SIDEF — DEPARTAMENTO DE DEFESA CIBERNÉTICA

Compartilhando Inteligência de Maneira Inteligente

Integração segura, governança de compartilhamento e enriquecimento de inteligência no MISP

Serpro

TLP:CLEAR

ROTEIRO

Agenda

1. Cooperação para Integração
2. Comunicação Segura
3. Diretrizes e Fluxo de Sincronização
4. Escopo de Compartilhamento
5. Módulo de Expansão MISP
6. Compartilhamento Enriquecido
7. Abordagens de Integração
8. Trabalho Atual

TLP:CLEAR

01

Cooperação para Integração

TLP:CLEAR

Motivações para Compartilhamento

Por que compartilhar inteligência?

Tempo real (IOC)

Indicadores de comprometimento compartilhados rapidamente para bloqueio e detecção imediatos entre parceiros.

“Se alguém já foi vítima, você não será a próxima"

Análise pós-incidente

Compartilhamento de contexto e lições aprendidas após a contenção, fortalecendo a resposta coletiva.

Inteligência estratégica

Visão de tendências e padrões de ameaça por setor, apoiando decisões de longo prazo.

TLP:CLEAR

Problema

Por que compartilhar inteligência é difícil?

Dados sensíveis

Informações que, se vazadas, expõem vítimas e infraestrutura.

Falta de confiança

Confiança limitada entre organizações dificulta a abertura do canal.

Risco de vazamento

Compartilhamento mal controlado amplia a superfície de exposição.

Perda de contexto

Informação sem contexto perde valor analítico e acionável.

"Compartilhar sem controle é tão perigoso quanto não compartilhar."

TLP:CLEAR

O desafio não é compartilhar — é controlar

"O MISP correlaciona e enriquece — e realimenta o SIEM com inteligência pronta para uso."

TLP:CLEAR

02

Comunicação Segura

TLP:CLEAR

Comunicação Segura

- **API Keys individuais —**
- uso de chaves próprias por usuário/organização
- **Associação direta —**
- chave vinculada a usuários e organizações específicas
- **Allowlist de IPs —**
- restrição de acesso via firewall/MISP
- **HTTPS (TLS) obrigatório —**
- criptografia em todo o canal de sincronização

- **Níveis de distribuição —**
- Organização, Comunidade, Todas as Comunidades
- **TLP —**
- uso do Traffic Light Protocol para classificação da informação
- **Acordos prévios —**
- definição clara de quais dados podem ser compartilhados

"Segurança não é opcional — é o que torna o compartilhamento possível."

TLP:CLEAR

03

Diretrizes e Fluxo de Sincronização

TLP:CLEAR

Diretrizes Iniciais

- **Acordos prévios —**
- definição de quais tipos de dados podem ser compartilhados entre as partes
- **Classificação da informação —**
- categorias como sensível e restrita orientam o tratamento de cada evento
- **TLP (Traffic Light Protocol) —**
- uso do protocolo para sinalizar limites de disseminação
- **Níveis de distribuição no MISP —**
- alinhamento entre política organizacional e configuração técnica

TLP:CLEAR

Fluxo de Sincronização em Duas Fases

Fase 1 — Empresa → Organização

1 — Envio de informações
Dados da instância da empresa enviados ao Parceiro

→

2 — Sync-user
Criação do usuário de sincronização

→

3 — Auth Key
Geração e compartilhamento da chave

→

4 — Firewall
Liberação de IPs envolvidos

→

5 — Push inbound
Configuração realizada pelo SERPRO

Fase 2 — Organização → Empresa

1 — Cadastro
Organização registrada no MISP local

→

2 — Sync-user
Criação do usuário de sincronização

→

3 — Auth Key
Geração e envio da chave do SERPRO

→

4 — Firewall
Liberação de IPs do SERPRO

→

5 — Remote Server
Configuração em modo push outbound

Fluxo espelhado em duas fases: na Fase 1 o SERPRO conduz a configuração em push inbound; na Fase 2 a organização parceira assume, em push outbound.

TLP:CLEAR

Validação

Teste de conectividade

Confirmação de que o canal entre as instâncias responde corretamente.

