

<<<<

AUTOMATIZANDO COLETAS DE CTI E POTENCIALIZANDO COM AI



QUEM SOU EU ?

- Pesquisador
- Especialista de Threat Intelligence;
- desenvolvedor;
- aspirante a inovação;
- Professor de IR e Threat Intelligence;
- nas horas vagas Jedi.



>>>>

O QUE ESTÁ ACONTECENDO, O QUE É MCP?



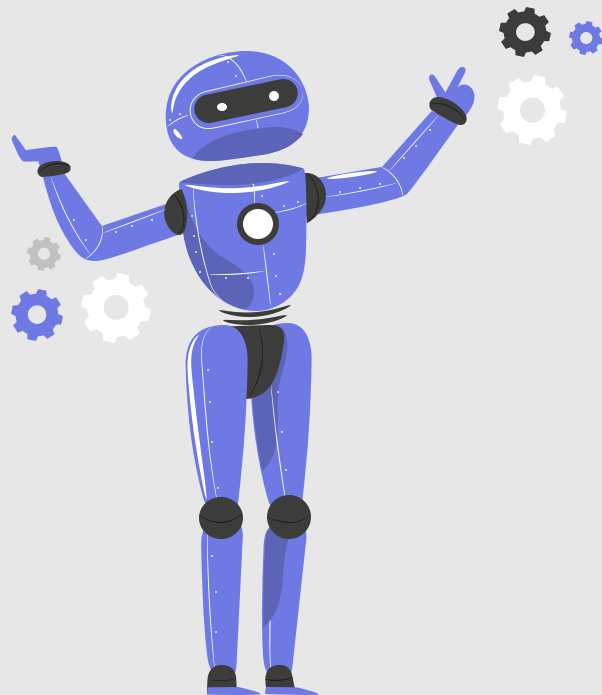
O QUE É MCP?



O Model Context Protocol (MCP) é um padrão criado pela Anthropic em 2024. Ele foi desenvolvido para melhorar a comunicação entre diferentes modelos de inteligência artificial, permitindo que eles compartilhem informações sobre o "contexto" em que estão operando.

O MCP define regras claras para como modelos podem trocar dados sobre tarefas, histórico de interações e configurações específicas. Isso ajuda a tornar as respostas mais precisas, personalizadas e consistentes, mesmo quando múltiplos modelos trabalham juntos.

