

snyk/agent-scan

CATEGORÍA · SEGURIDAD Y BUENAS PRÁCTICAS

Detecta agentes y servidores MCP en tu máquina y revisa más de 15 riesgos como inyección de prompts.

QUÉ VAS A ENCONTRAR

- 01 Qué es y qué resuelve
- 02 Para qué sirve
- 03 Dónde aplicarlo
- 04 Instalación en 3 rutas (con comandos)
- 05 El código en GitHub
- 06 Comprobación y errores frecuentes

FICHA DEL RECURSO

Qué es, para qué sirve y cómo se implementa

FUNCIÓN

Repositorio de código abierto (licencia en el repositorio). Detecta agentes y servidores MCP en tu máquina y revisa más de 15 riesgos como inyección de prompts.

PARA QUÉ SIRVE

Detecta agentes y servidores MCP en tu máquina y revisa más de 15 riesgos como inyección de prompts.

DÓNDE APLICARLO

Proyectos donde necesites esta capacidad instalada en tu equipo o dentro de Claude Code. Requiere tener instalado git y el entorno del lenguaje que usa el proyecto.

CÓMO IMPLEMENTARLO

- 1 Ruta rápida: pégale a Claude Code el enlace del repositorio con el prompt de la página siguiente — instala y comprueba solo.
- 2 Ruta manual: clona el repositorio y corre los comandos de instalación de tu lenguaje.
- 3 Revisa el README antes de instalar: requisitos, versión y licencia.
- 4 Pruébalo en un caso pequeño antes de usarlo en trabajo real.
- 5 Revisa qué permisos y llaves pide antes de conectarlo a tus cuentas.

EL RECURSO EN DETALLE

Qué resuelve y cómo funciona

Detecta agentes y servidores MCP en tu máquina y revisa más de 15 riesgos como inyección de prompts.

INSTALACIÓN

agent-scan

Detecta agentes y servidores MCP en tu máquina y revisa más de 15 riesgos como inyección de prompts.

EL CÓDIGO ESTÁ AQUÍ

<https://github.com/snyk/agent-scan>

Ruta 1 · La más simple. Abre Claude Code, pégale este mensaje y él hace el resto:

PÉGASELO A CLAUDE CODE

Instala esto por mi y explicame lo que haces:

<https://github.com/snyk/agent-scan>

Antes de correr nada, leete el README y dime:

1. que hace exactamente y para que sirve
2. que requisitos necesito instalados
3. que permisos o llaves va a pedir

Luego instalalo paso a paso, avisame de cada comando antes de ejecutarlo, y al final comprueba que quedo funcionando.

Ruta 2 · Manual, si prefieres controlar cada paso desde la terminal:

INSTALACIÓN MANUAL · TERMINAL

1. Clona el repositorio

```
git clone https://github.com/snyk/agent-scan.git
cd agent-scan
```

2. Sigue el apartado de instalacion del README

```
cat README.md
```

3. Regístralo como servidor MCP

Claude Desktop: Settings > Developer > Edit Config

y anade el bloque que indique el README bajo mcpServers

4. Reinicia Claude Desktop y revisa que aparezca el conector

Ruta 3 · Sin instalar nada. Entra al enlace de arriba y lee el README y los ejemplos para decidir si te sirve antes de bajarlo.

ANTES DE DARLO POR HECHO

Comprobación y errores frecuentes

- 1 No quedó instalado si no lo has probado: corre el ejemplo del README y comprueba que devuelve lo esperado.
- 2 Si un comando falla, casi siempre falta un requisito previo (versión de Node, Python o git). Pégale el error a Claude Code y pídele que lo resuelva.
- 3 Si pide una llave o token, créala en la cuenta correspondiente y guárdala fuera del código, en una variable de entorno.
- 4 Antes de conectarlo a cuentas reales, Pruébalo con datos de prueba o una cuenta secundaria.
- 5 Comprueba la licencia si lo vas a usar en trabajo de cliente: define qué puedes hacer con el código.

DATOS DEL RECURSO

Tipo: Repositorio open source

Categoría: Seguridad y buenas prácticas

Código: <https://github.com/snyk/agent-scan>

El ecosistema de IA cambia rápido: confirma en el repositorio que el proyecto sigue activo y que los comandos no han cambiado desde la fecha de esta ficha.

SIGUIENTE PASO

Instálalo hoy, en pequeño.

Elige la ruta 1, pégale el enlace a Claude Code y pruébalo en un caso real chico. Un recurso instalado y probado vale más que diez guardados para después.

MÁS GUÍAS GRATIS EN [377CREATIVE.COM/RECURSOS](https://377creative.com/recursos)