MISP - Threat Intelligence em Ação

Automatizando Bloqueios com MISP, Python e AWS

Guilherme Bidin e Andrey Souza
IMCNET Cibersegurança

30 de Julho de 2025

TLP:CLEAR

Contexto operacional

- **SOC as a Service**

Monitoramento e resposta a incidentes feito por uma equipe externa especializada, disponível 24/7

- **SIEM SaaS Multi Tenant**

Plataforma de análise de logs em nuvem, compartilhada entre múltiplos clientes com isolamento seguro

- **Modelo de SOC Hibrido**

Combina equipes internas e serviços terceirizados para monitoramento e resposta a ameaças

- **Foco em mercado SMB**

Serviços e soluções adaptados às necessidades e ao orçamento de pequenas e médias empresas

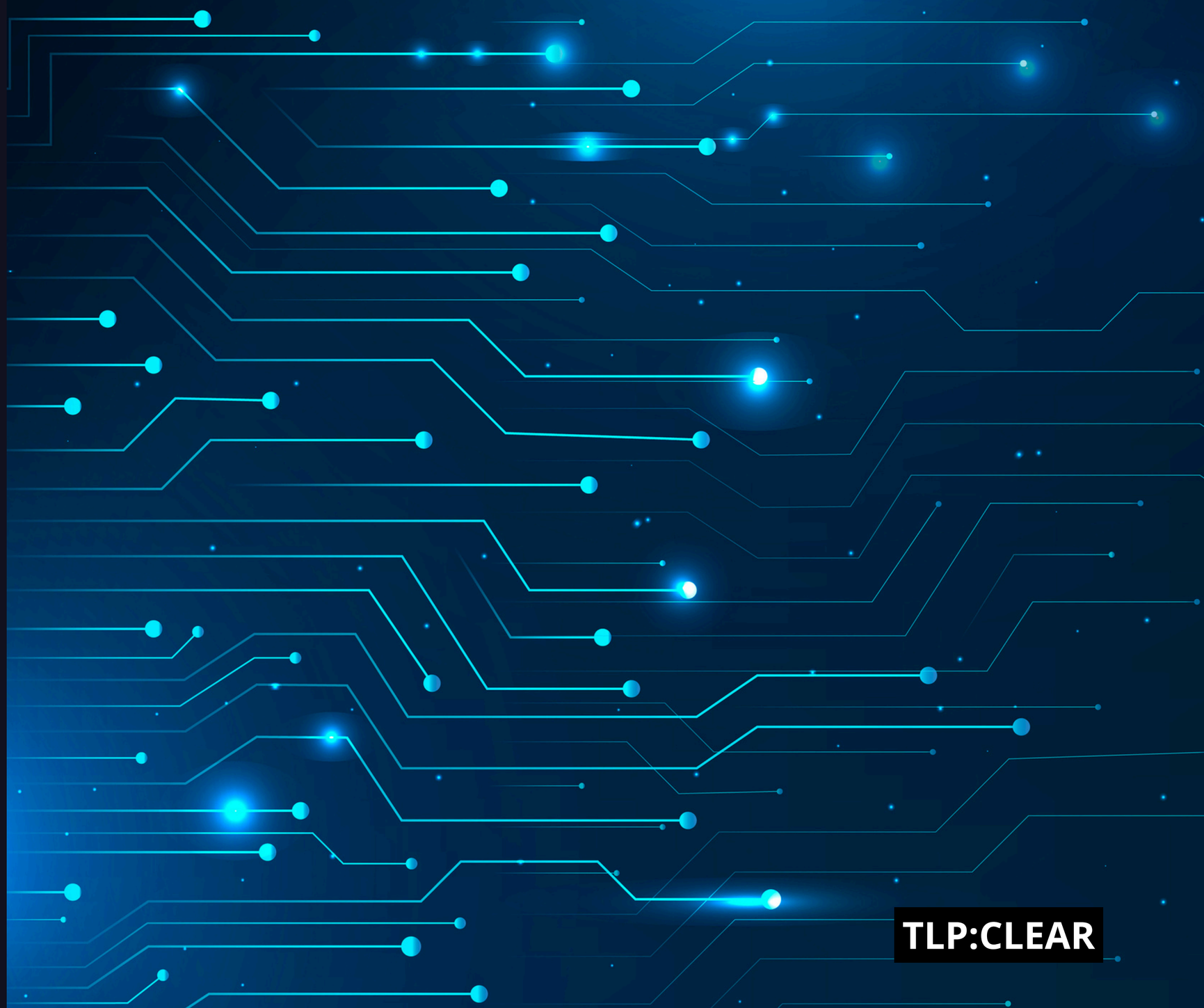
TLP:CLEAR

Desafios enfrentados

TLP:CLEAR

IOC “perdido” no ITSM

Impossibilidade de consultas, geração de relatórios ou automações



