nic.br cgi.br | cert.br

Workshop MISP

21 de setembro de 2022

São Paulo, SP

MISP:
Boas Práticas de Instalação, Configuração e Uso

Marcus Lahr
Analista de Projetos de Segurança
marcus@cert.br

Marcelo Chaves
Analista de Projetos de Segurança
mhp@cert.br

Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br nic.br cgi.br

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e Político

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

Agosto/1996: CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

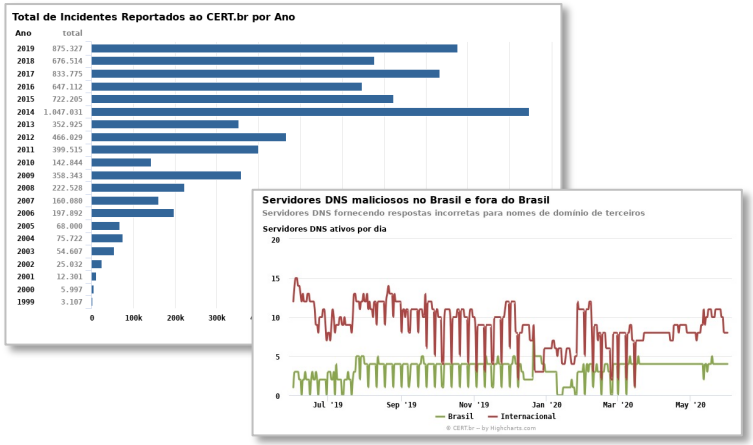
- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Tratamento de Incidentes:
Fontes dos Dados, Métricas e Compartilhamento

TLP:CLEAR

Notificações voluntárias de incidentes enviadas para: cert@cert.br



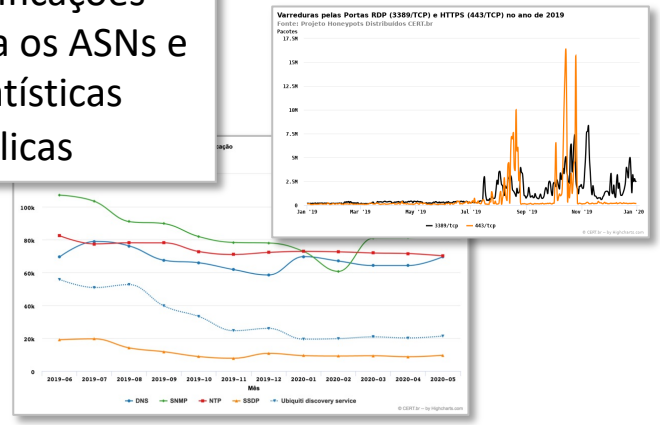
Compartilhamento via MISP

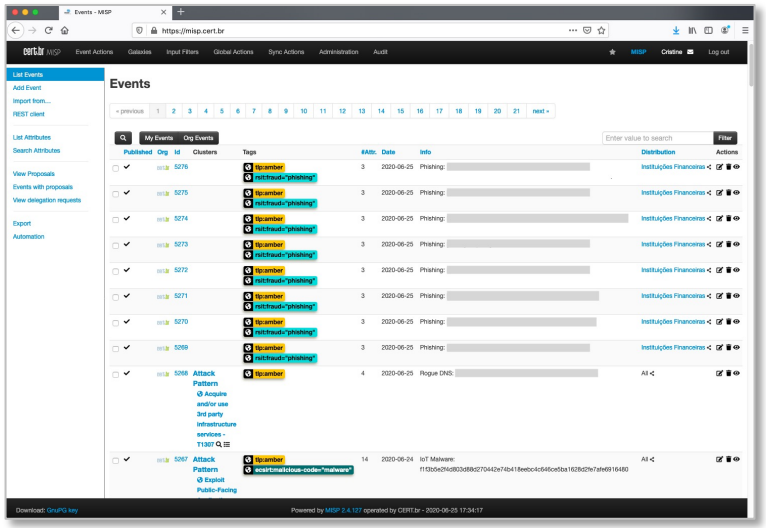
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

Threat feeds

- *Honeypots* Distribuídos do CERT.br
- Team Cymru
- SpamHaus
- ShadowServer
- Shodan
- Operações Anti-Botnet (Microsoft/FBI)

Notificações para os ASNs e estatísticas públicas





https://cert.br/stats

https://cert.br/misp/

Agenda

– Boas práticas para instalação do MISP
– Dicas sobre *sizing* de recursos de *hardware* para instâncias MISP
– Operações básicas do MISP
– Passo a passo para a criação de eventos reais
– Rodada de Q&A

Boas práticas para a instalação do MISP

cert.br nic.br cgi.br

Considerações de Segurança

A instância em produção precisa ter um bom *hardening*

- *Firewall* de *host* permitindo entrada da rede de gerência e de instâncias de parceiros, e saída para a Internet
- Acesso via SSH somente com chave criptográfica

Não utilizar imagens ou containers baixados da Internet para instâncias em Produção

- Impossível garantir que a imagem não possua vulnerabilidades ou Cavalos de Troia
- Impossível recuperar senhas, e configurações prévias podem atrapalhar processos futuros de atualização

Usar sempre um certificado válido

- Não utilizar certificados auto assinados e nunca desligar a checagem de certificados

A instância MISP precisa ser mantida atualizada e potencialmente terá *payloads* maliciosos

- A instância MISP precisa acessar a Internet para atualização do sistema e do MISP (GitHub)
- O WAF corporativo ou *proxy* reverso (se houver) não deve interferir no tráfego do MISP
- Ferramentas Anti-DDoS não devem classificar acessos de instâncias parceiras como ataques (por exemplo, classificar muitos SYNs como DDoS)

Instalação do MISP

Tutorial completo para instalação e *hardening* do MISP em sistemas Ubuntu:

https://www.cert.br/misp/tutorial-ubuntu/

Dicas sobre *sizing* de recursos de *hardware* para instâncias MISP

cert.br nic.br cgi.br

Sizing (1/3)

É possível rodar o MISP em ambientes virtualizados com apenas 1 CPU, 20GB de disco e 2GB de memória RAM, entretanto esses valores precisam ser alterados conforme a utilização do MISP

A única recomendação feita pelos desenvolvedores do MISP é: “A utilização de SSDs é extremamente recomendada para o MISP”

As demais configurações vão depender da utilização do MISP

Referências para *sizing*:

- https://www.misp-project.org/misp-training/a.c-deployment.pdf
- https://www.misp-project.org/sizing-your-misp-instance/

Sizing (2/3)

Os seguintes elementos do MISP podem impactar o servidor de diferentes formas:

- Quantidade de eventos
  - RAM, velocidade de disco

- Correlações
  - RAM, velocidade de disco, espaço em disco
    - Obs: Evitar correlações demasiadas

- Contextualizar eventos
  - RAM e velocidade de disco
    - Obs: Sempre que possível, utilizar tags e galáxias nos evento ao invés de colocar em cada um dos atributos

Sizing (3/3)

- Número de usuários simultâneos
  - RAM, CPU, velocidade de disco

- Estratégias para logs
  - Espaço em disco

- Usuário fazendo consultas via API (especialmente consultas pesadas)
  - RAM, CPU e velocidade de disco

Sizing – Exemplos

Recomendação do CIRCL:

– 16GB de memória RAM e 2 CPUs para servidores com uma pequena comunidade de compartilhamento de informações

Instâncias do CIRCL:

– 128 GB de memória RAM e 32 núcleos de processamento na instância CIRCL private (servidor *bare metal*)

– 8GB de memória RAM e 4 núcleos de processamento na instância COVID misp

– 2GB de memória RAM e 1 núcleo de processamento na instância de treinamento (recomendado apenas para testes e treinamentos)

Fonte: https://www.misp-project.org/sizing-your-misp-instance/

Operações básicas do MISP

cert.br nic.br cgi.br

Misp Concepts Cheat Sheet

MISP Concepts Cheat sheet

Glossary

Correlations: Links created automatically whenever an `Attribute` is created or modified. They allow interconnection between `Events` based on their attributes.

Correlation Engine: Is the system used by MISP to create correlations between `Attribute` 's value. It currently supports strict string comparison, SSDEEP and CDIR blocks matches.

Caching: Is the process of *fetching* data from a MISP instance or feed but only storing hashes of the collected values for correlation and look-up purposes.

Delegation: Act of transfering the ownership of an `Event` to another organisation while hidding the original creator, thus providing anonymity.

Deletion (hard/soft): *Hard deletion* is the act of removing the element from the system; it will not perform revocation on other MISP instances. *Soft deletion* is the act flagging an element as deleted and propagating the revocation among the network of connected MISP instances.

Extended Event: `Event` that extends an existing `Event` , providing a combined view of the data contained in both `Events` . The owner of the extending `Event` is the organisation that created the extension. This allows anyone to extend any `Events` and have total control over them.