Sincronização de eventos

Validação do envio e recebimento de eventos de teste.

Confirmação do canal

Canal aprovado para uso operacional contínuo.

"A integração segura no MISP depende tanto da configuração técnica quanto de acordos claros e prévios sobre o compartilhamento de dados."

04

Escopo de Compartilhamento

TLP:CLEAR

Relação com Distribuição no MISP

Níveis padrão

- Sua Organização (Your Organisation Only[1])
- Esta Comunidade (This Community Only[2])
- Comunidades Conectadas (Connected Communities[3])
- Todas (All Communities[4])

Sharing Groups

– Controle granular e customizado

– Define exatamente quem recebe o dado

Granularidade máxima

O MISP combina níveis padrão de distribuição com Sharing Groups para controle fino.

[1] [2] [3] [4] *Designação dentro da plataforma MISP.*

TLP:CLEAR

ESCOPO DE COMPARTILHAMENTO

Sharing Groups no MISP

Controle avançado de compartilhamento

Lista fechada de confiança

Definem quais organizações específicas podem acessar determinados eventos.

Aplicação granular

Funcionam em nível de evento e de atributo, inclusive sobre o contexto.

Precisão sobre alcance

Quem recebe é definido no detalhe, não no atacado.

"Compartilhar com todos é fácil. Compartilhar com precisão é maturidade."

TLP:CLEAR

Benefícios dos Sharing Groups

Sob medida

Evita exposição desnecessária de dados a quem não precisa deles.

Segmentação de parceiros

Grupos distintos conforme o nível de confiança de cada parceiro.

Redução de risco

Menor chance de vazamento de dados sensíveis para terceiros.

Complemento ao TLP

Ex.: TLP:AMBER combinado a um grupo específico de destinatários.

"Menos exposição, mais confiança."

TLP:CLEAR

Limitação Importante

- **Restrição —**
- um evento só pode ter um único Sharing Group associado
- **Sem múltiplos grupos —**
- não é possível vincular mais de um grupo ao mesmo evento
- **Replicação necessária —**
- quando parceiros diferentes precisam da mesma informação, o evento precisa ser duplicado

Resultado: duplicação de eventos no MISP

"Controle tem custo — e às vezes esse custo é duplicação."

TLP:CLEAR

O que Você Compartilha?

Compartilhar

- **IOCs —**
- IPs, domínios, hashes
- **Contexto —**
- vetor de ataque, TTPs observadas
- **Classificação —**
- categoria e descrição do evento

Evitar

- Dados sensíveis que identifiquem vítimas ou ativos internos
- Informações irrelevantes que não agregam valor analítico

Dados ≠ Inteligência: dado bruto sem critério; inteligência é contexto com propósito.

"Cada IOC conta uma história — nenhuma história deve expor a organização e os parceiros."

TLP:CLEAR

Dados sensíveis

Antes de compartilhar IOCs, remover ou anonimizar:

Identificação da vítima

Nome da empresa, usuários, domínios internos.

Infraestrutura interna

IPs privados, redes, VPNs.

Detalhes de ativos

Hostnames, sistemas específicos.

Caminhos e artefatos locais

Paths com usuários e estrutura interna.

Metadados ocultos

Autor, máquina, timezone, IDs únicos.

Evidências brutas

Headers, dumps, dados não sanitizados.

05

Módulo de Expansão MISP

TLP:CLEAR

Objetivo e Fluxo Básico

Objetivo

- Enriquecer atributos do MISP (IP, domínio, URL etc.)
- Integrar com APIs externas de reputação, bloqueio e SIEM

Desacoplado e reutilizável

O módulo plugável evita lógica de enriquecimento embutida no core do MISP.

Fluxo básico

1. **Recebe atributo** — MISP envia o atributo
2. **Identifica tipo** — IP, domínio, URL...
3. **Monta payload** — Padroniza o envio
4. **Chama API externa** — Serviço de enriquecimento
5. **Retorna ao MISP** — Resultado incorporado

Estrutura do Código

mispattributes

Define quais tipos de atributos o módulo aceita.

moduleinfo

Metadados do módulo: nome, versão e descrição.

handler(q)

Função principal — o coração do módulo.

