# MISP: Passo-a-Passo para Configuração e Utilização

19 de agosto de 2021

CERT.br
misp@cert.br

cert.br nic.br cgi.br

# Antes de Começar:
# **Considerações de Segurança**

TLP:WHITE

**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)

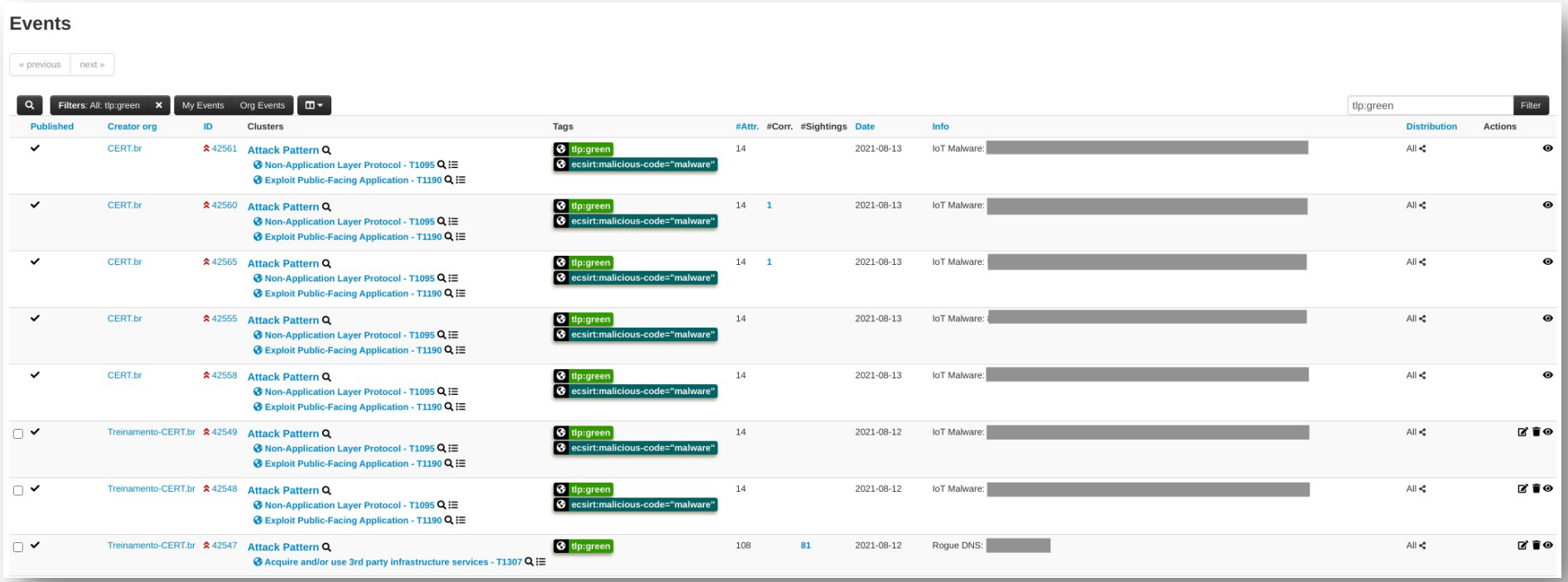
# Parte 1
# Utilizar uma Instância MISP

cert.br nic.br cgi.br

TLP:WHITE

# Parte 1:
# Utilizar uma Instância MISP

- Conhecer a arquitetura do MISP
- Usar uma instância própria ou de terceiros
- Entender o conceito de várias organizações
- Familiarizar-se com eventos e seus atributos
  - compartilhamento
  - visibilidade
    - **`sharing groups`**
    - **`communities`**