IOC “perdido” no ITSM

Centralização e visibilidade

TLP:CLEAR

IOC “perdido” no ITSM

Impossibilidade de consultas, geração de relatórios ou automações

Falta de integração

Coleta e centralização dos dados não tornava o ambiente “prático” mais inteligente

TLP:CLEAR

Falta de integração
Tesouro perdido

Ambiente X sofria um ataque

↓

Tratativa SOC

↓

Dado registrado no MISP

↓

FIM

TLP:CLEAR

IOC “perdido” no ITSM

Impossibilidade de consultas, geração de relatórios ou automações

Falta de integração

Coleta e centralização dos dados não tornava o ambiente “prático” mais inteligente

Volume elevado de acionamento para MSSP

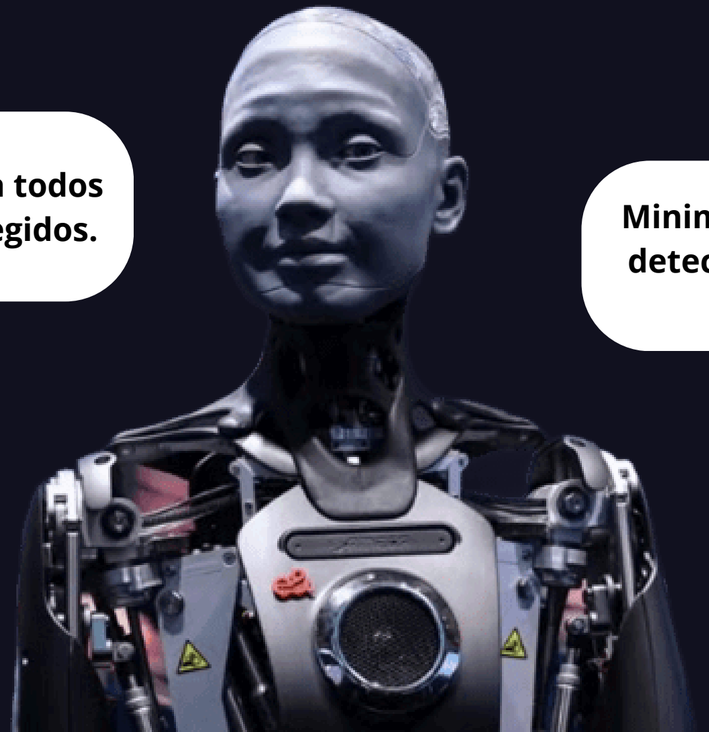
Tarefas simples com um consumo elevado de tempo

TLP:CLEAR

Objetivos da automação

Automação

Bloquear IPs maliciosos automaticamente via blocklist.



Distribuir IOCs para todos os ambientes protegidos.

