



MISP + AI

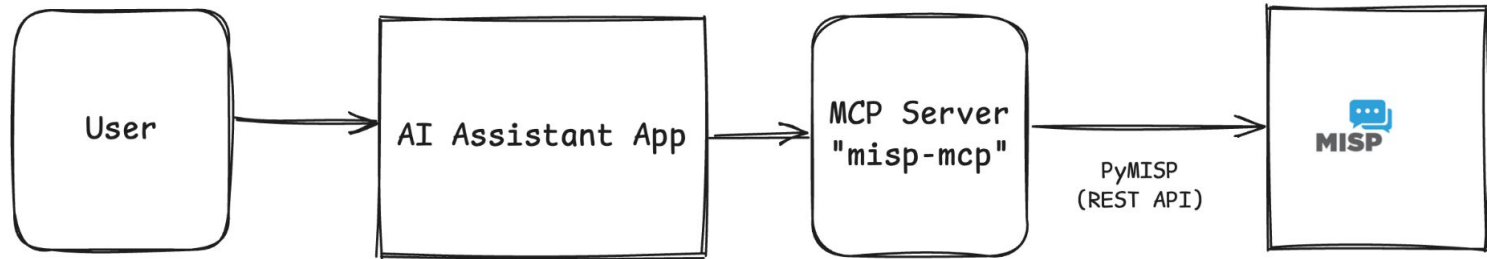
Marcelo de Souza
CISSP, GCTI, GCFA, GXPN

marcelo://about

- Pai da Ana Clara
- 25 anos em CyberSec
 - PenTest, DFIR, SOC, Consultoria, etc...
- Atualmente Team Lead
 - Criação de Ferramentas de Automação usando IA
- Hacker nas horas vagas
 - No bom sentido...



Diagrama Simplificado





Alguns Conceitos

AI / GenAI (Inteligência Artificial / IA Generativa)

- IA que "cria" alguma coisa (texto, imagem, vídeo, etc)

AI Assistant App

- App de conversação que usa GenAI, como **ChatGPT**, **Claude** e similares

LLM (Grande Modelo de Linguagem)

- "Motor" (ou parte do "cérebro") que está por trás do assistant app
- Alguns possuem capacidade de "pensar" ("reasoning models" ou "think mode") Ex.:
OpenAI o3, Anthropic Claude Sonnet 4, Grok 4

Function / Tool Calling (Chamada de Funções)

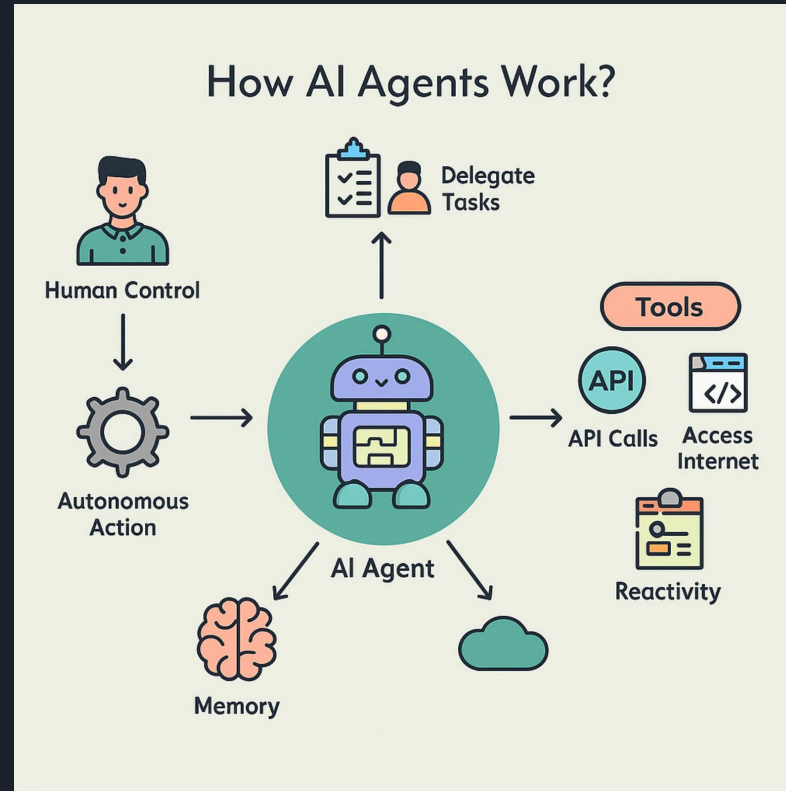
- Permite ao LLM executar ferramentas externas