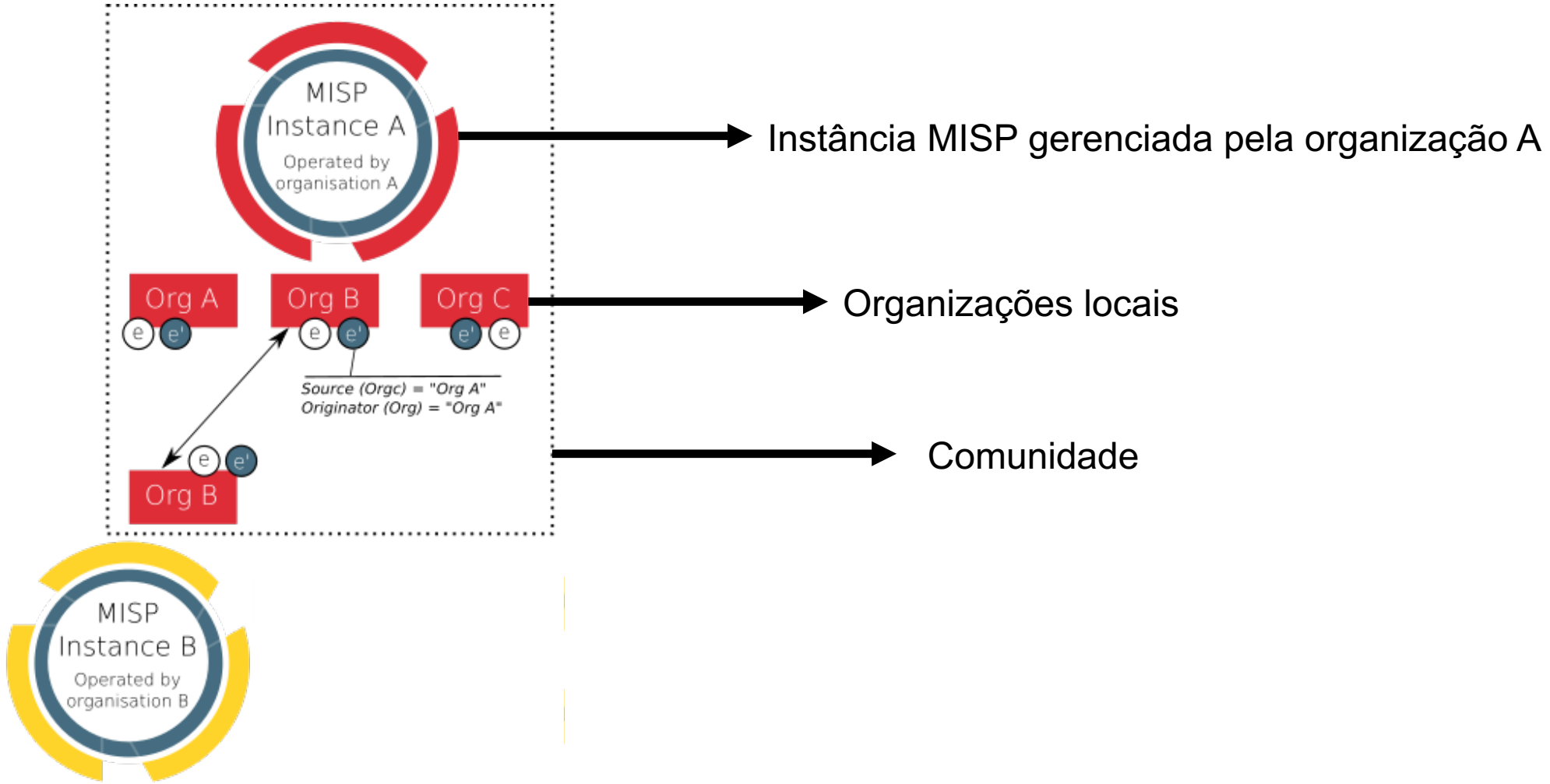
# Arquitetura do MISP
## Como interagir com uma instância