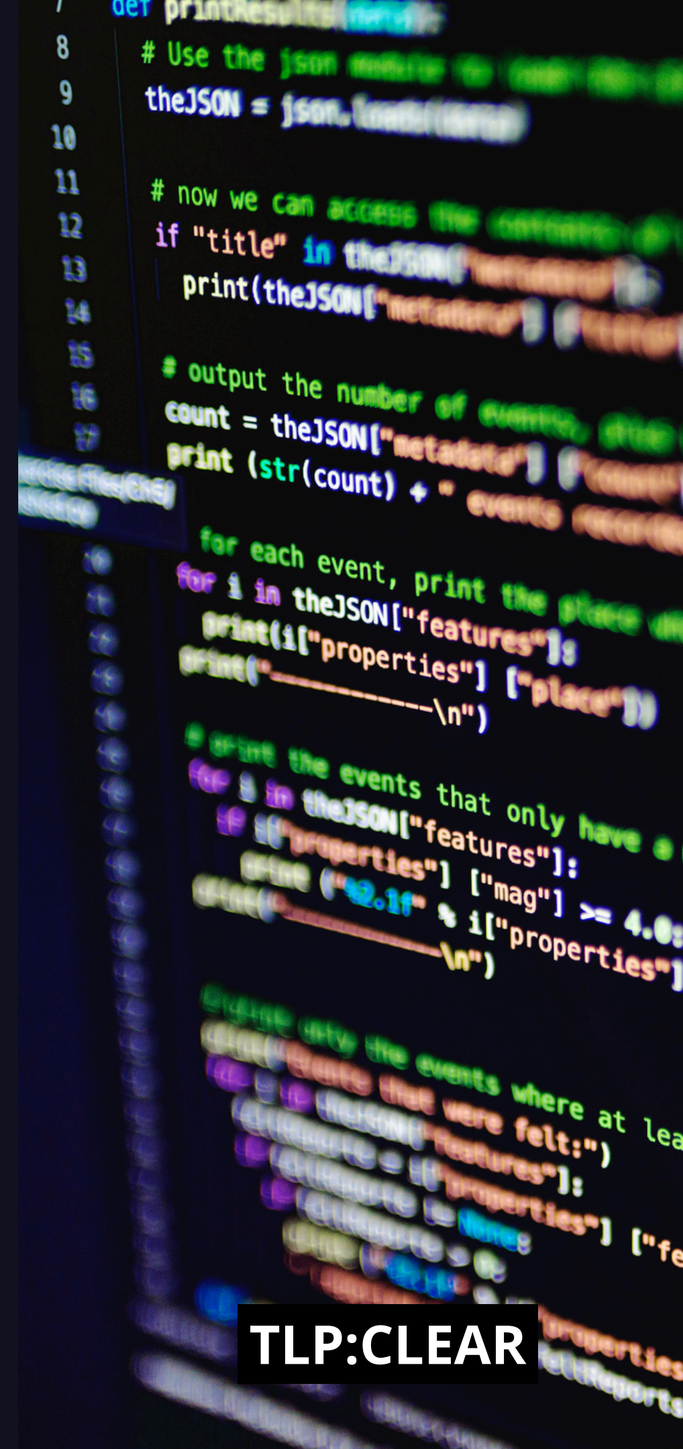
Minimizar o tempo entre detecção e mitigação de ameaças

TLP:CLEAR

Antes do MISP + AWS v1

	Origem	Referencia	Registrado no threat intel	IP MALICIOSO
0.149	Rússia	#371754		CONFIRMADO
7.18	China	#372129		CONFIRMADO
.80	Rússia	#373042		CONFIRMADO
29.27	China	#373110		CONFIRMADO
30.119	China	#373085		CONFIRMADO
.143	China	#373345		CONFIRMADO
9.5	Alemanha	#373445		CONFIRMADO
8.155	Singapura	#373561		CONFIRMADO
.66	China	#373778		CONFIRMADO
14.54	Russia	#373785		CONFIRMADO
.50	China	#373841		CONFIRMADO
.210	China	#373855		CONFIRMADO
87.100	China	#373881		CONFIRMADO
0.58	China	#373933		CONFIRMADO
.220	França	#373957		CONFIRMADO
27.133	Corea	#373957		CONFIRMADO
4.186	China	#373987		CONFIRMADO
6	netherlands	#374260		CONFIRMADO
6.107	China	#374345		CONFIRMADO
3.3	India	#374338		CONFIRMADO
5.163	Argentina	#374482		CONFIRMADO
7.57	China	#374491		CONFIRMADO
8.25	Brasil	#374498		CONFIRMADO
0.32	Holanda	#374549		CONFIRMADO
7.85	China	#411900		CONFIRMADO
87.165	China	#375018		CONFIRMADO
97.118	EUA	#375486		CONFIRMADO
5.25	Holanda	#375623		CONFIRMADO
.34	China	#375668		CONFIRMADO

- IOC registrado manualmente em uma planilha
- Ação programada de importar o dado para todos os ambientes