Funções auxiliares

introspection() e version(), obrigatórias para o MISP reconhecer o módulo.

Código Base (Configuração)

```
import json
import requests

API_ENDPOINT = "https://api.externa.local/ingest"
API_KEY = "CHAVE_API"

mispattributes = {
    'input': ['*'],
    'output': ['text']
}
```

Pontos-chave

Endpoint usando HTTPS. Aceita qualquer atributo do MISP. Preparado para integração genérica.

Função Principal (handler)

```
def handler(q=False):
    if not q:
        return False

    request = json.loads(q)
    event_id   = request.get('event', {}).get('id')
    attr_type  = request.get('type')
    attr_value = request.get('value')
```

Pontos-chave

Recebe o JSON do MISP e extrai: ID do evento, tipo do atributo e valor do atributo.

Construção do Payload

```
payload = {
    "source": "misp",
    "event_id": event_id,
    "attribute_type": attr_type,
    "attribute_value": attr_value,
    "raw_misp": request
}
```

Pontos-chave

Estrutura padronizada. Mantém os dados originais. Facilita integração com qualquer API.

Envio Seguro via HTTPS

```
response = requests.post(
    API_ENDPOINT,
    json=payload,
    headers={
        "Authorization": f"Bearer {API_KEY}",
        "Content-Type": "application/json"
    },
    verify=True,
    timeout=30
)
```

Boas práticas aplicadas

Validação do certificado SSL, uso de HTTPS, timeout definido e autenticação segura via Bearer token.

Retorno para o MISP

```
return {
  "results": [{
      "types": ["text"],
      "values": [
        f"status: {response.status_code}"
      ]
  }]
}
```

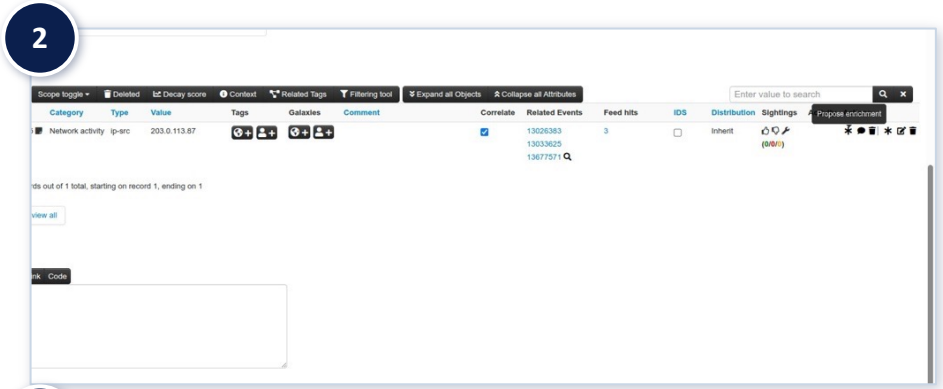
Pontos-chave

Formato obrigatório do MISP. Retorna o status da API. Pode incluir dados enriquecidos.