TLP:WHITE


Fonte: https://www.circl.lu/services/misp-malware-information-sharing-platform/

# Arquitetura do MISP
## **Instância, organizações e comunidade**

TLP:WHITE




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

TLP:WHITE

# Eventos

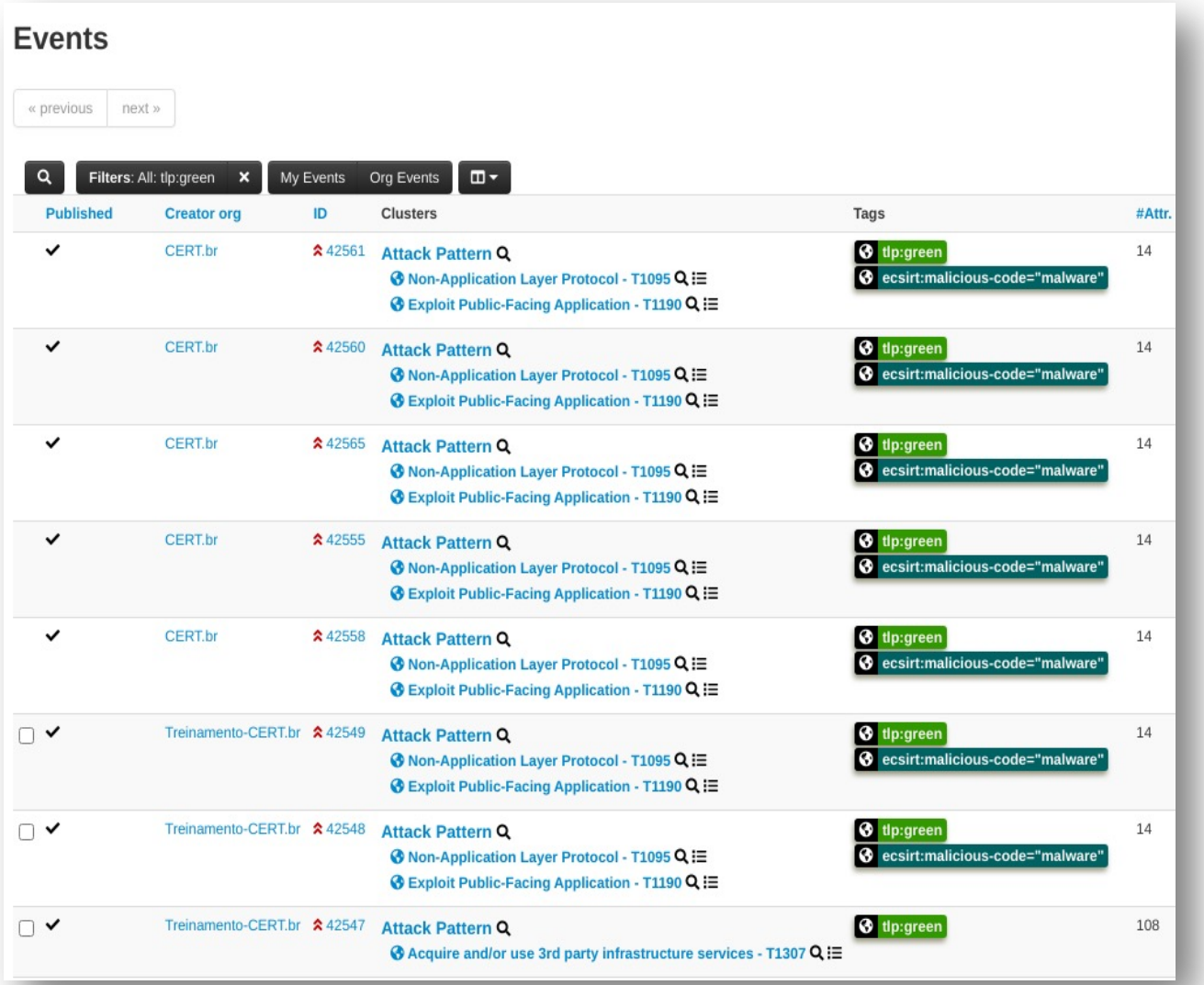
## Events

« 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<br>Non-Application Layer Protocol - T1095<br>Exploit Public-Facing Application - T1190 | tlp:green<br>ecsirt:malicious-code="malware" | 14 | | | 2021-08-13 | IoT Malware: | All | |
| ✔ | CERT.br | 42560 | Attack Pattern<br>Non-Application Layer Protocol - T1095<br>Exploit Public-Facing Application - T1190 | tlp:green<br>ecsirt:malicious-code="malware" | 14 | 1 | | 2021-08-13 | IoT Malware: | All | |
| ✔ | CERT.br | 42565 | Attack Pattern<br>Non-Application Layer Protocol - T1095<br>Exploit Public-Facing Application - T1190 | tlp:green<br>ecsirt:malicious-code="malware" | 14 | 1 | | 2021-08-13 | IoT Malware: | All | |
| ✔ | CERT.br | 42555 | Attack Pattern<br>Non-Application Layer Protocol - T1095<br>Exploit Public-Facing Application - T1190 | tlp:green<br>ecsirt:malicious-code="malware" | 14 | | | 2021-08-13 | IoT Malware: | All | |
| ✔ | CERT.br | 42558 | Attack Pattern<br>Non-Application Layer Protocol - T1095<br>Exploit Public-Facing Application - T1190 | tlp:green<br>ecsirt:malicious-code="malware" | 14 | | | 2021-08-13 | IoT Malware: | All | |
| ✔ | Treinamento-CERT.br | 42549 | Attack Pattern<br>Non-Application Layer Protocol - T1095<br>Exploit Public-Facing Application - T1190 | tlp:green<br>ecsirt:malicious-code="malware" | 14 | | | 2021-08-12 | IoT Malware: | All | |
| ✔ | Treinamento-CERT.br | 42548 | Attack Pattern<br>Non-Application Layer Protocol - T1095<br>Exploit Public-Facing Application - T1190 | tlp:green<br>ecsirt:malicious-code="malware" | 14 | | | 2021-08-12 | IoT Malware: | All | |
| ✔ | Treinamento-CERT.br | 42547 | Attack Pattern<br>Acquire and/or use 3rd party infrastructure services - T1307 | tlp:green | 108 | | 81 | 2021-08-12 | Rogue DNS: | All | |