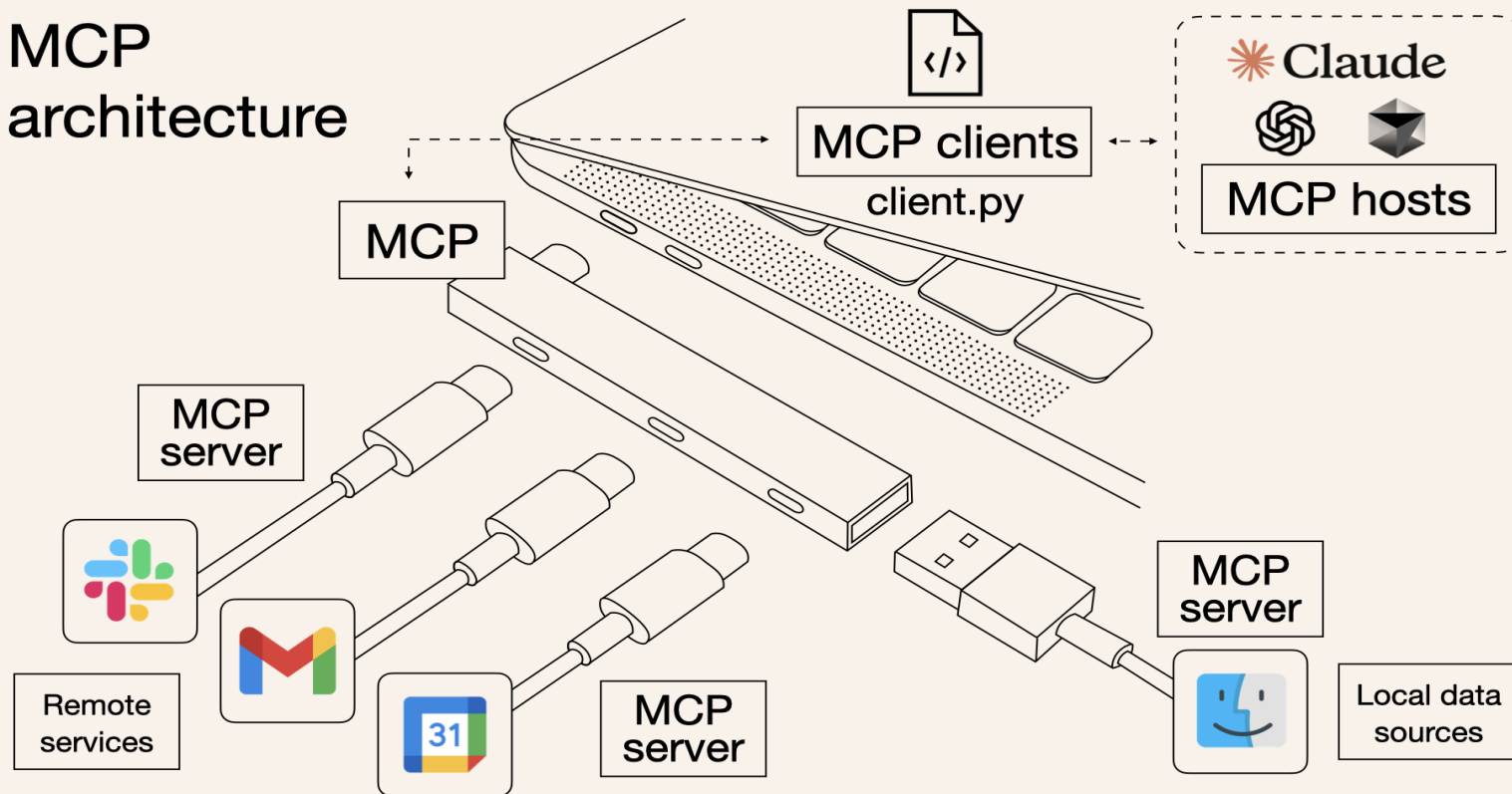
Em resumo, o MCP é uma forma de "fazer modelos conversarem entre si" de maneira organizada e eficiente.



AL
EN
AD

O QUE É MCP ?

MCP architecture



O QUE VAMOS USAR AQUI



PYTHON

Para facilitar as integrações e automações será usado Python



CURSOR

Para editar as automações e executar vamos usar o Cursor



GPT

Para executar as tarefas e interpretar os resultados vamos usar GPT

```
@mcp.tool(
    name="get_content_from_url",
    description=""" ...
)
async def get_content_from_url(url: str) -> TextContent:
    """ ...

    def fetch_content(url): ...

    response = fetch_content(url=url)
    if response and response.status_code in [200, 201, 202, 3
```

```
"threat_intelligence_mcp": {
  "command": "/Library/Frameworks/Python.framework/Versions/3.11/bin/python3",
  "args": [
    "--directory",
    "/Users/runner/.mcp/Developer/MCP/security",
    "run",
    "main.py"
  ],
  "env": {
    "MISP_URL": "https://localhost",
    "MISP_KEY": "gsp... ..",
    "URLSCANIO_API": "... ..",
    "VT_API_KEY": "1... ..",
    "ABUSEIPDB_API": "... .."
  }
}
```


Chat




Cursor Settings



@ Add context |

Plan, search, build anything

∞ Agent  gpt-4o



O QUE ESTÁ ACONTECENDO AQUI?



