

# Compartilhamento de ameaças

## Primeiros passos



**Establish goals and objectives**

1



**Identify internal sources of threat information**

2



**Define Scope of information sharing activities**

3



**Establish sharing rules**

4



**Join a sharing community**

5



**Plan to support provide ongoing for information sharing activities**

6

adaptado de NIST 800.150

# Compartilhamento de ameaças

Fornecimento de dados à Detecção (SOC)

01

## Importação de dados

- hashes
- domínios
- IPs

02

## Classificação de fontes

- Estabelecimento de fluxos de compartilhamento e proteção de dados sensíveis

03

## Enriquecimento em Plataforma TIP

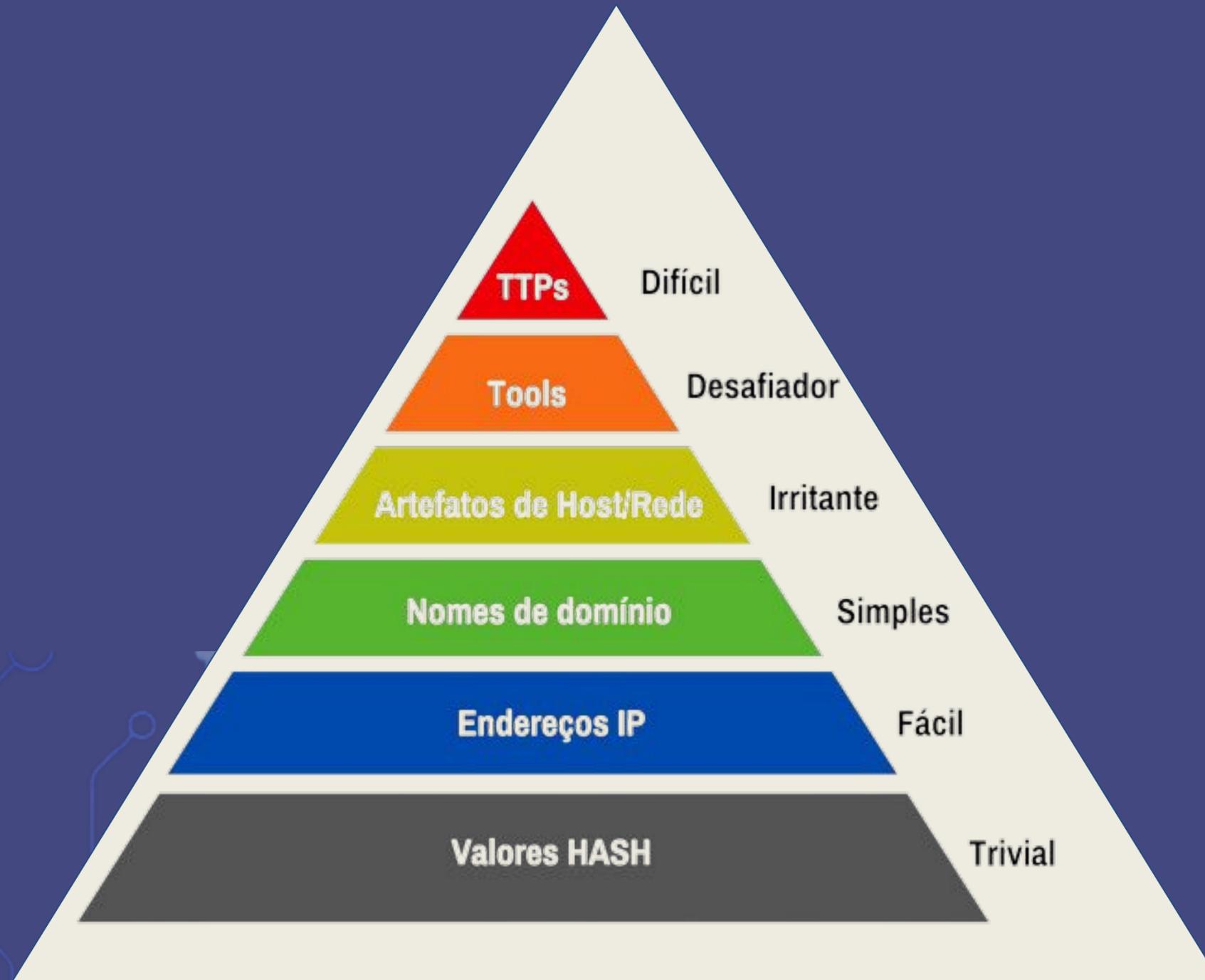
- OpenCTI

04

## Uso dos dados

- Criação de Collection de hashes, IP e domínios selecionados
- Correlacionamento no SIEM