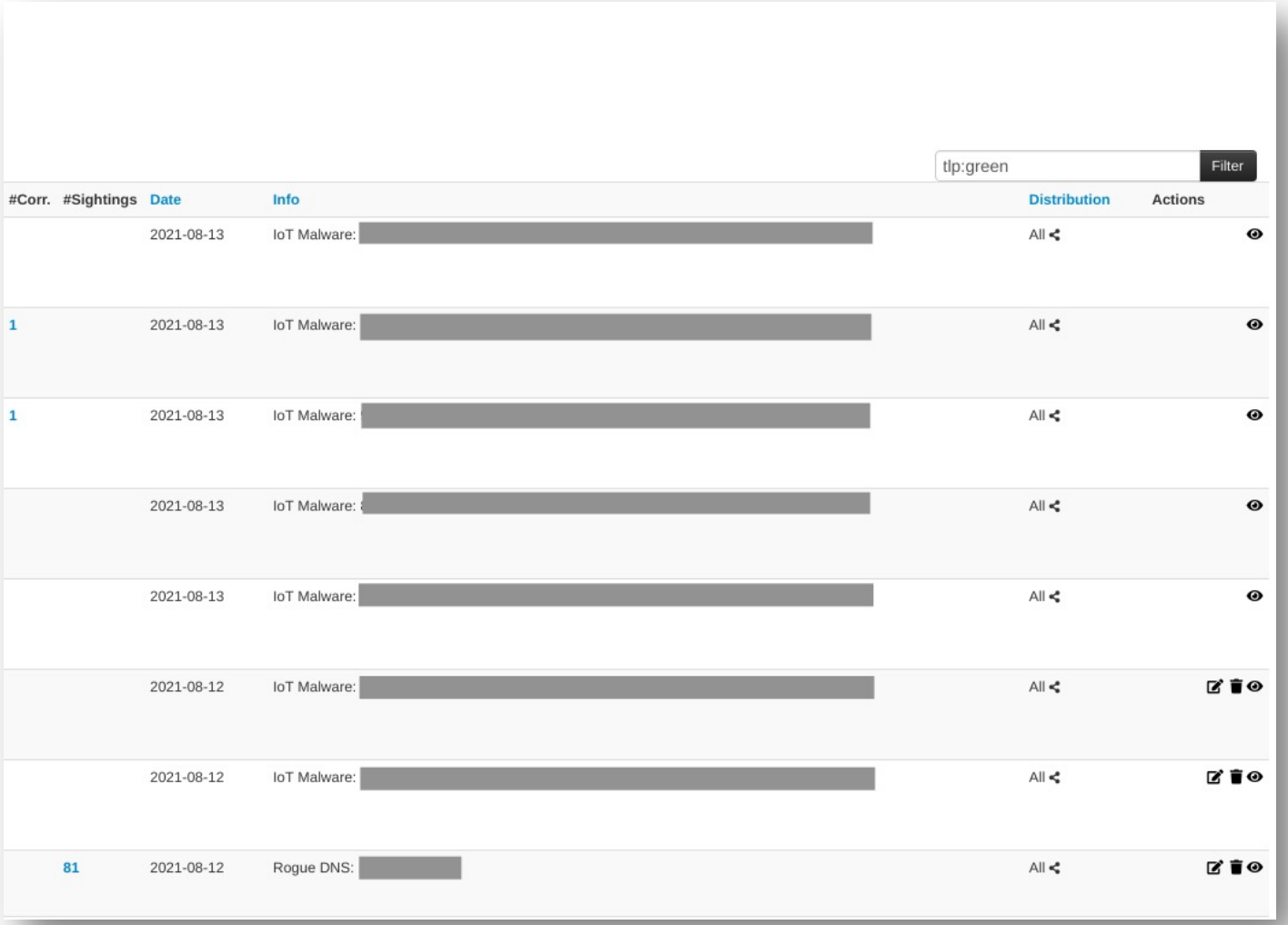
# Eventos




- **`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



TLP:WHITE

# Define a forma 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

# Parte 2
# Utilizar e Administrar a sua Instância MISP

cert.br nic.br cgi.br

# Parte 2:
# Utilizar e Administrar a sua Instância MISP

- Administrar uma instância
  - Alterar a senha
  - Criar usuários e organizações
- Sincronizar instâncias
  - **`Push`**
  - **`Pull`**
- Distribuir eventos
- Atualizar o MISP
- Automatizar consulta de eventos
  - API Rest do MISP