TLP:CLEAR

Antes do MISP + AWS v2

- Desenvolvido sistema interno
- Criado integração com SIEM

```
<form class="form" [formGroup]="form">

  <div class="input-group mb-3">
    <input matInput formControlName="ip" name="ip" type="text" class="form-control" placeholder="IP" aria-label="IP">
    <input matInput formControlName="description" name="description" type="text" class="form-control" placeholder="Descrição" aria-label="Descrição">
    <button class="btn btn-outline-secondary" type="button" (click)="createRow()">Adicionar</button>
  </div>
</form>

<!--<form class="form" [formGroup]="groupSearch">
  <div class="input-group mb-3">
    <input matInput formControlName="pesquisar" name="pesquisar" type="text" class="form-control" placeholder="Pesquisar" aria-label="Pesquisar">
    <button class="btn btn-outline-secondary" type="button" (click)="searchRow()">Pesquisar</button>
  </div>
</form>

  <p>
    <a class="btn btn-info text-black" href="">Novo IP</a>
  </p>-->

  <table  class="table table-hover">
    <thead class="thead-dark">
      <tr>
        <th></th>
        <th>Id</th>
        <th>Ip</th>
        <th>Descrição</th>
        <th></th>
        <th></th>
        <tr>
    </thead>
    <tbody *ngFor="let produto of produto
      <tr>
      <td></td>
        <td>
          {{ produto.id }}
        </td>
        <td>
          {{ produto.ip }}
        </td>
        <td>
          {{ produto.description | title
        </td>
        <td>
          <a class="btn btn-danger" type
            <span class="fa fa-trash"></
```

IMCNet

Black List

IP | Descrição

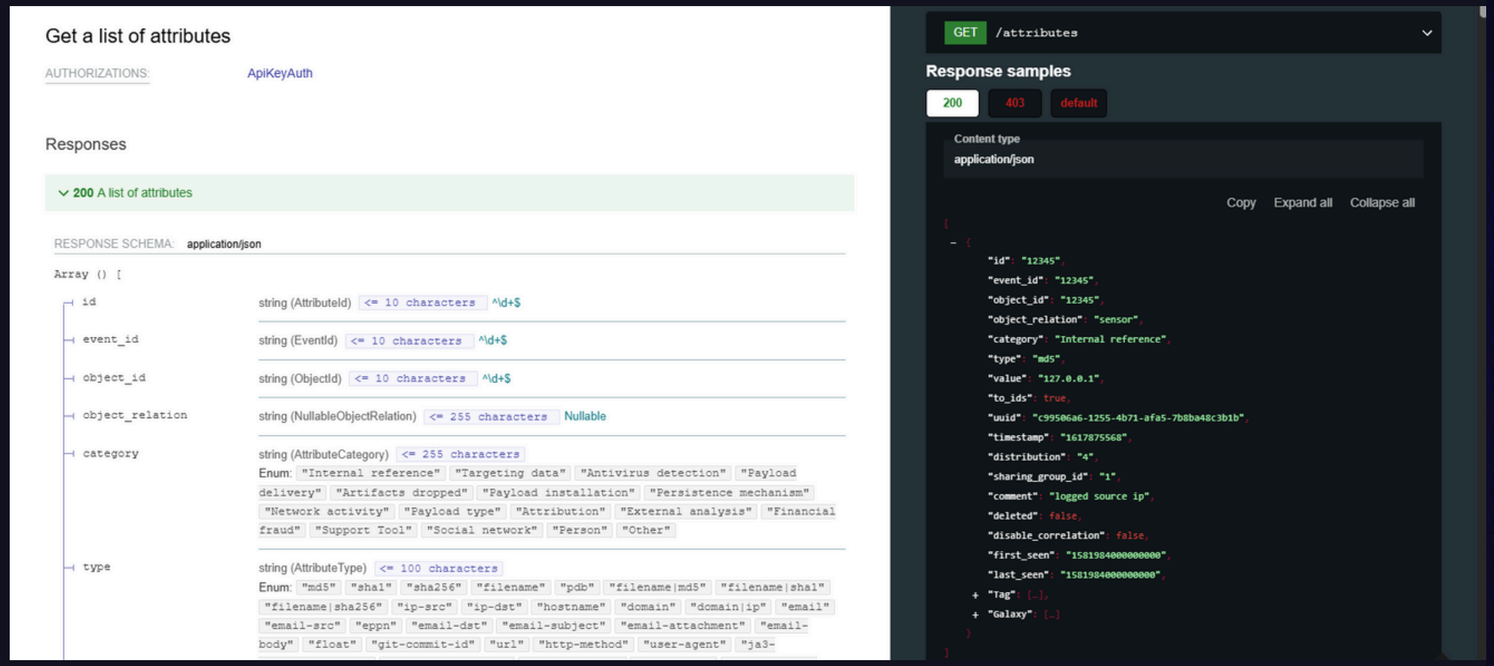
Id	Ip	Descrição

TLP:CLEAR

Fase 1- Etapas

1- Coleta via API MISP

Extração de atributos ip-src/ip-dst.