`Galaxy` Matrix: Matrix derived from `Galaxy Clusters` belonging to the same `Galaxy` . The layout (pages and columns) is defined at the `Galaxy` level and its content comes from the `Galaxy Clusters` meta-data themselves.

Indicators: `Attribute` containing a pattern that can be used to detect suspicious or malicious activity. These `Attributes` usually have their `to_ids` flag enabled.

Orgc / Org: *Creator Organisation* (**Orgc**) is the organisation that created the data and the one allowed to modify it. *Owner Organisation* (**Org**) is the organisation owning the data on a given instance and is allowed to view it regardless of the distribution level. The two are not necessarily the same.

Publishing: Action of declaring that an `Event` is ready to be synchronised. It may also send e-mail notifications and makes it available to some export formats.

Pulling: Action of using a user on a remote instance to fetch the accessible data and storing it locally.

Pushing: Action of using an uplink connection via a *sync. user* to send data to a remote instance.

Synchronisation: Is the exchange of data between two (or more) MISP instances throught the *pull* or *push* mechanisms.

Sync. filtering rule: Can be applied on a synchronisation link for both the *pull* and *push* mechanisms to block or allow data to be transfered.

Sync. User: Special role of a user granting addional sync permissions. The recommanded way to setup *push* synchronisation is to use *sync users*.

Proposals: Are a mechanism to propose modications to the creating organisations (**Orgc**). If a path of connected MISP instances exists, the `Proposal` will be synchronised allowing the creator to accept or discard it.

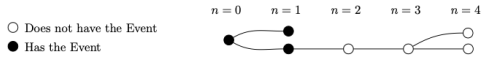
Distribution

Controls who can see the data and how it should be synchronised.

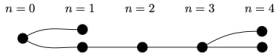
Organisation only: Only members of your organisation

This community: Organisations on this MISP instance

Connected Communities: Organisations on this MISP instance and those on MISP instances synchronising with this one. Upon receiving data, the distribution will be downgraded to `This community` to avoid further propagation. ($n \leq 1$)



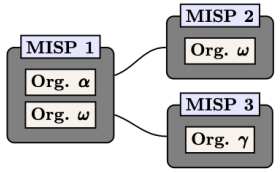
All Communities: Anyone having access. Data will be freely propagated in the network of connected MISP instances. ($n = \infty$)



Sharing Groups: Distribution list that exhaustively keeps track of which organisations can access the data and how it should be synchronised.

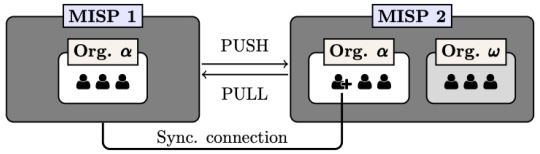
`Sharing Group` configuration	
Organisations	Org. α Org. ω Org. γ
Instances*	MISP 1 MISP 2 MISP 3

*Or enable roaming mode instead



Synchronisation

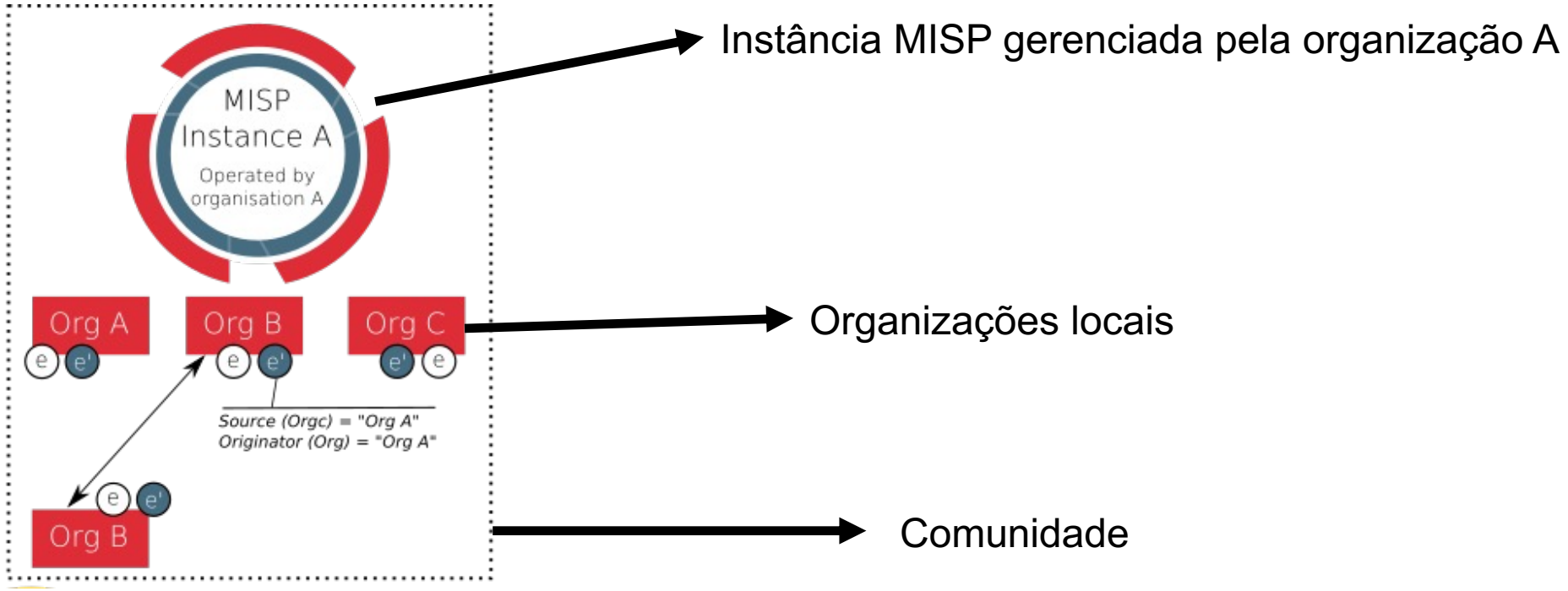
*The act of **sharing** where everyone can be a consumer and/or a producer.* A one way synchronisation link between two MISP instances. Organisation α created a *sync user* on MISP 2 and noted down the generated API Key. A synchronisation link can be created on MISP 1 using the API Key and the organisation of the *sync user*. At that point, MISP 1 can *pull* data from MISP 2 and *push* data to MISP 2.



Fonte: https://www.misp-project.org/misp-training/cheatsheet.pdf

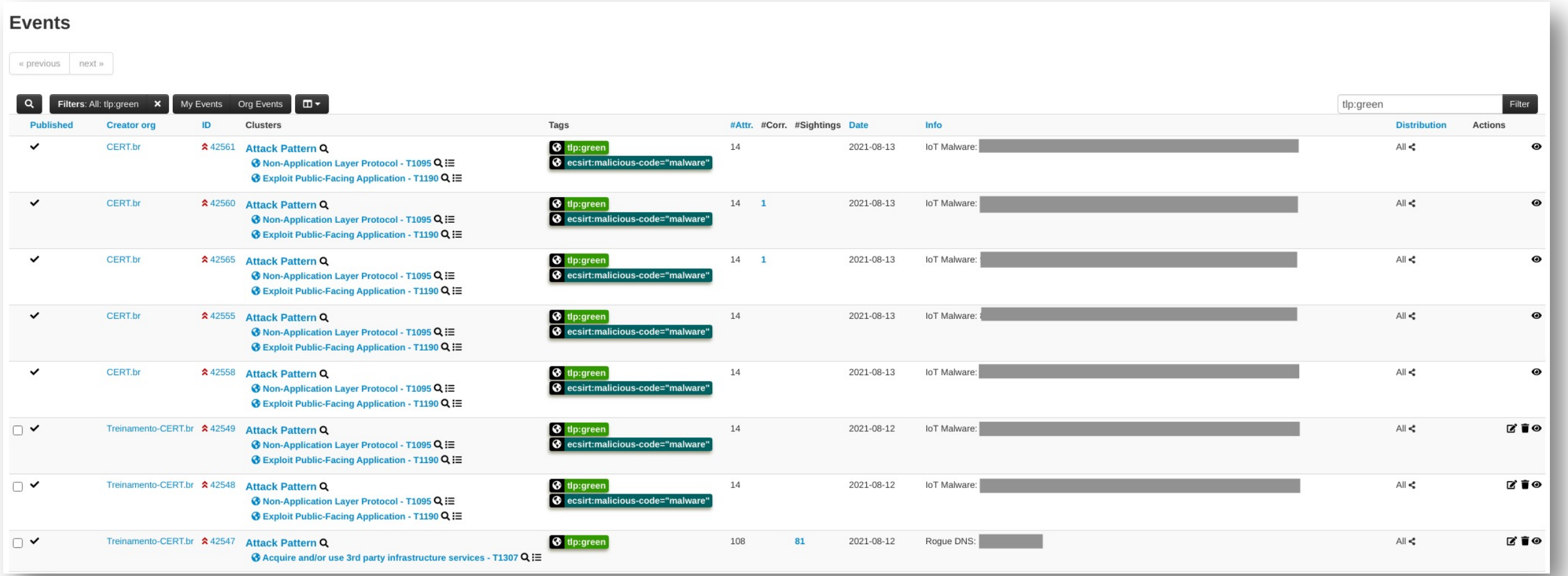
Arquitetura do MISP
Instância, organizações e comunidade