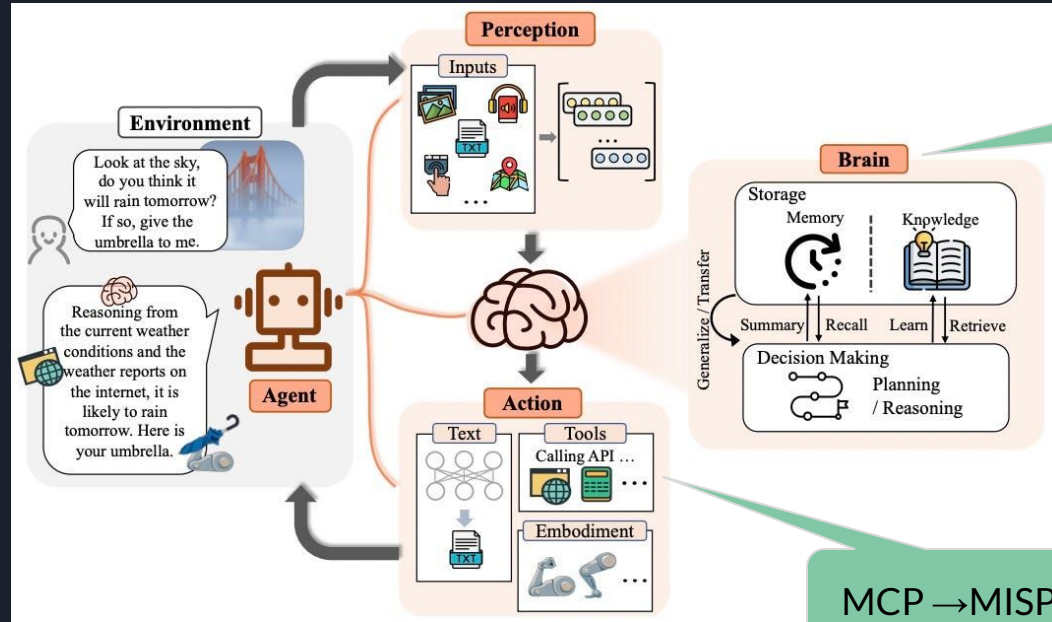
Demo 1

- Verificando se uma instância do MISP está funcionando

Agentes de IA (1 de 3)



Agentes de IA (2 de 3)