# Threat Intel Pyramid of Pain



Como extrair entendimento de cenário a partir dos dados recebidos no MISP?

# Metodologia Proposta



**Extração de metadados**



**Análise de Strings**

- Data Analytics & GenAI
- Contexto
- Idioma
- Setor
- Empresas

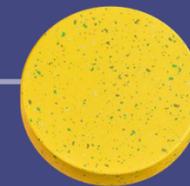


**Análise de Comportamento**

- TTPs



**Inclusão de IoC em monitoramento**



**Compartilhamento das informações**

# Hunting

## IOCs

Enriquecimento e hunting

## TTPs

Engenharia de detecção e hunting

**DOMAIN ...** ocsp.comodoca.com May 17, 2023

Author: **OPENCTI.BR**

Platform creation date: May 17, 2023 at 1:04:28 AM

Labels +

- botnet
- download
- malicious domain
- sandbox, malware
- virus

Modification date: May 1, 2024 at 12:17:28 PM

Standard STIX ID [i](#)

domain-name--2422db6c-224f-57a2-86d1--

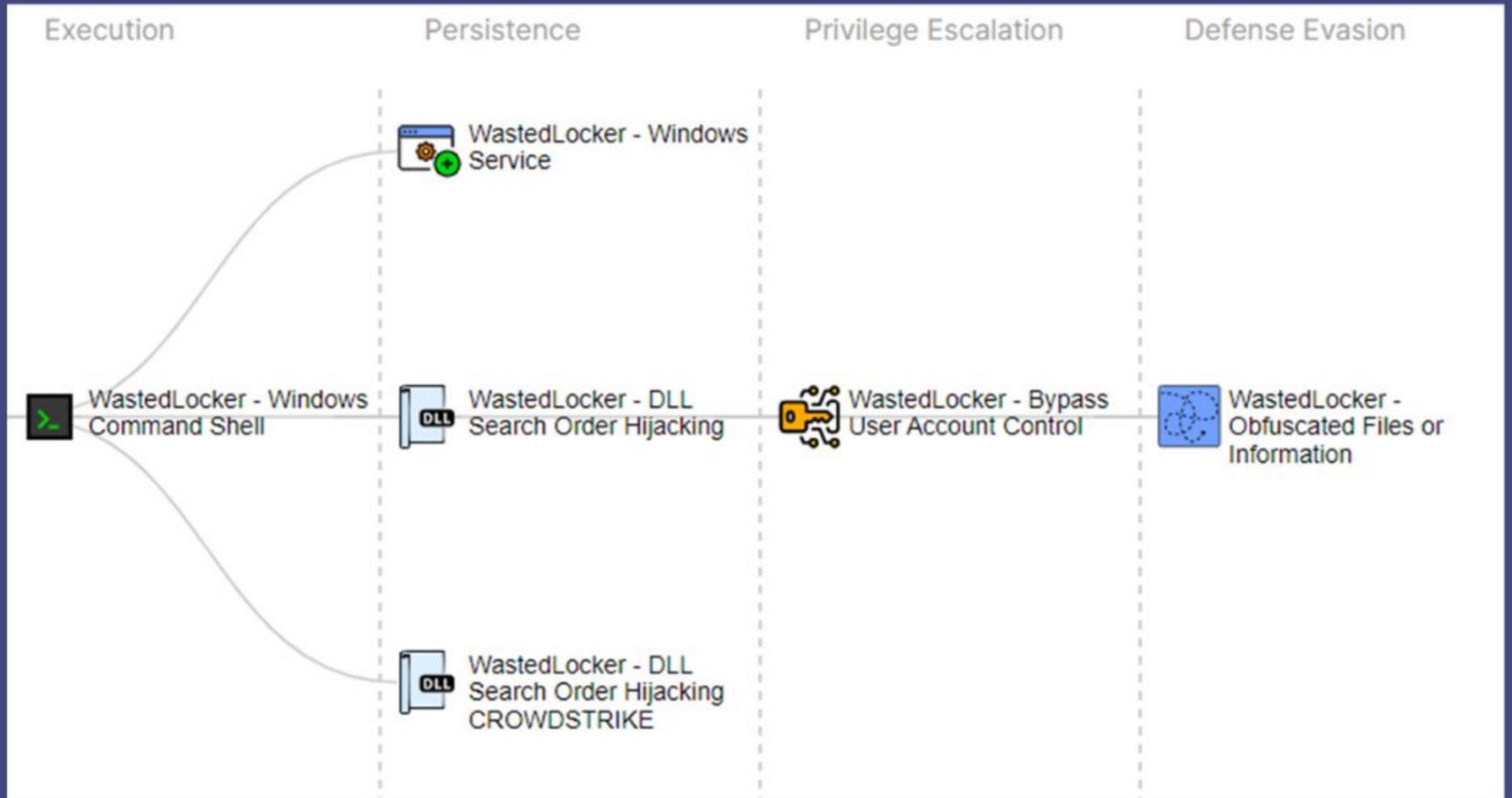
```
for aux_pw in df_raw["ParentImage"]:
    if aux_pw:
        if 'powershell.exe' in aux_pw.lower() or 'cmd.exe' in aux_pw.lower():
            power_list.append(1)
        else:
            power_list.append(0)
    else:
        power_list.append(0)
```

```
1 df_raw["CommandLine"][df_raw['OriginalFileName'] == "schtasks.exe"]
```