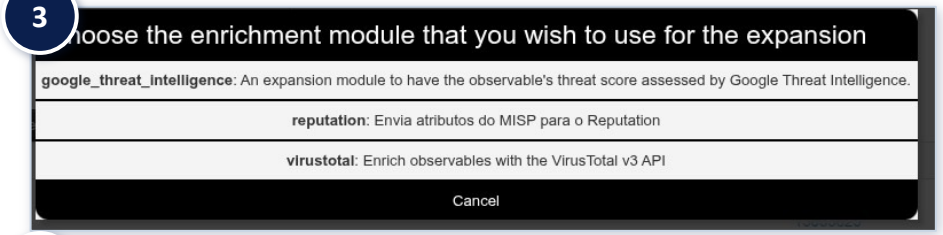
Passo a passo no MISP

1

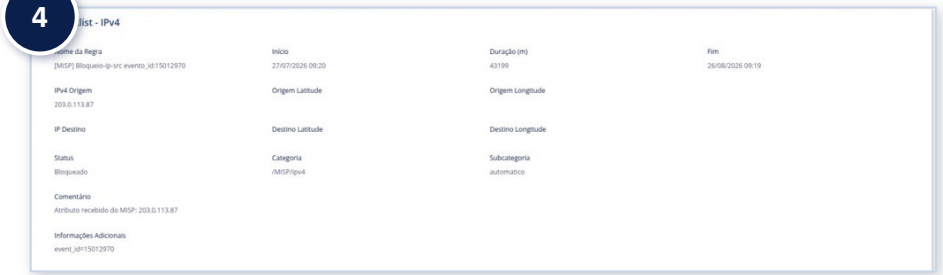
2



3



4



1 Evento no MISP · 2 Propor enriquecimento · 3 Escolher módulo (reputation) · 4 Regra de bloqueio criada no serviço

Na prática: o IOC vira bloqueio

```
# handler(q) envia o atributo:
POST https://api.externa.local/ingest
Authorization: Bearer •••
{
  "source": "misp",
  "event_id": 15012970,
  "attribute_type": "ip-src",
  "attribute_value": "203.0.113.87",
  "tag": "scanning:scan-rede"
}
```

Resultado no serviço

Blocklist · IPv4

Regra: [MISP] Bloqueio-ip-src evento_id:15012970

IPv4: 203.0.113.87 → Bloqueado

Categoria: /MISP/ipv4 · automatico

Validade: 30 dias (27/07 → 26/08)

Rastreável: event_id = 15012970

06

Compartilhamento Enriquecido

TLP:CLEAR

O que é Enriquecimento?

- **Transformação —**
- enriquecer dados é transformar indicadores em inteligência utilizável
- **Processo —**
- atributos (IOCs) são enriquecidos antes do compartilhamento
- **Contexto —**
- adiciona reputação, geolocalização e classificação de ameaça
- **Correlação —**
- cruza dados com múltiplas fontes externas e internas

Enriquece com

Geolocalização, ASN, histórico de atividades e classificação de ameaça.

"Dado sem contexto não é inteligência."

TLP:CLEAR

Módulos Padrão do MISP (Enrichment)

Exemplos que podem ser usados diretamente:

CIRCL Passive DNS
Histórico de resolução de domínios.

VirusTotal
Reputação de IP, domínio e hash.

GeoIP
Localização geográfica de IP.

ASN Lookup
Identificação de sistema autônomo.

WHOIS
Informações de registro de domínio.

URLhaus
Detecção de URLs maliciosas.

https://github.com/MISP/misp-modules/tree/main/misp_modules/modules/expansion

Módulo Genérico (API Externa)

Vantagens

- Aceita qualquer tipo de atributo
- Integra com qualquer sistema externo
- Desacoplamento da lógica de enriquecimento
- Flexibilidade para ambientes dinâmicos

Permite enviar dados para

APIs internas, data lakes e pipelines de segurança — centralizando inteligência em SIEM/SOAR.

07

Abordagens de Integração

TLP:CLEAR

Estratégia de Integração

Por onde começar?

- Priorizar integrações prontas de mercado
- Aproveitar conectores nativos (MISP ↔ SIEM/SOAR)
- Reduzir esforço de desenvolvimento e manutenção
- Maior confiabilidade e suporte da comunidade

Quando desenvolver integração própria?

- Necessidade específica do ambiente
- Sistemas legados ou APIs customizadas
- Requisitos não atendidos pelas integrações existentes

Primeiro reutilizar, depois construir.

TLP:CLEAR

Real-Time Streaming vs Scheduled Job

Critério	Real-Time Streaming (Socket)	Scheduled Job (Batch/Polling)
Latência	Mínima — dado chega ao MISP quase instantaneamente	Dependente do intervalo do próximo ciclo do job
Uso de recursos	Constante — listener sempre ativo	Sob demanda — apenas durante a execução
Complexidade	Maior— gestão de conexões, buffer, quedas	Menor — scripts simples de codificar e depurar
Escalabilidade	Excelente para alto volume por segundo	Melhor para volumes moderados/consultas a APIs
Resiliência	Perda possível se o listener cair sem buffer	Fácil retry e checkpoint de “onde parei”
Casos de uso	Logs de firewall, IDS/IPS, sensores (Syslog)	Enriquecimento via API, banco de dados, CSV/logs

Serpro

08

Trabalho Atual

log2misp normaliza · misp-classifier classifica

TLP:CLEAR

TRABALHO ATUAL

log2misp — normalizar qualquer log para o MISP

Somar um formato custa um leitor. O caminho do modelo canônico até o MISP existe uma vez só.

