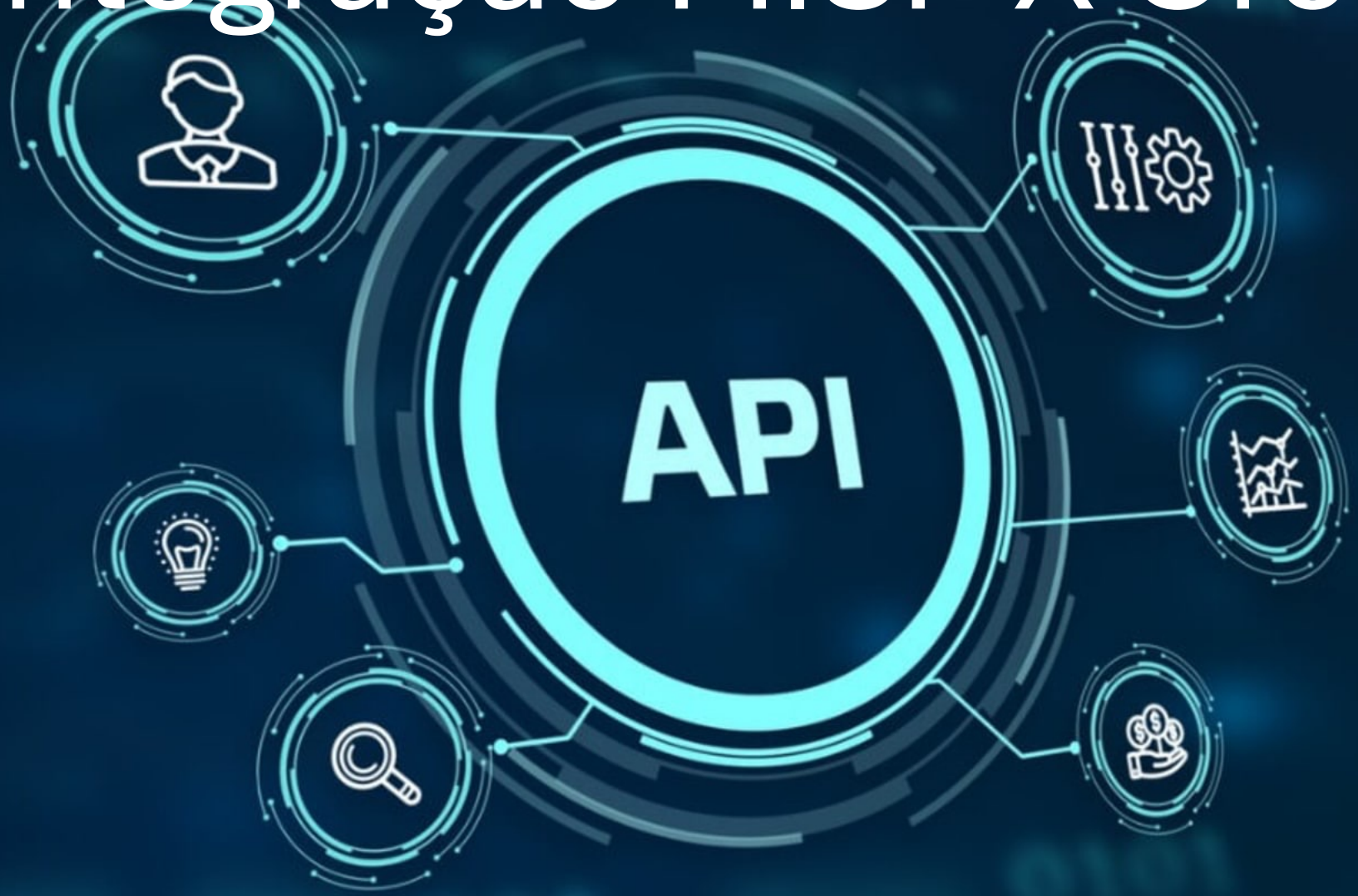
Integração MISP X Crowdstrike



TLP:CLEAR

Whoami

- Thiago Cunha
- Pai
- LinkedIn: thiagocunhasilva
- Github: Blu3B3ard
- Certificações: CRTO, CTIA, Security+, entre outras.
- Hobbies:
  - CTF
  - Vídeo Game
  - Bug Bounty

Problema

- Automatizar Detecção e bloqueio
- Ausência de documentação correta
- Qual pássaro usar?