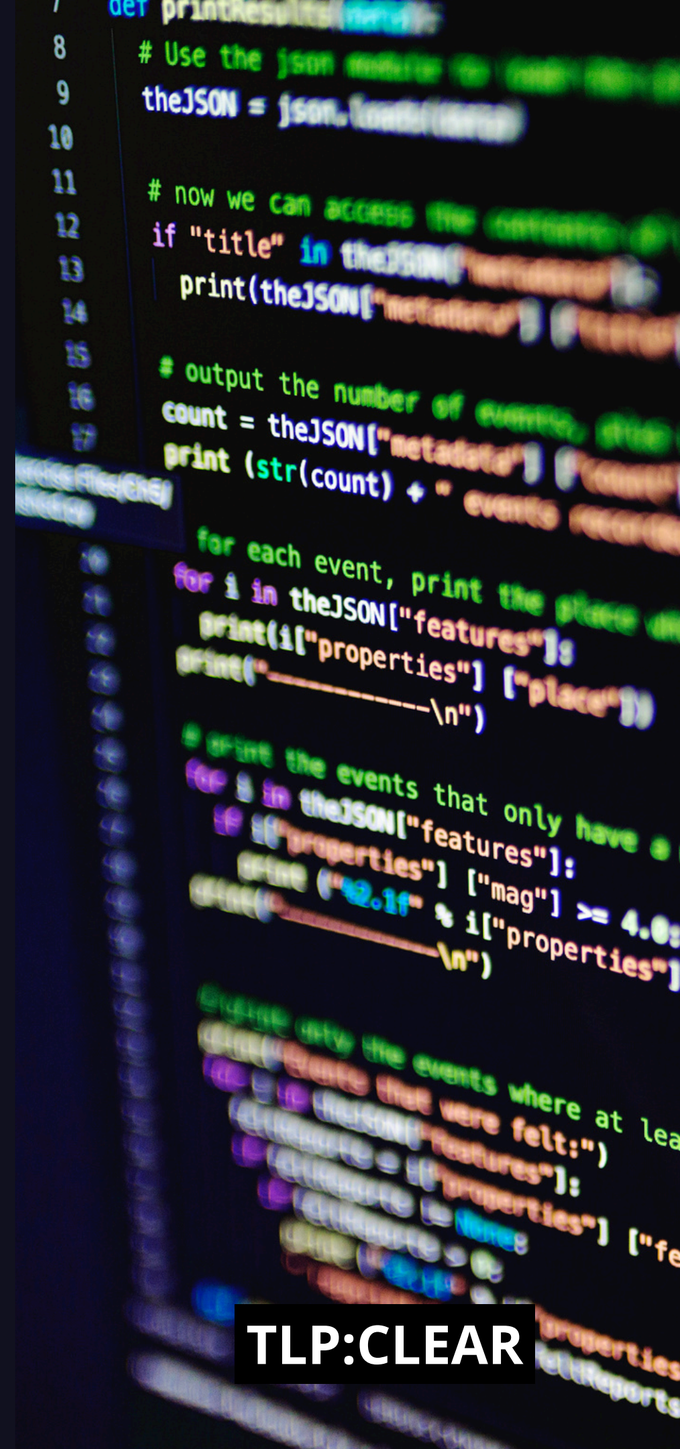
TLP:CLEAR

Fase 1- Etapas

```
123.60.141.107
206.168.34.115
170.84.62.15
120.82.67.10
123.249.114.36
45.156.130.8
36.139.217.213
27.210.154.220
165.154.20.200
207.90.244.6
95.214.55.43
47.89.218.135
185.224.128.59
95.214.55.138
45.148.10.242
89.190.156.137
47.84.79.4
185.224.128.47
94.156.66.238
141.98.11.122
36.50.176.173
47.254.84.31
76.76.21.21
8.216.86.85
185.165.191.26
39.106.18.244
23.94.20.2
47.89.230.62
95.214.27.169
66.240.236.116
117.187.117.6
8.212.134.63
5.42.86.0
35.190.39.113
152.32.156.136
128.199.36.184
8.216.87.143
78.189.103.63
207.90.244.3
185.196.11.114
47.236.90.162
8.216.121.252
8.216.91.239
```

2- Geração de Arquivo .txt

Criação de lista de IPs em formato de texto simples.