GPT

Procura a melhor
automação que
corresponde a minha
solicitação

OUTPUT

O resultado do script
é usado como
contexto



GPT

Solicito uma tarefa ao
GPT

SCRIPT PYTHON

O script selecionado
é executado

RESPOSTA

Uma resposta é
formada

>>>>

AL
EN
AD

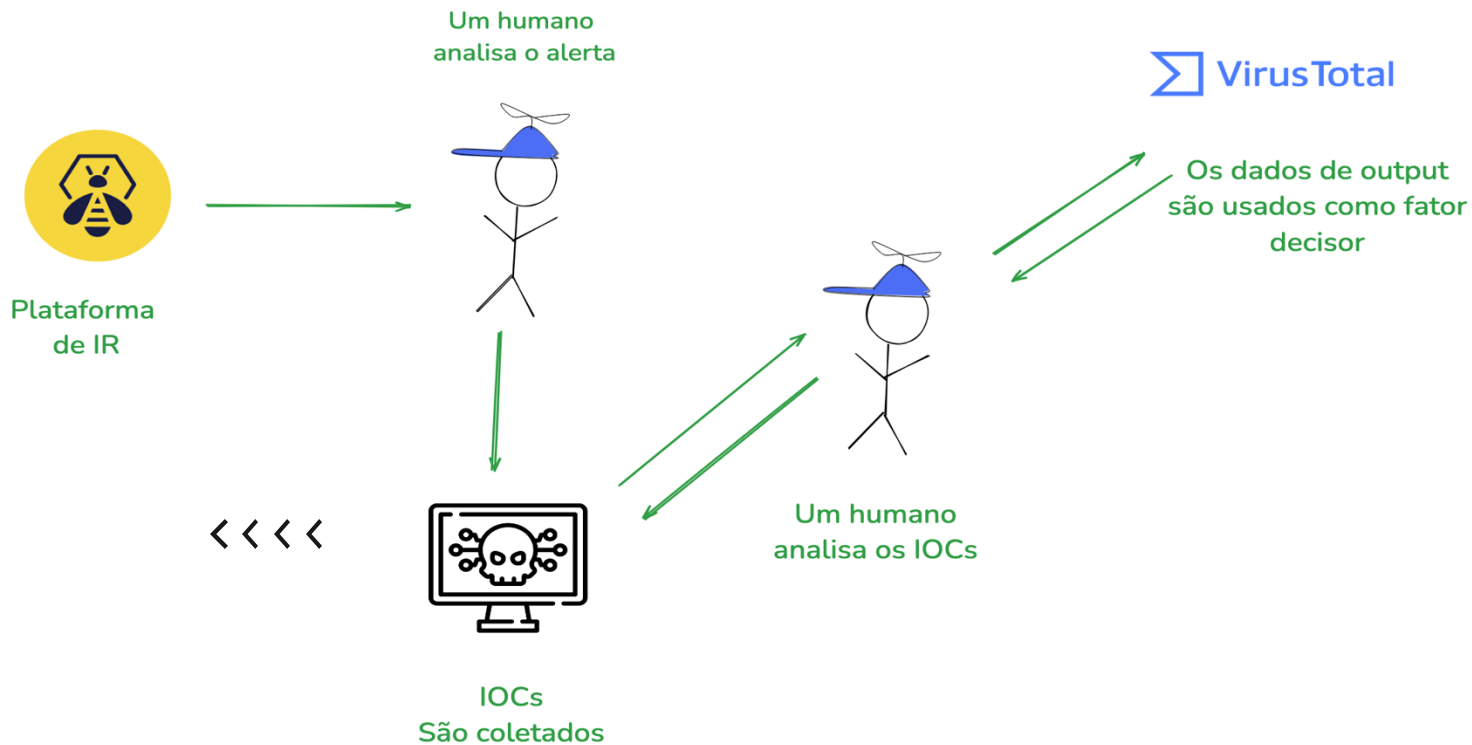


BLZ.

**E CADÊ O THREAT
INTELLIGENCE ?**



COMO FUNCIONA O TRADICIONAL



AGORA VAMOS PENSAR EM COMO USAR O MCP



PROCESSO

Criamos um contexto, e realizamos perguntas capazes de serem resolvidas

>>>>



AUTOMAÇÃO

Desenvolvemos automações de todos os dados complementares que precisamos para criar mais contexto

>>>>



RESULTADO

Melhora o processo de decisão e diminui o tempo de resposta

>>>>

```
def get_iocs_from_content(url: str) -> TextContent:
```

```
    """
```

```
    obtem os iocs do content da página web fornecida na pergunta pelo usuário.
```

```
    """
```

```
    cache['iocs'][url] = observables._iocs(raw=cache["content"][url])
```

```
    return TextContent(
```

```
        type="text",
```

```
        text=json.dumps(cache['iocs'][url], indent=2),
```

```
    )
```

Algumas Regex



usada para conectar-se a servidores VPS e realizar tarefas como interagir em sites de recrutamento de empregos e acessar serviços relacionados a criptomoedas. O artigo também menciona vídeos instrutivos que explicam como configurar servidores de comando e controle de malware Beavertail e como quebrar senhas de carteiras de criptomoedas. A Trend Vision One™ oferece proteção contra essas ameaças, centralizando a gestão de exposição a riscos cibernéticos e operações de segurança.