1 — Log

Qualquer formato: CEF, JSON (Suricata EVE), Syslog 5424, Zeek

→

2 — Leitor

Um por formato: traduz o formato dele, não conhece o MISP

→

3 — Modelo canônico

EventoNormalizado: um vocabulário só, comum a todos os leitores

→

4 — Mapeamento

Único: o papel source/destination escolhe ip-src × ip-dst

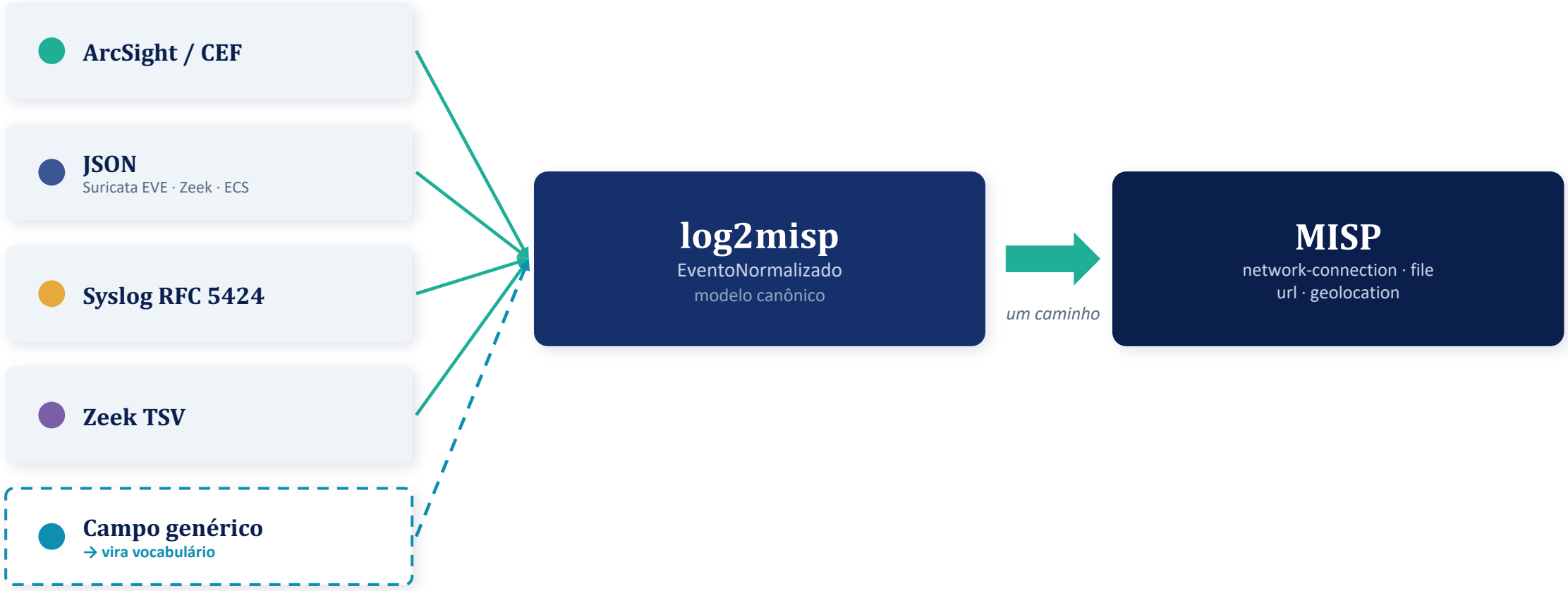
→

5 — MISP

Objetos coerentes: network-connection, file, url, geolocation

Serpro

Quatro formatos, um caminho até o MISP



3 → 1 parsers CEF · **0** dependências (só stdlib) · o papel escolhe ip-src × ip-dst