TLP:CLEAR



Adaptado de: https://www.circl.lu/doc/misp/sharing/

Eventos



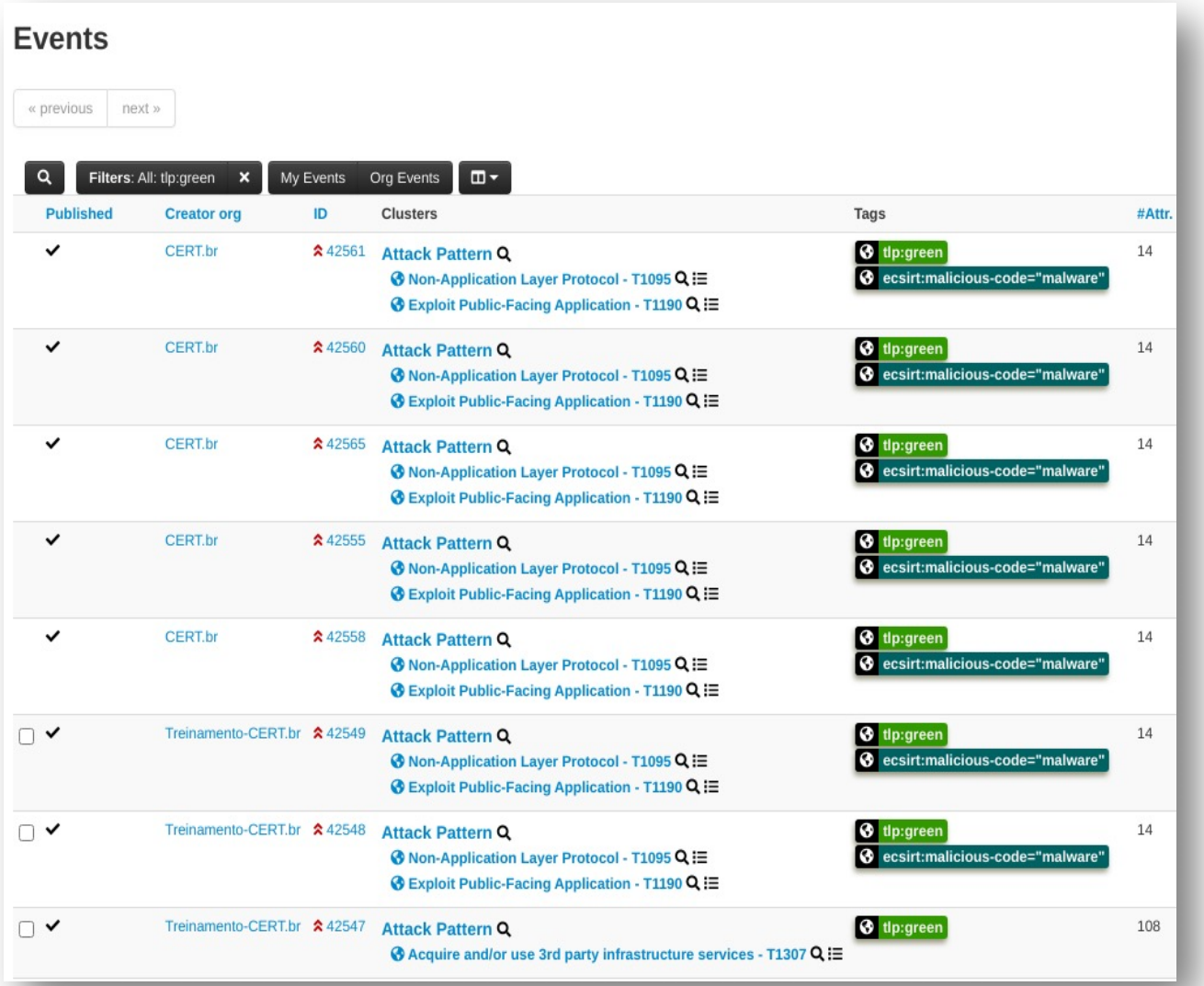
Events

« previous next »

Filters: All: tlp:green | My Events | Org Events | tlp:green | Filter

Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	#Sightings	Date	Info	Distribution	Actions
✔	CERT.br	42561	Attack Pattern Non-Application Layer Protocol - T1095 Exploit Public-Facing Application - T1190	tlp:green ecsirt:malicious-code="malware"	14			2021-08-13	IoT Malware:	All	
✔	CERT.br	42560	Attack Pattern Non-Application Layer Protocol - T1095 Exploit Public-Facing Application - T1190	tlp:green ecsirt:malicious-code="malware"	14	1		2021-08-13	IoT Malware:	All	
✔	CERT.br	42565	Attack Pattern Non-Application Layer Protocol - T1095 Exploit Public-Facing Application - T1190	tlp:green ecsirt:malicious-code="malware"	14	1		2021-08-13	IoT Malware:	All	
✔	CERT.br	42555	Attack Pattern Non-Application Layer Protocol - T1095 Exploit Public-Facing Application - T1190	tlp:green ecsirt:malicious-code="malware"	14			2021-08-13	IoT Malware:	All	
✔	CERT.br	42558	Attack Pattern Non-Application Layer Protocol - T1095 Exploit Public-Facing Application - T1190	tlp:green ecsirt:malicious-code="malware"	14			2021-08-13	IoT Malware:	All	
✔	Treinamento-CERT.br	42549	Attack Pattern Non-Application Layer Protocol - T1095 Exploit Public-Facing Application - T1190	tlp:green ecsirt:malicious-code="malware"	14			2021-08-12	IoT Malware:	All	
✔	Treinamento-CERT.br	42548	Attack Pattern Non-Application Layer Protocol - T1095 Exploit Public-Facing Application - T1190	tlp:green ecsirt:malicious-code="malware"	14			2021-08-12	IoT Malware:	All	
✔	Treinamento-CERT.br	42547	Attack Pattern Acquire and/or use 3rd party infrastructure services - T1307	tlp:green	108		81	2021-08-12	Rogue DNS:	All	