Para mais detalhes, você pode acessar o artigo completo [aqui](#).



@ Add context

Plan, search, build anything

∞ Agent ⓘ ^ gpt-4o ^





OK.

VAMOS MELHORAR

Vamos adicionar mais contexto para
melhorar nossa decisão




```
class Malicious:
```

```
    def virus_total(self, target: str, type: str) -> list:...
```

```
    def abuseipdb(self, iocs: dict) -> list:...
```

```
    def urlscanio(self, iocs: dict) -> list:...
```

```
    def hashes(self, iocs: dict, type: str ) -> list:...
```



- 80.237.84.255
- **CVE:**
 - CVE-2025-26633

Esses IOCs são associados a atividades cibercriminosas alinhadas com a Coreia do Norte, conforme discutido no artigo da Trend Micro.



@ Add context

Plan, search, build anything

∞ Agent  gpt-4o 



O QUE FAZER COM OS RESULTADOS ?



MISP

Você pode pedir para o chat criar um evento no MISP com os IOCs e contexto



EDR

Você pode bloquear esses IOCs no seu EDR favorito



SIEM

Você pode mandar os IOCs e dados para o seu SIEM favorito



SHOW.

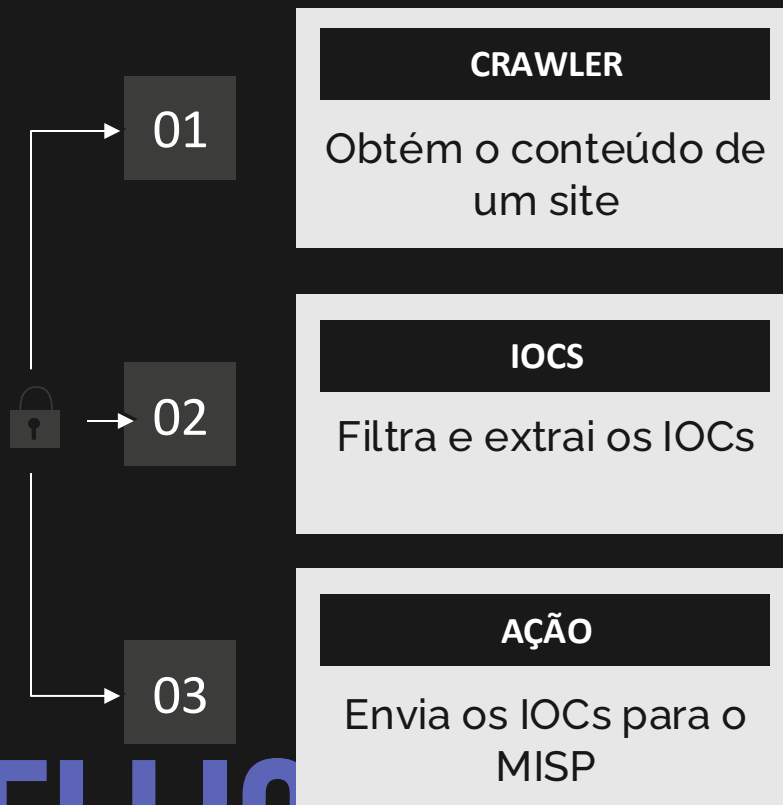
O QUE EU FAÇO AGORA?

Daqui em diante o céu é o limite



ENVIANDO IOCS PARA O MISP

Vamos classificar IOCs extraídos de um site e enviar eles para o MISP



ARTIFICIAL INTELLIGENCE (AI)

ARTIFICIAL

INTEL

[AI]

O QUE É MISP?



[AI]



Bloquear

- Prevenir
- Proteger a organização



Detectar

- Sistemas infectados
- Incidentes
- Descoberta de anomalias



Inteligência

- Quem usa sua empresa como target.
- Análise de comportamento

Coleta

Normaliza

Enriquece

Correlaciona

Analiza

Dissemina

Compartilha

```
@mcp.tool( ...
async def create_misp_event(chat_history: list, url: str) -> TextContent:
    """
    Antes de executar essa tarefa, você precisa me dizer quais são os IOCs maliciosos
    porque são esses IOCs que vão ser enviados para o MISP, por tanto faça um resumo

    Usa a última resposta do chat para extrair informações úteis, como IOCs.
    """
    iocs = None
    if not chat_history: ...

    if cache['matchs'].get(url, None) is None: ...

    try: ...
    except Exception as e: ...
```