TLP:CLEAR

TRABALHO ATUAL

misp-classifier — do valor ao tipo, por bytes

O que faz

- Valor bruto → tipo MISP: md5, ip-dst, domain, url, btc, filename…
- + categoria + machine tags (tlp:*, type:OSINT, ioc:*…)

Como: análise de bytes

- Cada valor vira um vetor de 22 grandezas: entropia, histograma, is_all_hex…
- 181 taxonomias — 100% do MANIFEST oficial do MISP
- Base SQLite de conversão reutilizável (valor → tipo/tags)

Em vez de depender só de regex: cada valor é uma sequência de bytes.

TLP:CLEAR

misp-classifier — performance e estatística

Benchmark — 1.050 amostras, 14 classes; medido nesta máquina, rode o seu. O determinístico classifica ~150 mil atributos/s em Python puro; os estatísticos entram como desempate.

Modelo	Acurácia	Vazão (itens/s)	µs / item
deterministic	**99,1%**	**150.892**	**6,6**
gaussian-nb	97,0%	8.763	114,1
nearest-centroid	93,5%	12.733	78,5
entropy-rule	61,9%	46.893	21,3

Juntos, sem acoplar

```
from log2misp import ler_auto, para_misp
from misp_classifier.log2misp_bridge \
    import tipo_de_valor

# tipa os campos "extras" que o
# esquema do log nao resolveu:

obj, attr = para_misp(
    ler_auto(linha),
    classificador=tipo_de_valor)
```

Composição sem acoplar

O log2misp normaliza; o misp-classifier tipa o que o esquema não resolve, pelo caminho determinístico rápido. O classificador é injetado, não importado — os projetos não se acoplam.

Aprende com a sua instância

1 · UNIVERSAL

Formato

Os leitores (ArcSight, JSON, syslog, Zeek) mapeiam cada campo → tipo e papel pelo esquema do formato. Vêm no projeto, iguais para toda instância.

2 · APRENDIDO

Vocabulário

Campo desconhecido não é chutado: fica em extras. A triagem confirma xpto_origem = ip · source e isso vira regra — dado, não código.

3 · RESULTADO

Cobertura

O campo que caía no blob vira observável ip com direção — montando o objeto MISP correto. Por instância e auditável.

Regra curada e auditável — não é um modelo de ML que muda sozinho.

TLP:CLEAR

O incerto não entra no MISP

Trava de confiança

- Dado não-compreendido é tratado na etapa 2 — o classificador, não o leitor.
- Cada palpite carrega confidence e ambiguous_with.
- Abaixo do limiar (min_confidence) ou tipo text → não vai pro MISP: vai pro blob / triagem.

Loop de aprendizado

- A triagem transforma a exceção em regra aprovada — sem editar JSON na mão.
- Registra quem, quando e o quê: trilha JSONL auditável.
- SIGHUP recarrega o coletor sem reiniciar — a regra passa a acertar.
- Por instância e reversível; não é ML caixa-preta.

O incerto não polui o MISP: vira fila de triagem — e a triagem vira acerto.

TLP:CLEAR

Conclusão

- **Controle antes de alcance —**
- Sharing Groups e TLP dão precisão ao compartilhamento, mesmo ao custo de alguma duplicação
- **Segurança é pré-requisito —**
- API Keys, HTTPS e acordos prévios tornam o canal de sincronização confiável
- **Enriquecimento agrega valor —**
- módulos padrão e genéricos transformam IOCs isolados em inteligência acionável
- **Reutilizar antes de construir —**
- conectores nativos reduzem custo; desenvolva integrações próprias apenas quando necessário.
- **Padrões evoluem —**
- TLP 2.0 e as atualizações contínuas do MISP exigem revisão periódica das políticas internas

Obrigado!

Mailson Ribeiro Santos
Ulisses de Sá Alencar e Moraes

SIDEF — Departamento de Defesa Cibernética

– mailson.santos@serpro.gov.br
– ulisses.moraes@serpro.gov.br

/serprobrasil @serprobrasil @serpro /serpro serpro.gov.br

Serpro

TLP:CLEAR