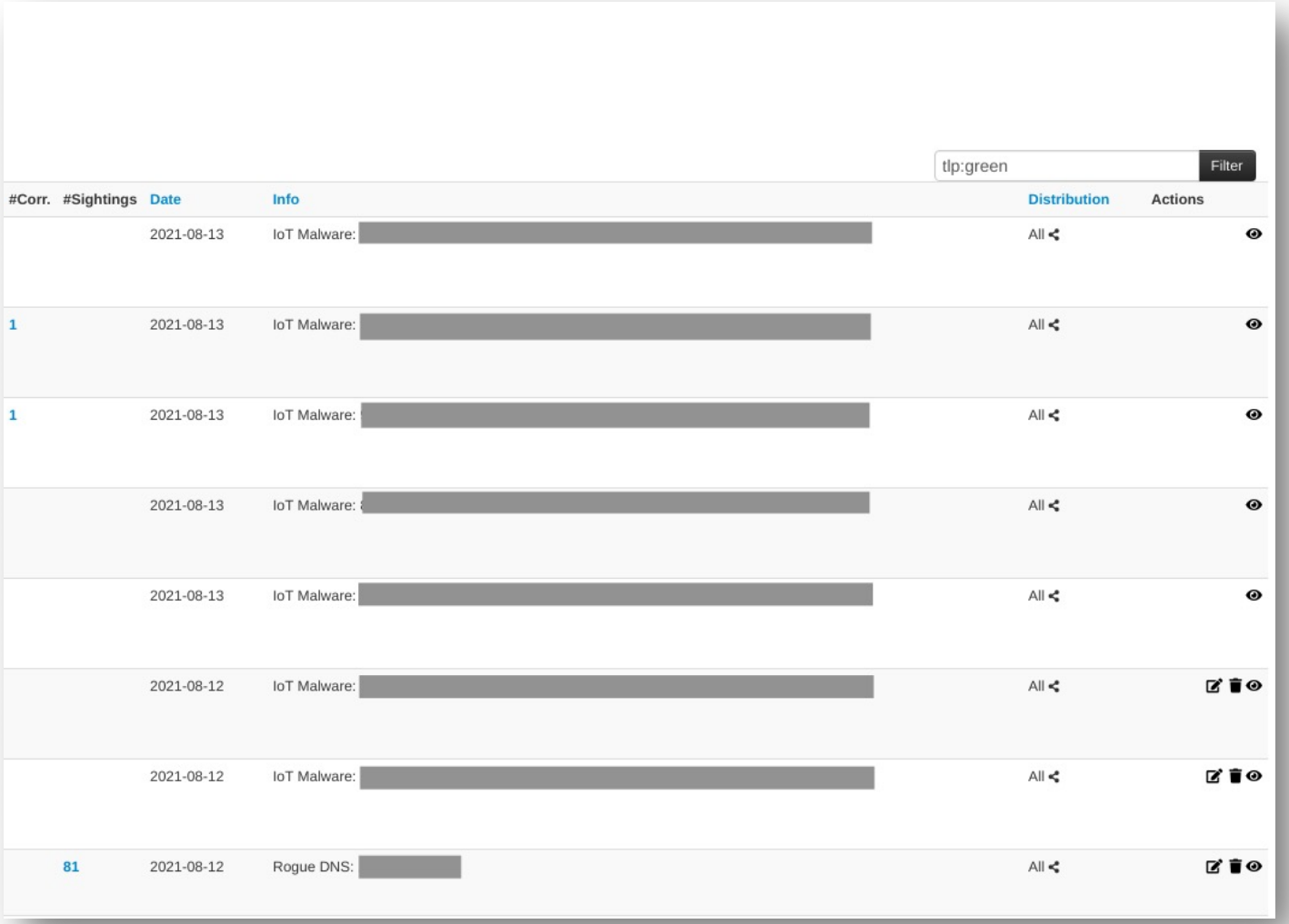
Eventos



- **`Published:`** *status* do evento (publicado ou não)
- **`Creator org:`** organização que criou o evento
- **`ID:`** número sequencial atribuído pelo MISP a cada evento criado ou sincronizado
- **`Clusters:`** também chamados de "**`Galaxies`**", são um método para associar estruturas mais complexas a eventos ou atributos; as galáxias são pré-definidas e expressam informações de inteligência para serem interpretadas por analistas
- **`Tags:`** usadas para classificar eventos ou atributos, em geral de acordo com uma Taxonomia pré-definida, permitindo criar *links* entre eventos ou filtros, facilitando automação
- **`#Attr:`** número de atributos de um evento

Eventos

- **`#Corr:`** número de correlações de um evento
- **`#Sightings:`** permitem que um usuário interaja com os eventos, indicando que viu um atributo como uma URL de *phishing* ou um IP em seus *logs*
- **`Date:`** data de criação do evento
- **`Info:`** uma breve descrição do evento
- **`Distribution:`** forma de distribuição/compartilhamento do evento
- **`Actions:`** o que o usuário pode fazer com o evento, neste exemplo, editar, apagar e visualizar



Atributos

Uma dúvida recorrente na criação de eventos é quando utilizar atributos e objetos

Atributos são utilizados quando apenas uma informação simples é adicionada a um evento

Um atributo pode ser um endereço IP, uma URL, um endereço de e-mail, um nome de arquivo

É necessário escolher bem o tipo de atributo, por exemplo ip-src ou ip-dst

Uma lista completa dos atributos do MISP pode ser consultada em:
https://www.misp-project.org/datamodels/#attribute-categories-vs-types

Objetos

Objetos são utilizados para agrupar atributos

Quando a informação é composta por mais de um elemento, como por exemplo endereço IP e porta, ou um nome de um arquivo e um hash, a utilização de objetos é fortemente recomendada

O uso de um objeto não obriga a utilização de todos os seus atributos. É possível utilizar apenas alguns atributos de um objeto. Alguns objetos podem ter atributos que são obrigatórios

A lista de todos os objetos do MISP pode ser consultada em:

https://www.misp-project.org/objects.html

Sincronização entre Instâncias/Servidores MISP

Termo utilizado pelo MISP para a troca de informações entre duas ou mais instâncias MISP:

- requer a criação de usuários "**`Sync User`**" e respectivas **`authkeys`**
- pode ser feita através de um dos seguintes mecanismos:

`push`
- uma instância **A** **envia** os eventos para uma instância **B**
- distribuição de um evento ocorre de forma automática após sua publicação

`pull`
- uma instância **B** **busca** eventos em uma instância **A**
- precisa de uma intervenção do administrador via interface *web* ou então de um *script* rodando no **`cron`**

TLP:CLEAR

Sincronização: `Push` vs. `Pull`

	Push	Pull
Direção	**A** envia eventos para **B**	**B** busca eventos em **A**
Propagação de eventos	Automática No momento da publicação do evento	Manual Via interface do MISP ou via **`cron`**
Dados para configuração de sincronia	**A** manda para **B**: – **`UUID`** e **`ORGNAME`** **B** manda para **A**: – **`URL`**, **`Authkey`**, **`UUID`** e **`ORGNAME`**	**B** manda para **A**: – **`UUID`** e **`ORGNAME`** **A** manda para **B**: – **`URL`**, **`Authkey`**, **`UUID`** e **`ORGNAME`**
Criação de contas e servidores para sincronia	**B** cria: - Org. local com os dados de **A** – **`Sync-user`** para **A** na Org. local criada **A** cria: - Servidor de sincronia, com a opção **`push`** marcada, com os dados de **B**	**B** cria: - Servidor de sincronia, com a opção **`pull`** marcada, com os dados de **A** **A** cria: - Org. local com os dados de **B** – **`Sync-user`** com "**`Authkey read only`**" para **B** na Org. local criada
Configuração de Rede	**B** precisa permitir conexões vindas de **A** na porta 443/TCP	**A** precisa permitir conexões vindas de **B** na porta 443/TCP

Considerações sobre `Push`

Na sincronização via **`push`**, uma instância **A** **envia** os eventos para uma instância **B**

- Problemas de conexão ou problemas com os **`workers`** podem impedir eventos de serem sincronizados via **`push`**
- Eventos gerados como "**`Your organization only`**" não serão sincronizados via **`push`**
- Eventos gerados como "**`This community only`**" só serão sincronizados via **`push`** se a organização pertencente à sua comunidade for uma organização local

Considerações sobre `Pull`

Na sincronização via **`pull`**, uma instância **B** **busca** eventos na instância **A**

- A sincronia via **`pull`** não acontece de forma automática, precisa de uma intervenção do administrador via interface *web* ou então de um *script* rodando no **`cron`**
- Na sincronia via **`pull`**, eventos compartilhados como "**`this community only`**" e "**`your organization only`**" podem ser baixados para uma instância remota se o usuário utilizado para a sincronia pertencer à mesma organização que criou os eventos
- Até a versão 2.4.147 do MISP não era possível impedir que uma instância buscando eventos via **`pull`** alterasse as configurações do servidor de sincronia e enviasse eventos de volta via **`push`**
- Na versão 2.4.147 o MISP introduziu uma opção de "**`Read only`**" na **`authkey`** do usuário, permitindo que ele faça apenas a leitura dos eventos de uma instância e não consiga fazer **`push`** de eventos

Formas de distribuição de eventos

Define como cada organização, mesmo local, enxergará os eventos e como serão compartilhados.

Os eventos podem ser distribuídos da seguinte forma:

- **`Your organisation only`**
  - Apenas usuários da sua organização recebem os eventos

    IMPORTANTE: se não souber como será o compartilhamento, crie como "**`Your organisation only`**"

    Não é possível controlar/forçar a remoção de um evento propagado indevidamente
- **`This community only`**
  - Usuários de outras organizações no seu servidor MISP recebem os eventos
- **`Connected communities`**
  - Usuários de organizações de servidores MISP conectados diretamente ao seu servidor MISP recebem os eventos
- **`All communities`**
  - Usuários de todas as comunidades recebem os eventos, que são propagados livremente de um servidor MISP para outro
- **`Sharing group`**
  - Apenas organizações selecionadas em servidores selecionados recebem os eventos