@ Add context |

Plan, search, build anything

∞ Agent %I ▾ gpt-4o



ART
INT
[AI]

REGEX

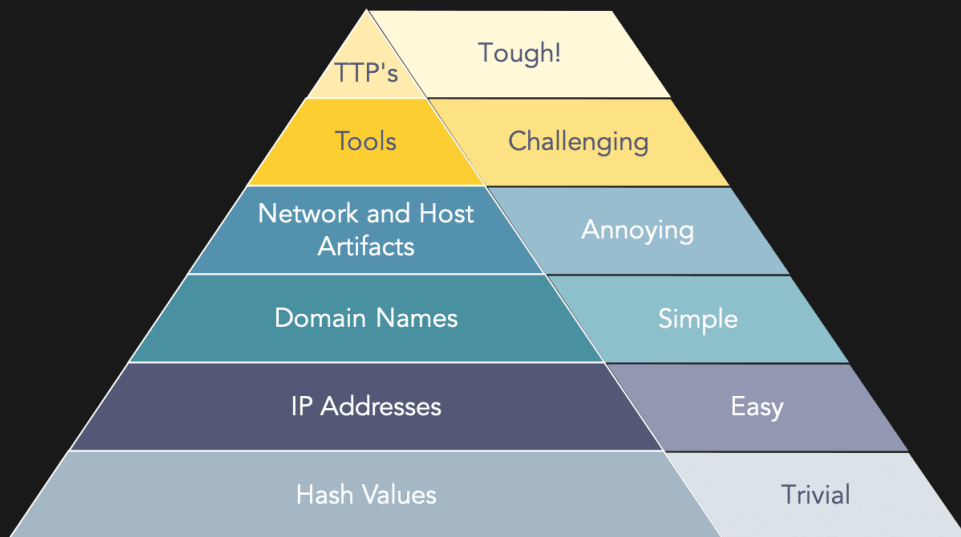
Extraia mais dados de
um noticia ou relatório

CONTEXTO

Crie mais contexto
para o chat e seu
destino final



EXPLORANDO O MÁXIMO DE DADOS



01

TTPs

Extraia e classifique as TTPs

02

Tools

Extraia e tenha contexto de ferramentas

03

Threat Actors

Explore o mais contexto de Threat Actors

ARTIFICIAL INTELLIGENCE (AI)

class Galaxys:

url_threat_actor: str = <https://raw.githubusercontent.com/MISP/misp-galaxy/refs/heads/main>

url_https: str = <https://raw.githubusercontent.com/MISP/misp-galaxy/refs/heads/main>

url_malware: str = <https://raw.githubusercontent.com/MISP/misp-galaxy/refs/heads/main>

url_tool: str = <https://raw.githubusercontent.com/MISP/misp-galaxy/refs/heads/main>

def yara_single(self, raw: str, yadir: str = None, yararaw: str = None) -> dict: ...

def create_rule(self, name: str, items: list) -> str: ...

def matches(self, content: str) -> dict: ...

- Undetected: 33

- Harmless: 61

20. 188.43.136.255

- Malicious: 0

- Suspicious: 0

- Undetected: 35

- Harmless: 59

Esses IOCs foram analisados em termos de sua detecção como maliciosos, suspeitos, não detectados ou inofensivos.



@ Add context

Plan, search, build anything

∞ Agent 88I ~ gpt-4o ~





ORKL.

OUTRO EXEMPLO DE CTI

Mais uma maneira de você usar dados de
inteligência



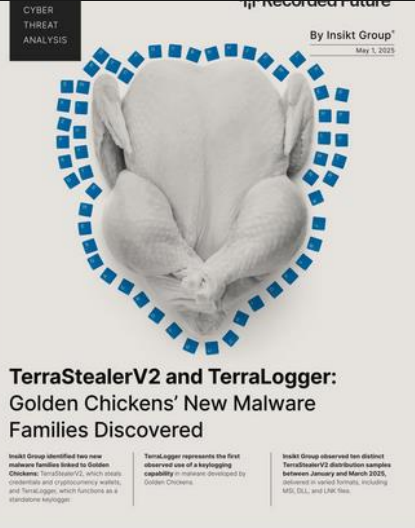
- ☐ APNotes 683
- ☐ ETDA 409
- ☐ MITRE 405
- ☐ OTX 251
- ☐ MISPGALAXY 192
- ☐ AGRO 122
- ☐ ORKL 104