TLP:CLEAR

Fase 1- Etapas

1- Coleta via API MISP

Extração de atributos ip-src/ip-dst.

2- Geração de Arquivo .txt

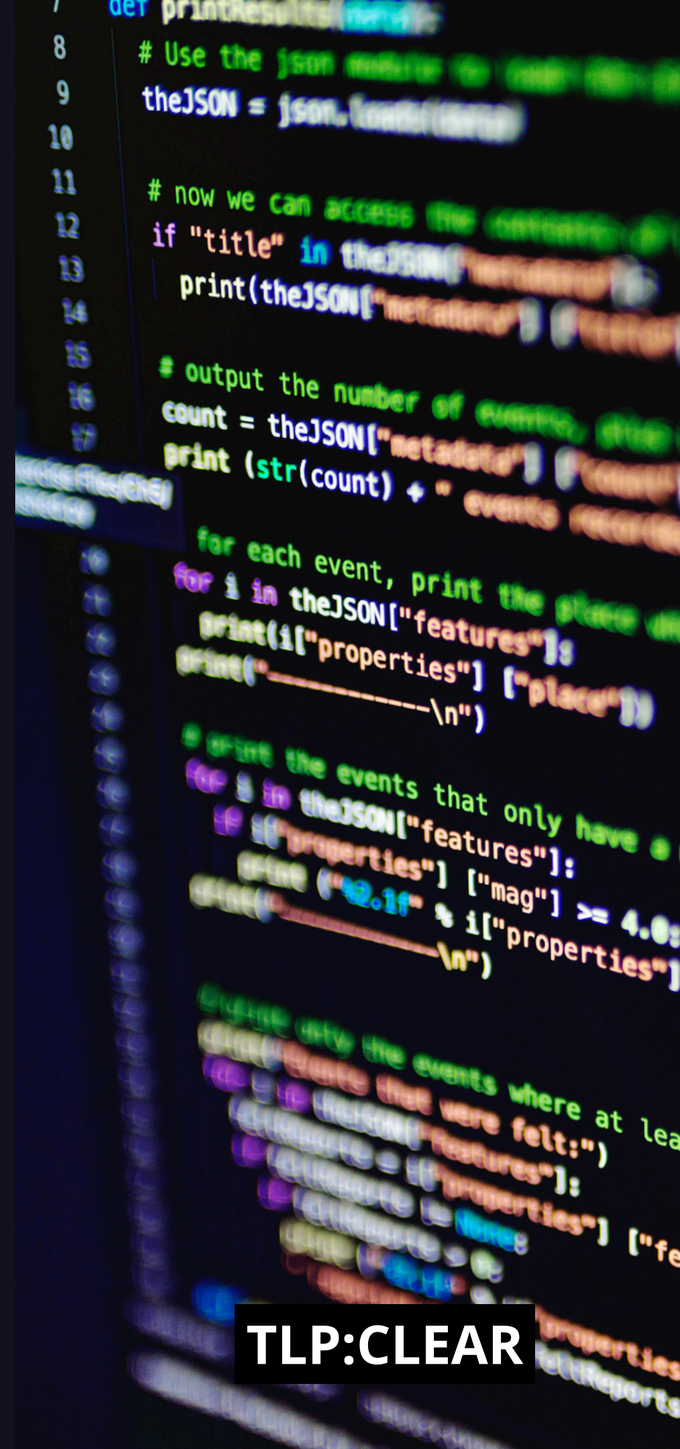
Criação de lista de IPs em formato de texto simples.

3- Publicação em Bucket S3

Disponibilização do arquivo com URL pública.

4- Consumo via dispositivos de segurança

Bloqueios automaticos.



Desenvolvimento

```
9
10  MISP_API_KEY = os.getenv('MISP_API_KEY')
11  MISP_URL = os.getenv('MISP_URL')
12  BUCKET_NAME = os.getenv('BUCKET_NAME')
13  OBJECT_KEY = os.getenv('OBJECT_KEY')
14
15  aws_access_key = os.getenv('AWS_ACCESS_KEY')
16  aws_secret_key = os.getenv('AWS_SECRET_KEY')
17
```

Armazena as configurações e credenciais da API do MISP e do AWS S3 usando variáveis de ambiente.

```
17
18  headers = {
19      'Authorization': MISP_API_KEY,
20      'Accept': 'application/json',
21      'Content-Type': 'application/json'
22  }
```

Define os cabeçalhos HTTP para autenticação e formatação da requisição à API do MISP.