Considerações sobre TLP

– A tag TLP **NÃO** é levada em consideração na distribuição dos eventos

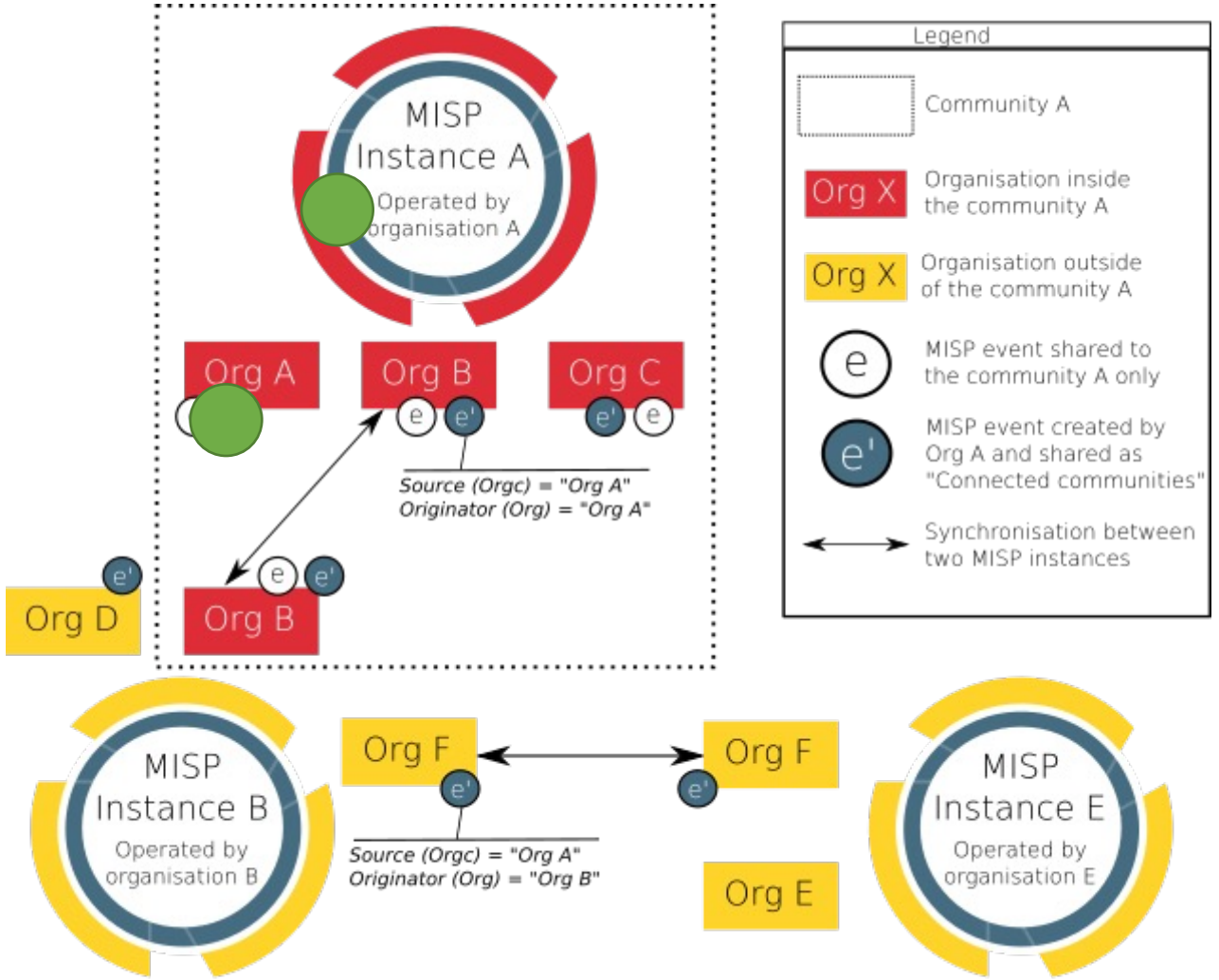
– O MISP **NÃO** filtra **AUTOMATICAMENTE** os eventos com base na tag TLP

– É possível criar filtros para distribuição de eventos via PUSH baseados em TLP

– Também é possível criar filtros quando os eventos são buscados via PULL, mas este filtro é criado por quem busca a informação e não pelo detentor da informação