Languages

- ☐ EN 12870
- ☐ ZH 132
- ☐ DE 70
- ☐ JA 54
- ☐ KO 52
- ☐ FR 38
- ☐ ES 28
- ☐ RU 27
- ☐ NONE 25
- ☐ NL 20

Clear refinements

Most Recent (PDF)



TerraStealerV2 and TerraLogger: Golden Chickens' New Malware Families Discovered

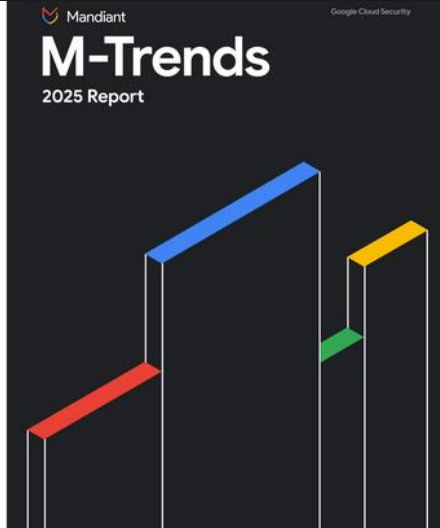
Insikt Group identified two new malware families linked to Golden Chickens: TerraStealerV2, which steals credentials and cryptographic wallets, and TerraLogger, which functions as a standalone logger.

TerraLogger represents the first observed use of a keylogging capability in malware developed by Golden Chickens.

Insikt Group observed two distinct TerraStealerV2 distribution samples between January and March 2025, delivered in varied formats, including MSF, DLL, and LNK files.

TerraStealerV2 and TerraLogger: Golden Chickens' New Malware Families Discovered

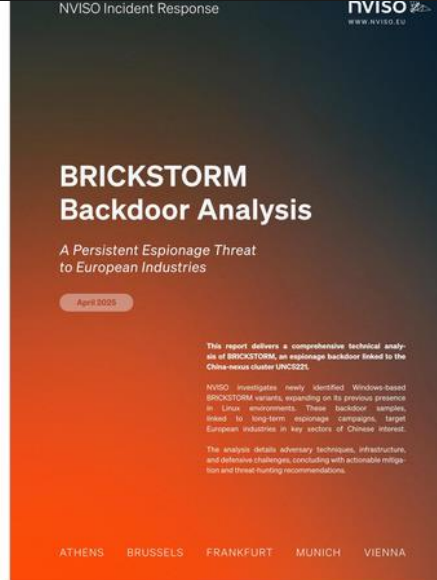
----- CYBER THREAT ANALYSIS ##
 Executive Summary Insikt Group identified two new malware families — TerraStealerV2 and TerraLogger — linked to the financially motivated threat actor Golden Chickens (also...



m-trends-2025-en.pdf

----- **Mandiant M-Trends 2025 Report**
 2 **Table of Contents** **4**
 Introduction **5** **By the Numbers** 7 Campaigns and Global Events 9 Targeted Attacks 26 Ransomware...

Malpedia



NVISO-BRICKSTORM-Report.pdf

NVISO Incident Response #
 BRICKSTORM Backdoor Analysis ### *A
 Persistent Espionage Threat * to
 European Industries* April 2025 W W
 N V I S O . E U...

ETDA

UTILIZANDO RELATÓRIOS

MISPGALAXY:Cobalt

..too many TAs to show

MISPGALAXY:RansomHub

..too many TAs to show

..too many TAs to show

by Unknown Author created 2025-04-09 (1

```
@mcp.tool(  
    name="fetch_latest_threat_reports",  
    description="" ...  
)  
async def fetch_latest_threat_reports() -> TextContent:  
    async with httpx.AsyncClient() as client: ...
```

/CAID





Free plan · [Upgrade](#)

 Welcome, Andrey

How can I help you today?