TLP:CLEAR

Desenvolvimento

```
24    s3 = boto3.client('s3',
25                      aws_access_key_id=aws_access_key,
26                      aws_secret_access_key=aws_secret_key)
```

Cria um cliente do S3 usando as credenciais da AWS para realizar operações como upload de arquivos.

```
27
28  def get_ips_from_misp():
29      try:
30          response = requests.get(MISP_URL, headers=headers, verify=False)
31          response.raise_for_status()
32
33          data = response.json()
34
35          ips = [attr['value'] for attr in data if attr['type'] in ['ip-src', 'ip-dst']]
36
37          return ips
38
39      except requests.exceptions.RequestException as e:
40          print(f"Erro na requisição à API do MISP: {e}")
41          return []
```

Faz uma requisição à API do MISP para buscar os atributos do tipo ip-src e ip-dst. Em caso de erro, exibe uma mensagem e retorna uma lista vazia.

TLP:CLEAR

Desenvolvimento

```python

def save_ips_to_txt_and_s3(ips):
    try:
        file_name = 'blocklist-imcnet.txt'
        with open(file_name, 'w') as file:
            for ip in ips:
                file.write(f"{ip}\n")
        print("Arquivo 'blocklist-imcnet.txt' gerado com sucesso!")

        with open(file_name, 'rb') as file_data:
            s3.put_object(Bucket=BUCKET_NAME, Key=OBJECT_KEY, Body=file_data, ContentType='text/plain')
        print(f"Arquivo {file_name} enviado para o S3 com sucesso!")

    except Exception as e:
        print(f"Erro ao salvar o arquivo ou fazer upload para o S3: {e}")

```

Salva a lista de IPs em um arquivo .txt e envia esse arquivo para o bucket S3 definido nas variáveis de ambiente.
Em caso de falha, mostra o erro