Tipo de distribuição:
`Your organisation only`

TLP:CLEAR

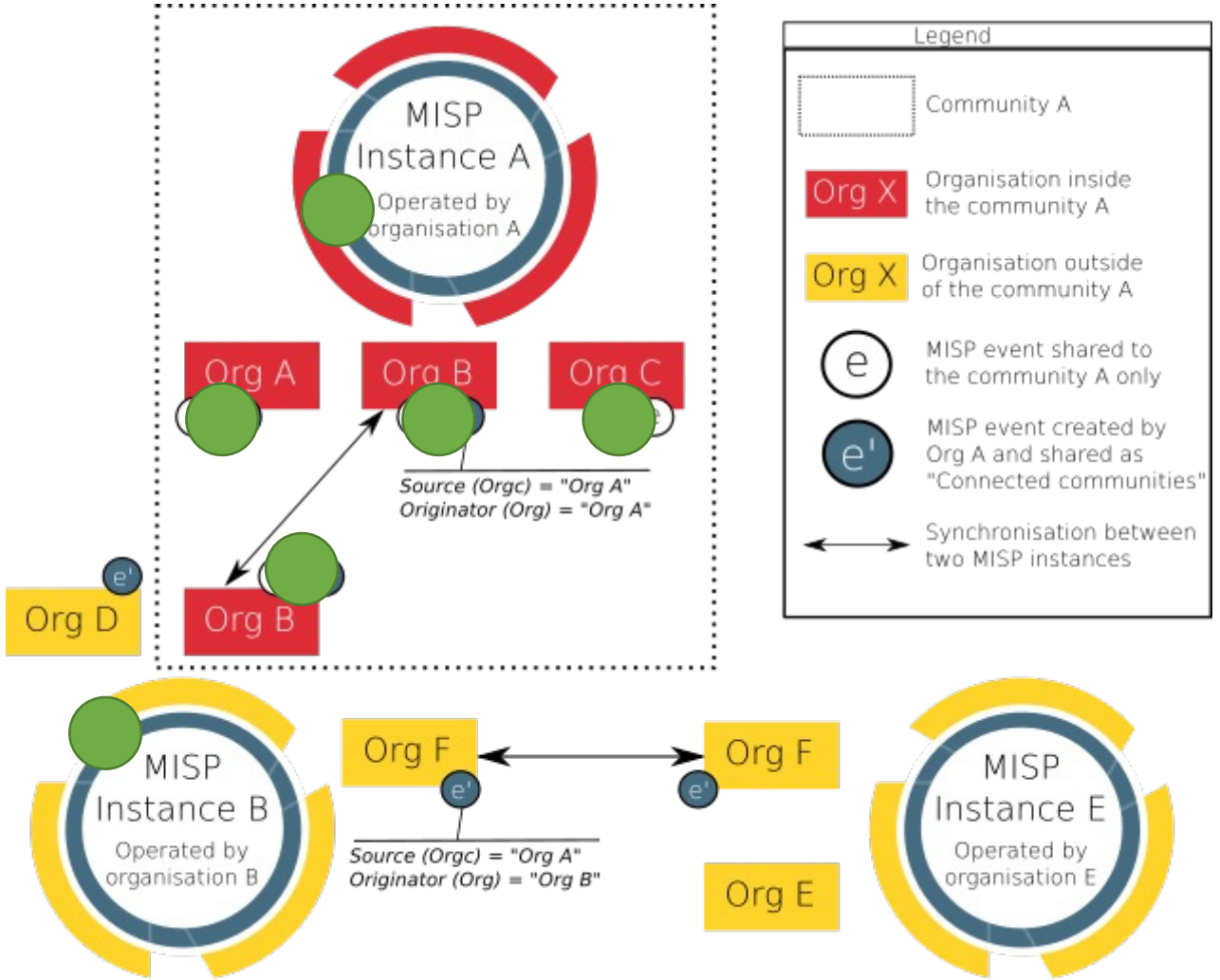


Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

Adaptado de: https://www.circl.lu/doc/misp/sharing/#community

Tipo de distribuição:
`This community only`

TLP:CLEAR

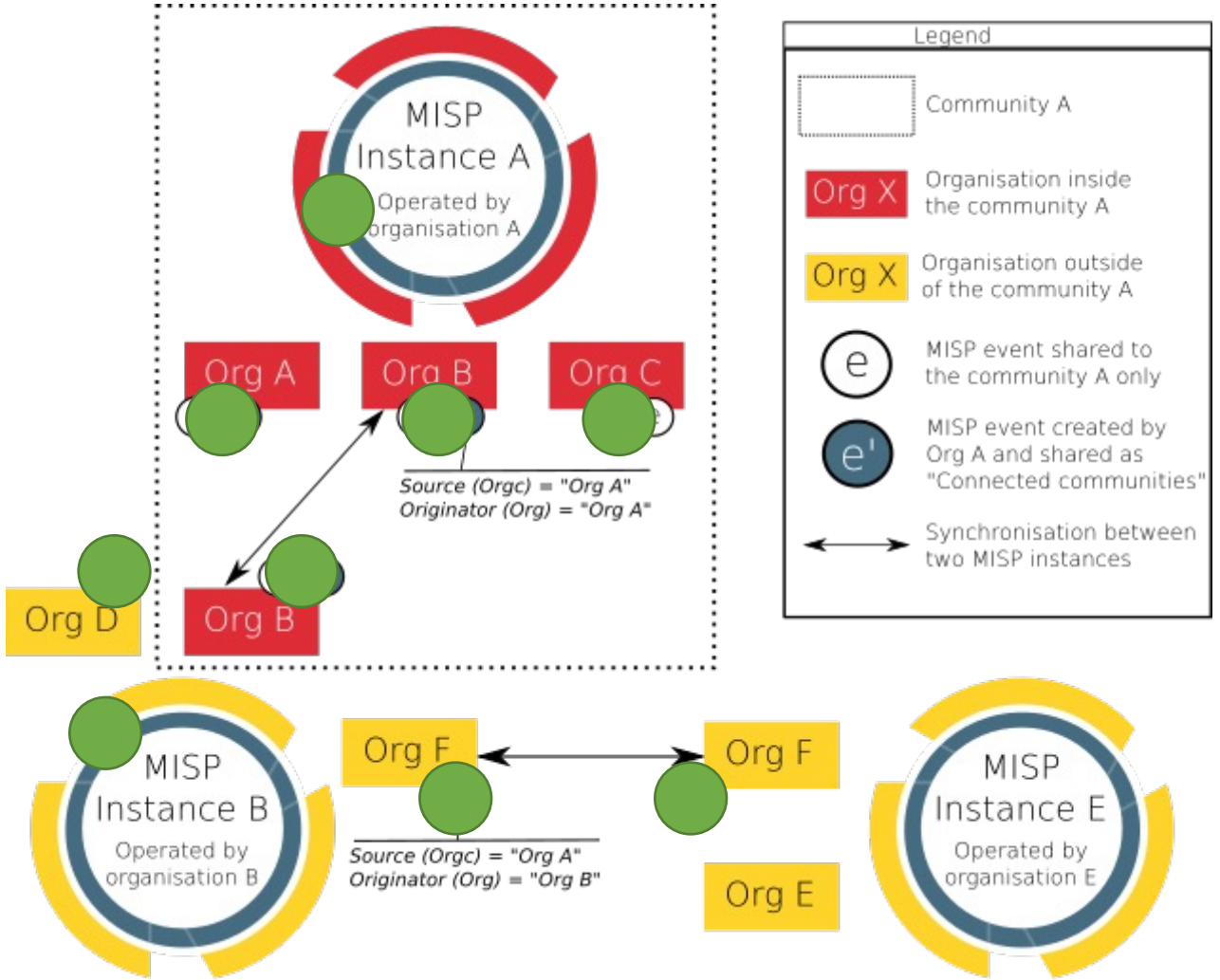


Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

Adaptado de: https://www.circl.lu/doc/misp/sharing/#community

Tipo de distribuição:
Connected communities

TLP:CLEAR

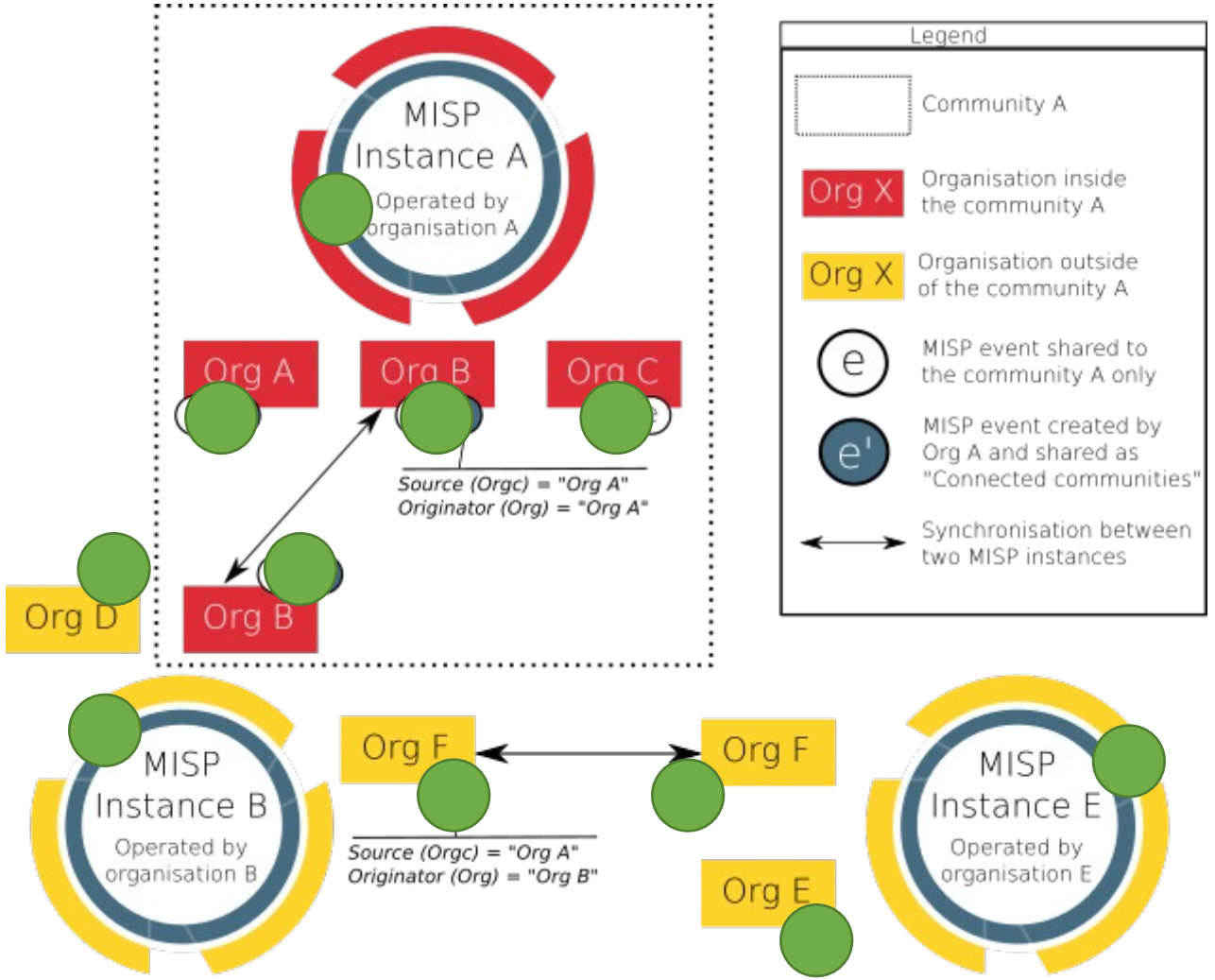


Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

Adaptado de: https://www.circl.lu/doc/misp/sharing/#community

Tipo de distribuição:
`All communities`

TLP:CLEAR



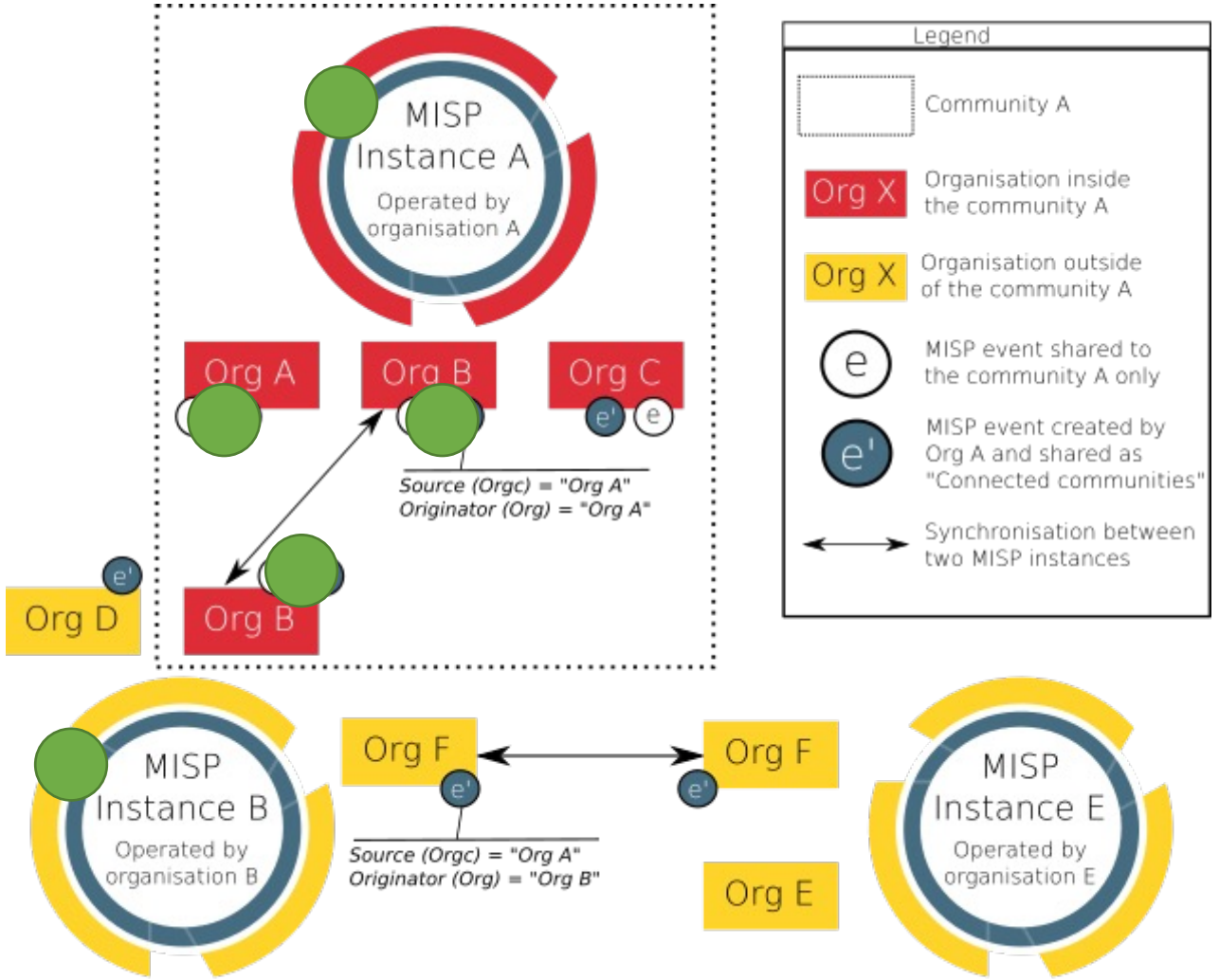
Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