Claude 3.7 Sonnet ▾



```
@mcp.tool(  
    name="fetch_threat_report_details",  
    description="""...  
)  
async def fetch_threat_report_details(report_id: str) ->  
    async with httpx.AsyncClient() as client: ...
```



- Colaboração entre especialistas da Mandiant/FireEye e Microsoft
- PowerShell continua sendo um vetor de ataque prevalente para entrega e execução de malware

Este resumo destaca as principais tendências e ameaças recentes que merecem atenção especial em sua análise de ameaças, incluindo novos malwares, atividade de APTs, ransomware, e técnicas específicas como ofuscação de PowerShell e ataques a infraestrutura crítica.



Retry ▾

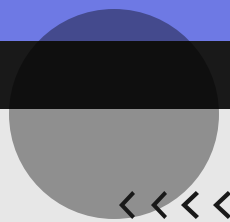
Claude can make mistakes. Please double-check responses.

Reply to Claude...



Claude 3.7 Sonnet ▾





OSINT.

EXPLORANDO MAIS O MCP





Busca de Inteligência em Fontes Abertas

○ Auto

▼

Digite email, telefone, username, CPF, CNPJ etc

Q

Ao realizar uma busca, você concorda com nossos [Termos de Serviço](#) e [Política de Privacidade](#)



AUTOMATIZANDO COLETAS DE OSINT

Resultados

anderson@gmail.com

Resumo

Tabela

Grade

Grafo


Timeline

Mapa

Resumo gerado por IA

The data provides a comprehensive list of usernames, names, emails, phones, and locations associated with Anderson. The information is sourced from various platforms, including DeHashed, Google Dorks, and other online sources. The data contains 1,000+ entries of information, including names, emails, and phone numbers. The information is structured in a way that provides a detailed overview of Anderson's online presence. The data includes information about Anderson's online activities, such as their email addresses, phone numbers, and locations. The information is publicly available and can be used for various purposes, including cybersecurity and data analysis. The data provides a detailed overview of Anderson's online presence and can be used to understand their behavior, interests, and activities. The data is a collection of information that can be used to identify patterns and relationships between different data points. The data provides a comprehensive overview of Anderson's online presence and can be used for various purposes, including cybersecurity and data analysis. The data is a collection of information that can be used to understand Anderson's online behavior and activities. The information is sourced from various online platforms, including DeHashed, Google Dorks, and other online sources. The data provides a detailed overview of Anderson's

Imagens 44



Nomes 61

...

Adam Anderson

Anderson

Anderson Anderson Scantlebury

Nomes de Usuário 38

19248 anderson@gmail.com

21cecilio anderson@gmail.com

569108224

65186913

af1283f45eae186af4328250

Endereços de Email 5

a*****@g*****.com

anderson@gmail.com

anderson@gmail.com, silvanaoliveira.so67@gmail.com

ramanderson@gmail.com, anderson@gmail.com

sorilota756@gmail.com, anderson@gmail.com

Telefones 34

(21)*****-7442

2035308055, 35308055

2087130140

2398485642, 12398485642

2566823238

Endereços IP 4

104.28....

14.229....

206.62....

45.178....

ORIGEM

Unifique a origem de dados

CONTEXTO

Utilize os resultados para trazer mais contexto



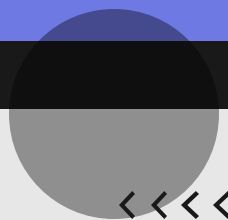
```
@mcp.tool(  
    name="search_email",  
    description=""" ...  
)  
def search_email(email: str) -> TextContent:  
    searchId = None  
  
    response = requests.post(...  
  
    if response.status_code in [200, 201]: ...  
  
    return TextContent(  
        type="text",  
        text=json.dumps(cache["content"][email], indent=2),  
    )
```


@ Add context |

Plan, search, build anything

∞ Agent ⓘ ▾ gpt-4.1





MAIS.

USANDO USERNAME

Vamos utilizar os usuários de output para
obter mais sobre o E-mail



```
@mcp.tool( ...
def get_more_info(email: str = None, username: str = None) -> TextContent:
    data = None
    uuids = []

    if cache["content"].get(email, None) is not None: ...
    elif cache["content"].get(username, None) is not None: ...

    if data is not None: ...

    return TextContent(
        type="text",
        text=json.dumps(cache["usernames"][data], indent=2),
    )
```

Chat



Cursor Settings



Se desejar detalhes sobre algum vazamento específico, análise de senhas expostas ou investigação de perfis públicos, por favor, especifique!



@ Add context

Ba

∞ Agent ⅈI ^

Auto ^





PERGUNTAS?