러리를 사용하고 관련 의존성 파일이 파일 목록에 포함되어 있는 경우 해당 파일에 대한 오픈소스 분석을 요청함으로써 컴포넌트 취약점 및 라이선스 관련 문제를 확인할 수 있습니다.

적용 사례 및 방법

Sparrow MCP는 개발 IDE와 바로 연결할 수 있습니다. 따라서 개발 단계에서 작성된 코드 및 참고한 오픈소스 소프트웨어를 검사하기에 매우 편리합니다. 다음과 같이 설정하세요.

1. IDE 플러그인 등을 통해 IDE를 LLM에 연결
2. Sparrow MCP 패키지를 설치하고 MCP 설정 파일을 생성
3. Sparrow On-Demand 토큰을 발급받아 MCP 설정 파일에 입력

베스트 시나리오

소프트웨어 개발자가 IDE에서 개발을 진행하는 과정 중 IDE의 LLM 채팅 창에 다음과 같이 Sparrow MCP를 사용하여 개발 프로젝트를 분석하도록 프롬프트를 작성합니다. 사용자의 필요에 따라 다음과 같은 내용을 프롬프트에 추가할 수 있습니다.

1. 오탐 자동 분류 및 검토 우선순위 자동 판단

- 분석 결과에서 오탐에 해당하는 이슈를 판별해서 제외
- 우선적으로 대응해야 할 이슈 선별 후 차례대로 안전한 코드 제안

소스 코드 분석의 경우 잠재적으로 위험한 코드를 검출하는 특성으로 인해 오탐이 다수 발견됩니다. 위와 같은 사용자 규칙을 설정하여 MCP를 통해 분석을 수행하면 불필요한 내용을 제외하고 실제 대응이 필요한 결과를 확인할 수 있습니다. 또한, 너무 많은 이슈가 발견되는 경우 개발자가 먼저 확인해야 하는 이슈부터 순서대로 수정할 부분을 제시하도록 요청할 수 있습니다.

2. 특정 코드 변경마다 자동 분석 수행 및 특정 문구 표시

- 새로운 코드에 파일이나 DB 입출력 등 외부 데이터 관련 조작이 포함되는 경우 코드 자동 분석
- 결과를 설명할 때 특정 문구로 위험성을 표시

위와 같은 사용자 규칙을 설정하면 외부 데이터와 관련된 코드가 변경될 때마다 자동으로 코드를 분석하고 분석 결과를 어떻게 적용해야 하는지를 설명하도록 활용할 수 있습니다. 외부 데이터 관련 코드뿐만 아니라 중요한 검출 대상이 있는 경우 해당하는 항목을 사용자 규칙에 입력하여 특별한 주의를 기울일 수 있습니다.

3. 안전한 코드를 제안하고 파일에 바로 적용 및 재확인

- 코드를 분석한 후 안전한 코드를 파일에 바로 적용
- 코드 수정 후 재분석을 통해 코드 확인

위와 같은 사용자 규칙을 통해 분석을 수행할 때마다 안전한 코드를 자동으로 적용할 수 있습니다. 수정된 코드를 다시 분석함으로써 LLM으로 변경한 코드의 안전성이 확보되었는지를 재확인합니다. 덧붙여 코드 변경으로 인해 코드가 개발자의 의도와 다르게 변경될 가능성이 있는 부분을 따로 확인하도록 지시할 수 있습니다.

신뢰 가능한 AI 개발

AI 개발이 소프트웨어 개발의 중심이 되어가고 있는 시대에서 개발 산출물이 신뢰 가능한지를 확인할 방법이 필요합니다. Sparrow MCP는 AI 개발이라는 뉴 노멀에 요구되는 보안과 품질을 보장해주는 핵심적인 도구입니다. 특히, 다양한 소프트웨어 보안 컴플라이언스 및 가이드에 매핑되어 있는 소스 코드 검출 규칙 및 대규모의 데이터 웨어하우스에서 관리되는 오픈소스 소프트웨어의 취약점 및 라이선스 정보를 통해 정제된 분석 결과를 확인할 수 있다는 점에서 LLM을 단독으로 활용하여 얻을 수 있는 정보와 뚜렷한 차이가 있습니다.

앞으로 Sparrow MCP는 소스 코드 분석 및 컴포넌트 분석을 더욱 고도화하는 동시에 사용자의 개발 워크플로우를 지원할 수 있는 편의 기능을 추가할 예정입니다. 프로젝트의 코드가 특정 컴플라이언스 기준에 적합한지를 선택적으로 분석하거나 사용자가 수정한 이슈 패턴을 다음 코드 생성에 반영하는 등 AI를 통해 최적화된 개발 경험을 제공하려 합니다. 이를 통해 고객이 AI 개발 워크플로우에 완전한 보안 체계를 구축할 수 있도록 AI 개발 시장을 지원할 것입니다.