# Emulação de Adversários

## TTPs

Emulação de pontos de estrangulamento na cadeia de TTPs.



# CASE 2

## GenAI Insight

```
4b8d7e016ac84d73d574  
7cc84847f4cc0583b185fe  
636e3ccd3e1f713650425d  
.  
.exe
```



Recebimento do  
Hash via MISP



Análise de  
Strings com  
inputs da  
Gen AI

### GenAI Output

:

There is no specific mention to brazilian banks, payment system or specific portuguese terms in the string.

But the path

"C:\Users\Musquitao\Desktop\BR\_2023\ExemplosCoder\TesteAntiDebug\TesteAntiDebug\x64\Debug\TesteAntiDebu.pdb"

"

strongly suggest a Brazilian Portuguese environment due to:

- "Musquitao" is a portuguese word.
- "BR\_2023" refers to Brazil and the year 2023.
- "ExemplosCoder" translate to "Coder Examples" in Portuguese.
- "TesteAntiDebug" translate to "AntiDebug Test" in Portuguese.

[...]

**\*\* The PDB path strongly suggests \*\*Brazil\*\* as the development or testing environment.**

# Resultados

## Ampliação da capacidade de Inteligência

- capacidade de identificação de grupo ou ator com alvo direcionado
- Capacidade de compreensão rápida das táticas e técnicas do adversário com ataque direcionado



# Resultados

Continuação

- Ampliação da capacidade de hunting
- Fornecimento de informação mais assertivas para as equipes de detecção e anti-fraudes.
- Fornecimento de inteligência para decisão sobre testes de emulação



# Intenções futuras

Validação de processo  
de hunting baseado  
nos “insights”  
fornecidos pela  
metodologia e  
automação

Machine Learning  
para classificação de  
famílias de malware.

# Contato



**Jaqueline Duarte**

Analista de Threat hunting & Intel

**BANCO DO BRASIL**

<https://www.linkedin.com/in/jaqueline-d>



**Pedro Chagas Junior**

Analista de Threat hunting & Intel

**BANCO DO BRASIL**

<https://www.linkedin.com/in/pedro-chagas-jr>