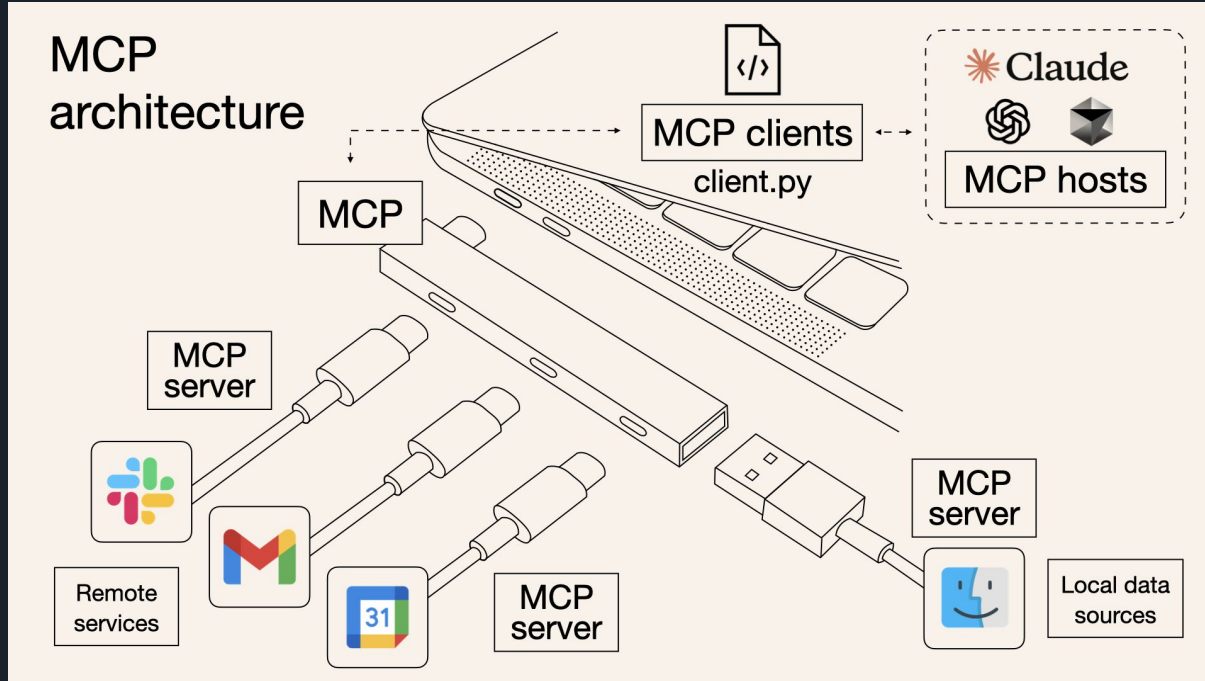


Agentes de IA (3 de 3)

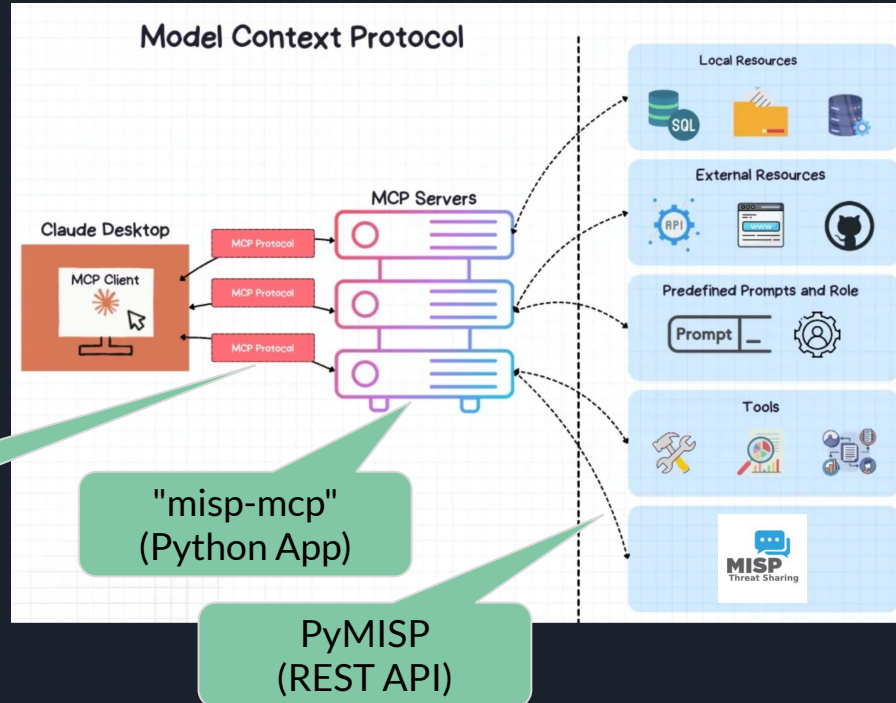
"J.A.R.V.I.S. do Iron Man"



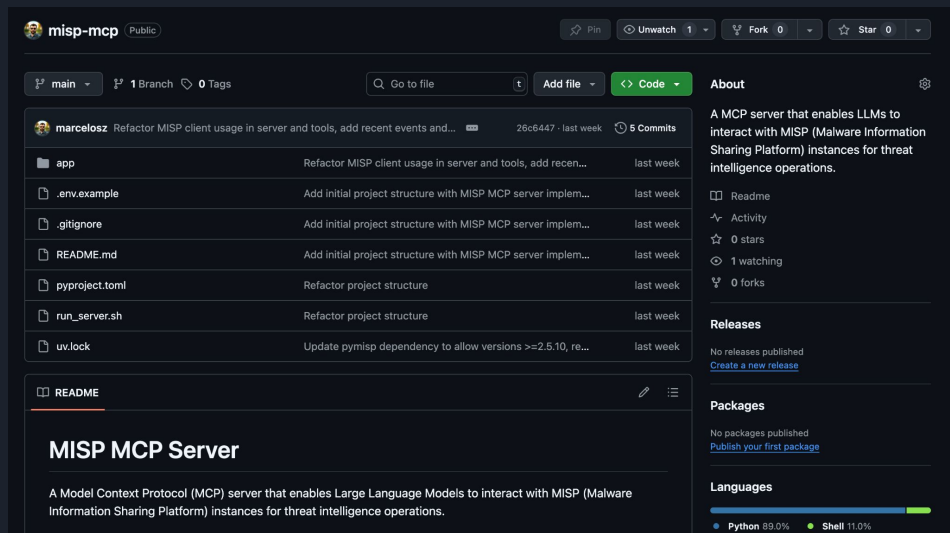
MCP - Model Context Protocol



Explicando as Integrações via MCP



"misp-mcp"