:(
Your PC ran into a problem and needs to restart. We're
just collecting some error info, and then we'll restart for
you.
20% co
CROWDSTRIKE

TLP:CLEAR

Modos

- Detect – Funciona com IP’s, Dominios e Hash’s
- Prevent – Funciona com Hash’s

TLP:CLEAR

IOC’s

- HASH’s – MD5 e SHA256
- IP e Domínios

TLP:CLEAR


GitHub
TLP:CLEAR

Pré-requisitos

- Python 3.9 ou superior
- Authkey (MISP)
- ClientID e Client Secret (Crowdstrike)
- Criar uma Tag “crowdstrike” (MISP)

TLP:CLEAR

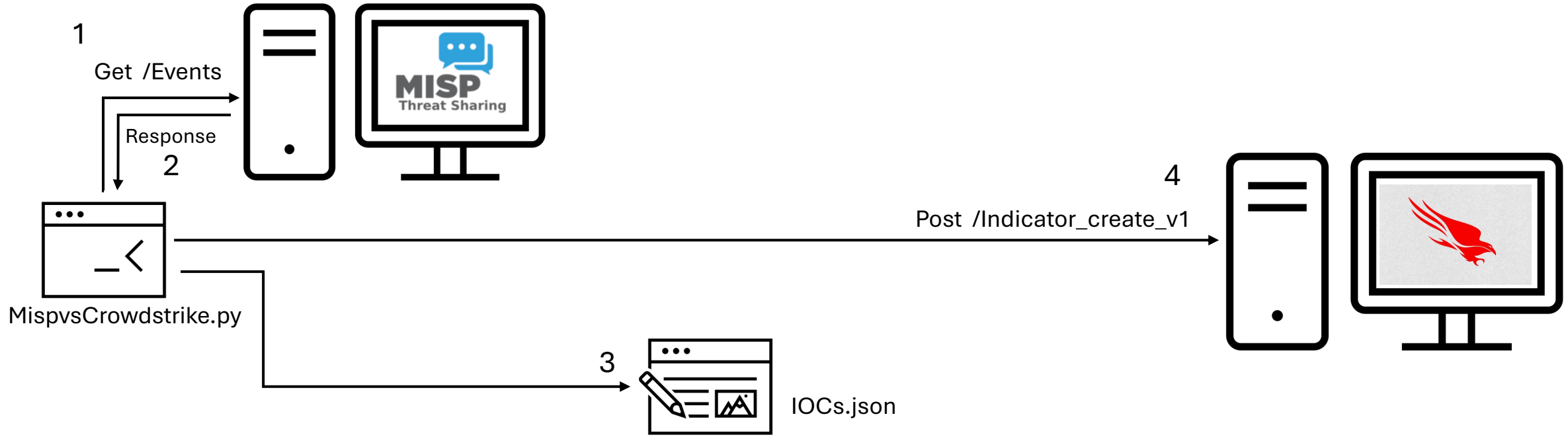
Show me the code

```python
# MISP Configuration
MISP_URL = 'https://site.com'
MISP_KEY = '<your_api_key>'

# MISP conection
misp = ExpandedPyMISP(MISP_URL, MISP_KEY, True)

# Get the events in MISP with the TAG "crowdstrike"
events = misp.search(tags=['crowdstrike'])
```

```python
# Define all credentials to Crowdstrike API
CLIENT_ID = '<your_client_id>'
CLIENT_SECRET = '<your_client_secret>'
```

TLP:CLEAR

Como funciona




```
"source": "MISP",
"action": "detect OU prevent",
"expiration": "2023-01-22T15:00:00.000Z",
"description": "IOC from MISP",
"type": attribute['type'],
"value": attribute['value'],
"platforms": ["linux“, “darwin”,”windows”],
"severity": "LOW",
"applied_globally": True
```

TLP:CLEAR


TLP:CLEAR

The End

TLP:CLEAR