TLP:CLEAR

Fase 1 - Novo fluxo

Ambiente x sofria um ataque

↓

Tratativa SOC

↓

Dado registrado no MISP

↓

IOC publicado na blocklist

↓

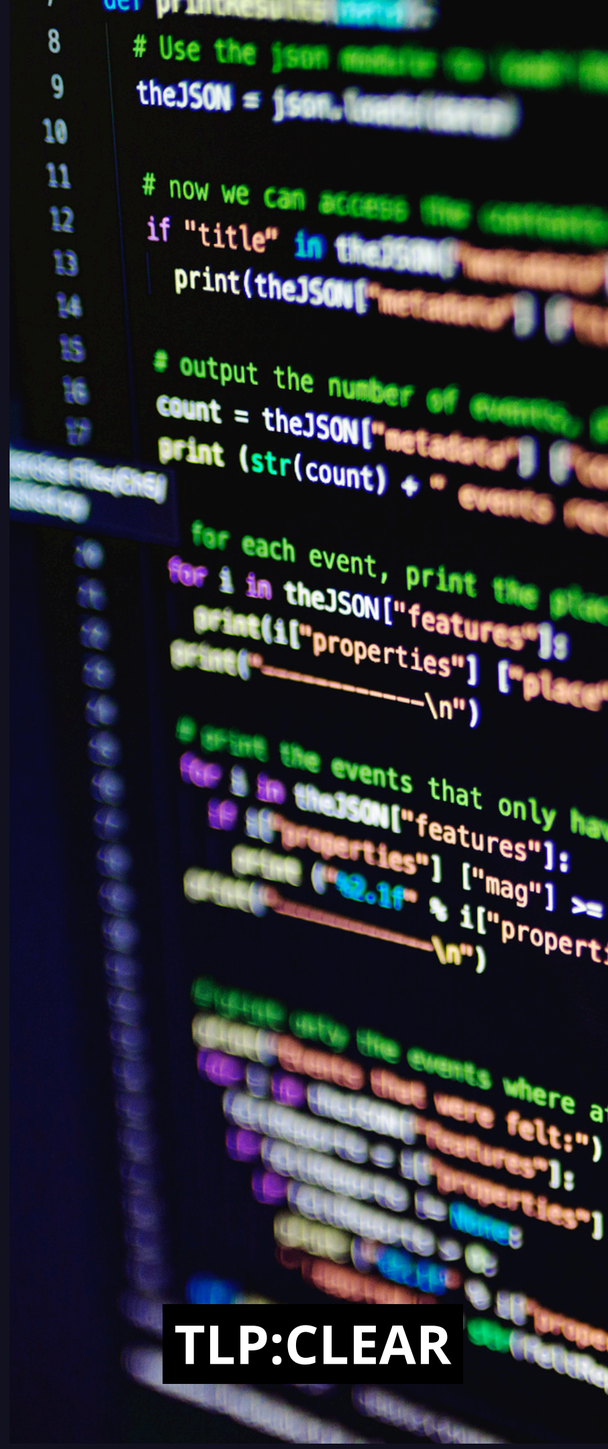
Dispositivo consome indicador

↓

Conexão bloqueada

↓

FIM



TLP:CLEAR

Fase 2

1- Consumo de IOCs

Ampliação da coleta de indicadores de comprometimento.

2- Integração com SIEM

Busca, correlação e análise de eventos de segurança.

AWS - MISP	Healthy	Hosted
misp Amazon S3	Healthy	

TLP:CLEAR

Fase 2

3- Correlação dos indicadores

Criação de incidentes para análise

Active - Match

Threat Intel - MISP

Severity

Dynamic

TLP:CLEAR

Fase 2

1- Consumo de IOCs

Ampliação da coleta de indicadores de comprometimento.

2- Integração com SIEM

Busca, correlação e análise de eventos de segurança.

3- Correlação dos indicadores

Criação de incidentes para análise

TLP:CLEAR

Resultados Alcançados: Impacto da Automação

A implementação da automação trouxe benefícios significativos para nossa operação e para a postura de segurança dos clientes.

100%

Manutenção e Escala

Solução fácil de manter e escalar para novos ambientes.

24/7

Postura de Segurança

Dados atualizados em tempo real, mitigação proativa.

80

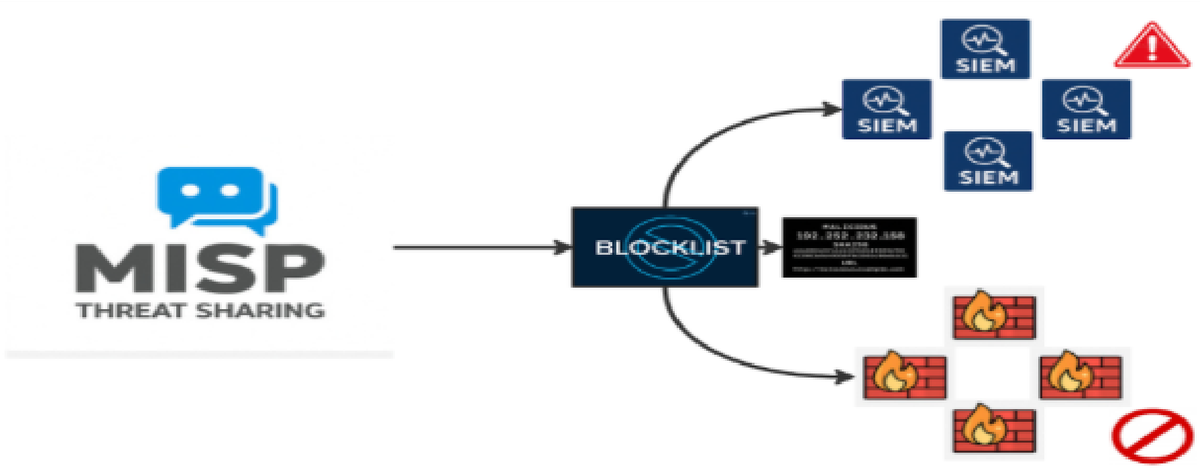
Horas/Mês Economizadas

Redução de tarefas manuais repetitivas.

Evolução de maturidade das partes envolvidas

TLP:CLEAR

- MISP tem sido uma excelente ferramenta para centralizar e compartilhar IOCs
- Integre
- Automatize
- Ganhe visibilidade
- Torne simples para quem interage com a ferramenta



TLP:CLEAR

Obrigado!

MISP - Threat Intelligence em Ação

Automatizando Bloqueios com MISP, Python e AWS

Andrey Souza
/in/andrey-souza-dev

Guilherme Bidin
/in/guilhermebidin

TLP:CLEAR