The screenshot shows the GitHub repository page for `marcelosz/misp-mcp`. The repository is public and has 1 branch, 0 tags, 0 forks, and 0 stars. The main branch is selected. The repository description is: "A MCP server that enables LLMs to interact with MISP (Malware Information Sharing Platform) instances for threat intelligence operations." The repository contains 5 commits and 10 files. The files listed are: `app`, `.env.example`, `.gitignore`, `README.md`, `pyproject.toml`, `run_server.sh`, `uv.lock`, `README`, `MISP MCP Server`, and `A Model Context Protocol (MCP) server that enables Large Language Models to interact with MISP (Malware Information Sharing Platform) instances for threat intelligence operations.`

File	Description	Last Commit
<code>app</code>	Refactor MISP client usage in server and tools, add recent events and...	last week
<code>.env.example</code>	Add initial project structure with MISP MCP server implem...	last week
<code>.gitignore</code>	Add initial project structure with MISP MCP server implem...	last week
<code>README.md</code>	Add initial project structure with MISP MCP server implem...	last week
<code>pyproject.toml</code>	Refactor project structure	last week
<code>run_server.sh</code>	Refactor project structure	last week
<code>uv.lock</code>	Update pymisp dependency to allow versions >=2.5.10, re...	last week

README

MISP MCP Server

A Model Context Protocol (MCP) server that enables Large Language Models to interact with MISP (Malware Information Sharing Platform) instances for threat intelligence operations.

About

A MCP server that enables LLMs to interact with MISP (Malware Information Sharing Platform) instances for threat intelligence operations.

Releases

No releases published
[Create a new release](#)

Packages

No packages published
[Publish your first package](#)

Languages

Python 89.0% Shell 11.0%

marcelosz/misp-mcp



A MCP server that enables LLMs to interact with MISP (Malware Information Sharing Platform) instances for threat intelligence operations.

<https://github.com/marcelosz/misp-mcp>



Demo 2

- Buscando por eventos recentes
- Obtendo detalhes de um evento específico
- Solicitando apoio para detecção de vulnerabilidade
- Solicitando apoio para Threat Hunting, Detection Engineering
- Pedindo a criação de relatório detalhado com base no evento



Demo 3

- Criando um evento com base em relatório PDF

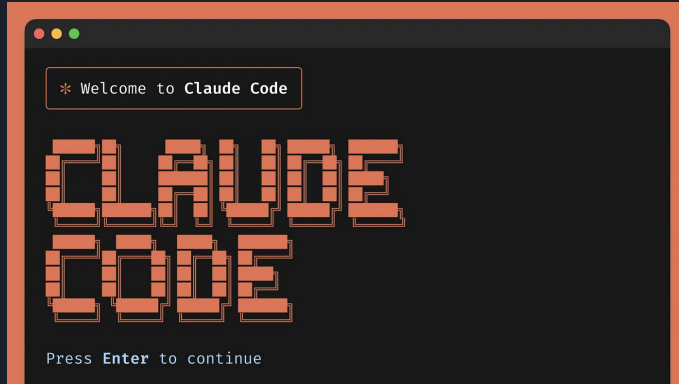


Demo 4

- Criando um evento com base em busca na web

Alternativas ao Claude Desktop

Opções compatíveis um MCP Client STUDIO atualmente



VS Code





Considerações Finais

Custos do software utilizado / AI

- **misp-mcp** → totalmente gratuito (open source)
- **Claude AI** → R\$100/mês (plano Pro, que permite integrações MCP)
- **Gemini CLI** → gratuito

Segurança/Privacidade envolvendo ferramentas (LLM) de terceiros

- **Anthropic** (do Claude), entre outros, possui planos Enterprise
 - Termos de privacidade mais rígidos
- Algumas ferramentas permitem o uso de:
 - LLMs acessíveis via CSPs como GCP (Vertex AI) e AWS (Bedrock)
 - LLMs locais (Importante → quanto maior/melhor o LLM, mais GPU será necessário)
- No fim do dia, teremos uma situação similar à "Cloud Migration"



Perguntas?

Siga-me no X, LinkedIn
e inscreva-se na minha newsletter

linktr.ee/marcelosz

Obrigado!