Adaptado de: https://www.circl.lu/doc/misp/sharing/#community

Tipo de distribuição: **Sharing group**

TLP:CLEAR

Sharing group contendo apenas as organizações A e B



Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

Adaptado de: https://www.circl.lu/doc/misp/sharing/#community

Alguns Erros em Instâncias Reais

cert.br nic.br cgi.br

Caso 1 – excesso de correlações

- Participante **FOO** pede para enviar eventos para a instância do CERT.br
- Recebemos 67 eventos do participante **FOO**
- Após recebimento desses eventos, notamos a navegação na interface web da nossa instância bem mais lenta
- Ao verificar as estatísticas do MISP, notamos que:
  - Tínhamos um total de **27.132.386** correlações
  - Sendo **27.031.540** dos 67 eventos do participante **FOO**
  - No banco de dados, nossa tabela de correlações saltou de **31MB** para **7GB**

- Alertamos o participante sobre essas correlações
- Impossível apagar eventos via interface web (*timeout*)
- Eventos foram apagados diretamente no banco de dados
  - Cerca de 1h para apagar cada evento

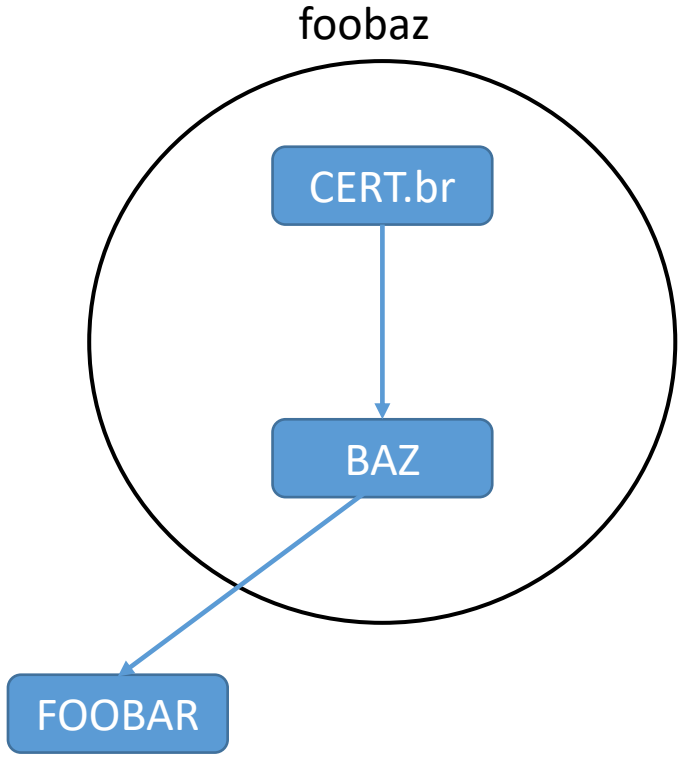
```
MariaDB [misp]> DELETE FROM correlations WHERE event_id =
'606' OR 1_event_id = '606';
Query OK, 1433760 rows affected (1 hour 16 min 11.645
sec)
```

Caso 2 – Eventos sendo distribuídos fora do *sharing group*

– Participante **BAZ** começa a receber nossos eventos, incluindo eventos restritos ao *sharing group* **foobaz**

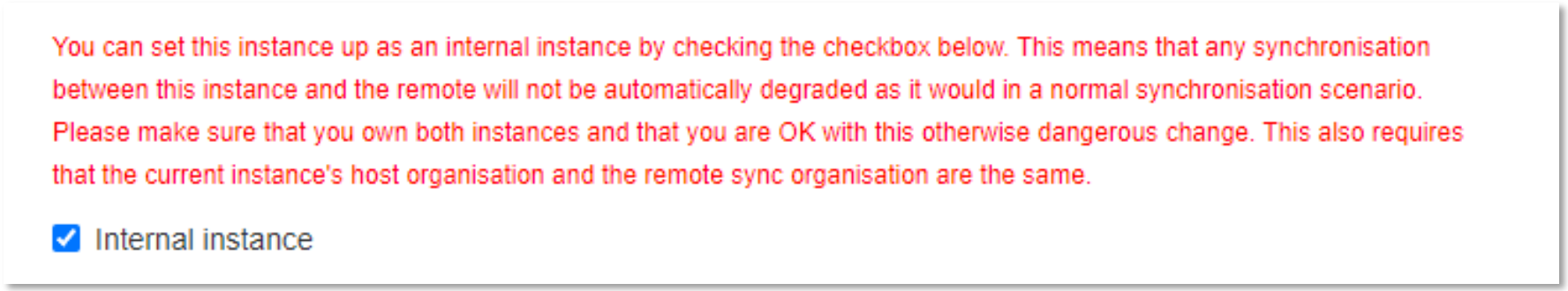
– Dias depois, ao ajudar a organização **FOOBAR** a depurar um problema, notamos que ela estava recebendo eventos do *sharing group* **foobaz** via organização **BAZ** como "*Owner Org*"

– A organização **FOOBAR** não faz parte desse *sharing group* e **não deveria** receber esse tipo de evento



Caso 2 – Eventos sendo distribuídos fora do *sharing group*

– Em contato com a organização **BAZ**, apuramos que:
  – Organização **BAZ** e organização **FOOBAR** começam a trocar eventos entre si
  – Ao criar o servidor de sincronia para a organização FOOBAR, a organização **BAZ** marcou por engano a opção "*Internal instance*", tornando o servidor da organização **FOOBAR** uma extensão da organização **BAZ**



Esse tipo de configuração estava enviando para a organização **FOOBAR TODOS** os eventos da organização **BAZ**, incluindo eventos do tipo "***Your organisation Only***"

Caso 3 – Certificados quase expirando

– Participantes deixam para renovar certificados ACME na mão no último dia:

Days_left: 0!!!!


```
{
  "url": "https://misp.example.org",
  "tls_version": "TLSv1.2",
  "tls_cipher": "ECDHE-RSA-AES256-GCM-SHA384",
  "alpn": "http/1.1",
  "ocsp": false,
  "certificate_chain": [
    {
      "subject": "CN=misp.example.org",
      "issuer": "CN=R3,O=Let's Encrypt,C=US",
      "san": "misp.example.org",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 0
    },
    {
      "subject": "CN=R3,O=Let's Encrypt,C=US",
      "issuer": "CN=ISRG Root X1,O=Internet Security Research Group,C=US",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 1427
    },
    {
      "subject": "CN=ISRG Root X1,O=Internet Security Research Group,C=US",
      "issuer": "CN=DST Root CA X3,O=Digital Signature Trust Co.",
      "key": "RSA 4096 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 1077
    }
  ],
  "status": "certificate expiring soon"
}
```

Caso 4 – Participantes com certificado expirado

24 dias com certificado expirado →


```
{
  "url": "https://misp.example.org",
  "tls_version": "TLSv1.2",
  "tls_cipher": "ECDHE-RSA-AES256-GCM-SHA384",
  "alpn": "http/1.1",
  "ocsp": false,
  "certificate_chain": [
    {
      "subject": "CN=misp.example.org",
      "issuer": "CN=R3,O=Let's Encrypt,C=US",
      "san": "misp.example.org",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": -24
    },
    {
      "subject": "CN=R3,O=Let's Encrypt,C=US",
      "issuer": "CN=ISRG Root X1,O=Internet Security Research Group,C=US",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 1403
    },
    {
      "subject": "CN=ISRG Root X1,O=Internet Security Research Group,C=US",
      "issuer": "CN=DST Root CA X3,O=Digital Signature Trust Co.",
      "key": "RSA 4096 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 1053
    }
  ],
  "status": "certificate has expired"
}
```

Caso 5 – Chain incorreta


```
{
  "url": "https://misp.example.org/",
  "tls_version": "TLSv1.2",
  "tls_cipher": "ECDHE-RSA-AES256-GCM-SHA384",
  "alpn": "http/1.1",
  "ocsp": false,
  "certificate_chain": [
    {
      "subject": "CN=misp.example.org",
      "issuer": "CN=GlobalSign GCC R3 DV TLS CA 2020,O=GlobalSign nv-sa,C=BE",
      "san": "misp.example.org",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 335
    },
    {
      "subject": "CN=GlobalSign,O=GlobalSign,OU=GlobalSign Root CA - R3",
      "issuer": "CN=GlobalSign,O=GlobalSign,OU=GlobalSign Root CA - R3",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 2505
    }
  ],
  "status": "unable to get local issuer certificate"
}
```

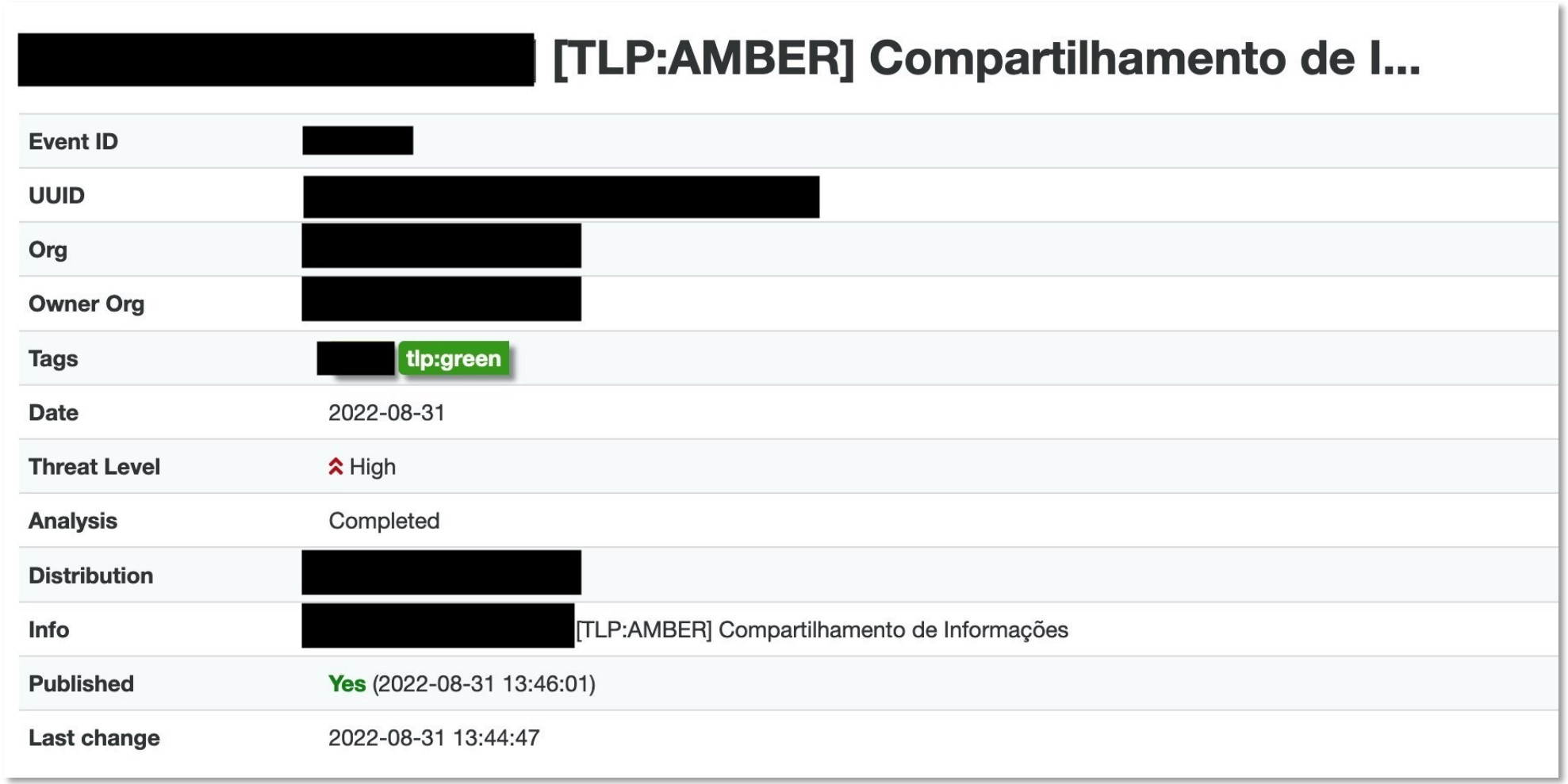
Caso 5 – Chain após correção


```
{
  "url": "https://misp.example.org/",
  "tls_version": "TLSv1.2",
  "tls_cipher": "ECDHE-RSA-AES256-GCM-SHA384",
  "alpn": "http/1.1",
  "ocsp": false,
  "certificate_chain": [
    {
      "subject": "CN=misp.example.org",
      "issuer": "CN=GlobalSign GCC R3 DV TLS CA 2020,O=GlobalSign nv-sa,C=BE",
      "san": "misp.example.org",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 260
    },
    {
      "subject": "CN=GlobalSign GCC R3 DV TLS CA 2020,O=GlobalSign nv-sa,C=BE",
      "issuer": "CN=GlobalSign,O=GlobalSign,OU=GlobalSign Root CA - R3",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 2430
    }
  ],
  "status": "valid"
}
```

Caso 6 – Chain incompleta


```
{
  "url": "https://misp.example.org/",
  "tls_version": "TLSv1.2",
  "tls_cipher": "ECDHE-RSA-AES128-GCM-SHA256",
  "alpn": "",
  "ocsp": false,
  "certificate_chain": [
    {
      "subject": "CN=*.misp.example.org,O=MISP,ST=SP,C=BR",
      "issuer": "CN=Sectigo RSA Organization Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB",
      "san": "*.misp.example.org",
      "key": "RSA 2048 bits",
      "sig_algo": "SHA256withRSA",
      "days_left": 297
    }
  ],
  "status": "unable to get local issuer certificate"
}
```

Caso 7 – Evento criado com TLP conflitante



[redacted] [TLP:AMBER] Compartilhamento de I...

Event ID	[redacted]
UUID	[redacted]
Org	[redacted]
Owner Org	[redacted]
Tags	[redacted] tlp:green
Date	2022-08-31
Threat Level	High
Analysis	Completed
Distribution	[redacted]
Info	[redacted] [TLP:AMBER] Compartilhamento de Informações
Published	Yes (2022-08-31 13:46:01)
Last change	2022-08-31 13:44:47

Caso 8 – Provedor solicitando verificação com JavaScript

```
misp.example.org

Checking if the site connection is secure

Enable JavaScript and cookies to continue
misp.example.org needs to review the security of your connection before proceeding.
Ray ID: 74782dfb5901a513
Performance & security by Cloudflare
```

Hands-on

cert.br nic.br cgi.br

Caso 1 – Phishing

[2022-07-26T10:35:42Z]

– Funcionário da empresa reporta ao CSIRT e-mail de *phishing* para o webmail da empresa com o link: `https://webmail.evildomain.example.org/index.html`

[2022-07-26T10:45:15Z]

– Funcionário do CSIRT verifica que o *phishing* está online

[2022-07-26T10:47:35Z]

– Página de *phishing* aponta para o IP `198.51.100.10`, que está alocado para o ASN `64514`

Caso 2 – Artefato suspeito

[2022-07-30T09:56:08Z]

– CSIRT vai investigar uma câmera de segurança que está fazendo conexões para o IP `2001:db8:cafe:1001::1020` na porta `1312/TCP`

[2022-07-30T10:12:12Z]

– CSIRT encontra o binário `phantom.mips` rodando na câmera

[2022-07-30T10:25:54Z]

– CSIRT analisa logs de rede e determina que este arquivo foi baixado em `2022-07-29T19:35:12Z` da URL `http://evilhost.example.org/bins/phantom.mips`, que resolve para o IP `192.0.2.200`.

Caso 3 – Lista de IPs

[2022-07-30T12:17:30Z]

– CSIRT recebe uma lista de IPs de CnC de uma botnet utilizada para realização de ataques de negação de serviço.

```
198.51.100.11
198.51.100.15
198.51.100.18
[...]
```

<ver arquivo `ips.txt`>

Caso 4 – Log de rede

[2022-07-30T10:55:05Z]

– CSIRT recebe os seguintes logs do firewall da organização:

```
2022-08-25T19:14:03Z 198.51.100.86.20096  > 203.0.113.80.3389: S
2022-08-25T19:14:05Z 198.51.100.92.10257  > 203.0.113.80.3389: S
2022-08-25T19:14:09Z 198.51.100.127.45678 > 203.0.113.80.3389: S
```

<logs disponíveis no arquivo `log.txt`>

Q&A

cert.br nic.br cgi.br

Obrigado

marcus@cert.br
mhp@cert.br
jessen@cert.br

Notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br