Fonte: https://www.circl.lu/services/misp-malware-information-sharing-platform/

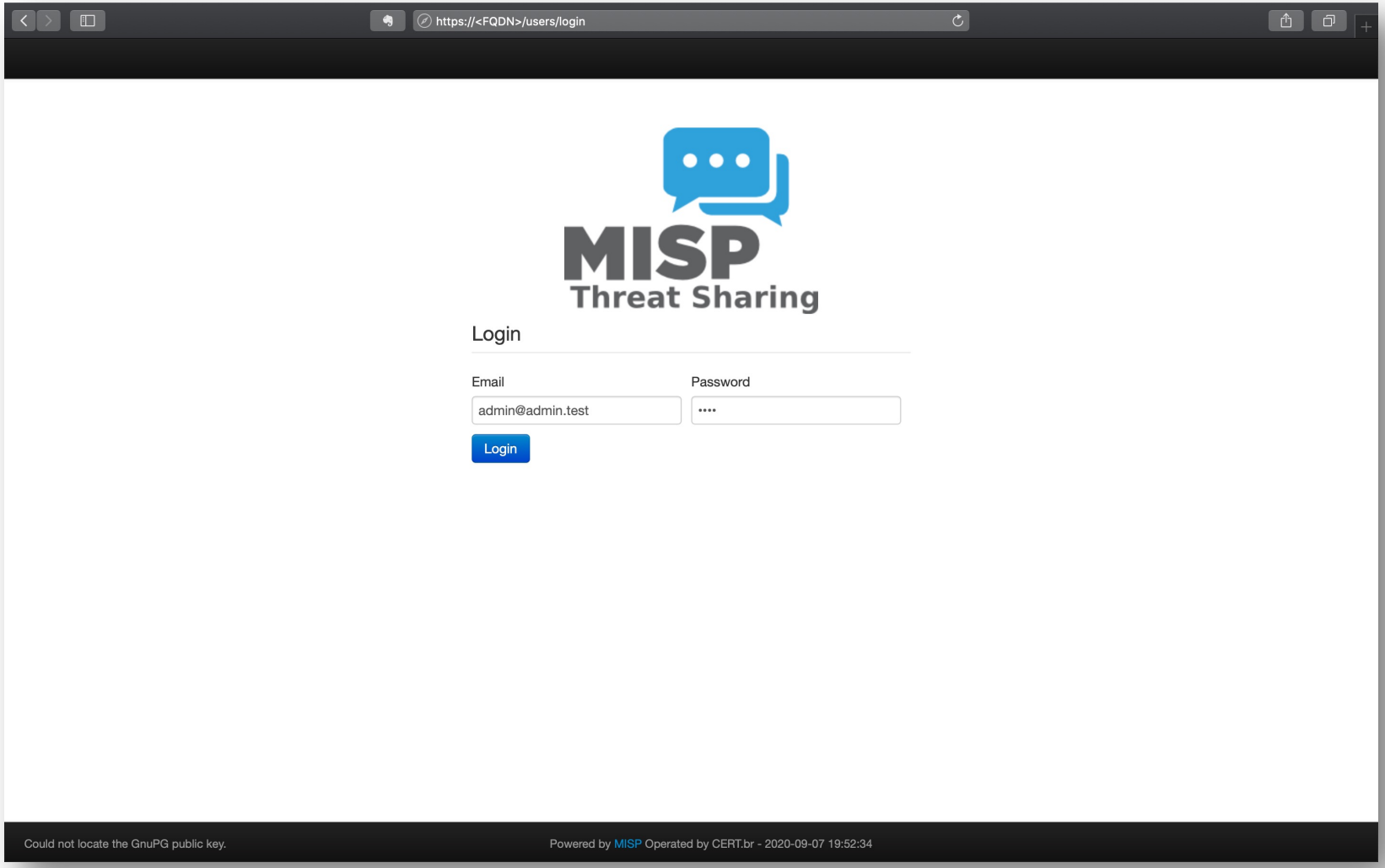
# Primeiro *login (1/2)*

Acesse o servidor MISP pela URL:

`https://<FQDN>`

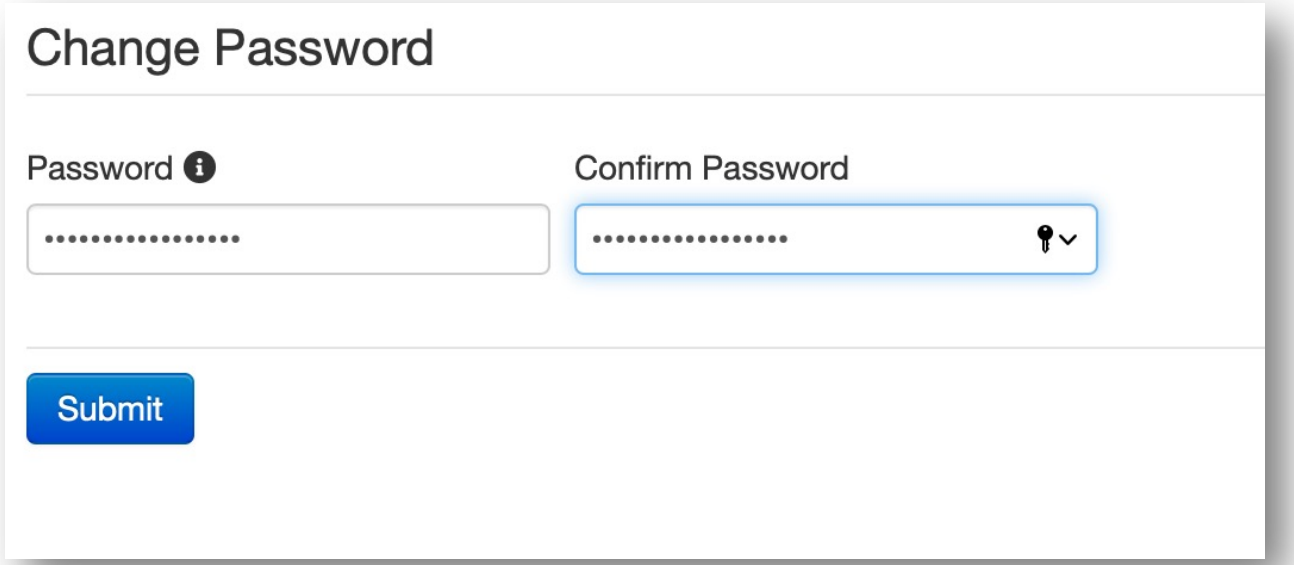
Faça o *login* com os dados:

- Email: **`admin@admin.test`**
- Password: **`admin`**



# Primeiro *login (2/2)*

O MISP exige a alteração da senha do usuário **`admin`** após o primeiro *login*




O MISP obriga a utilização de uma senha forte.

Guarde esta senha em um local seguro.

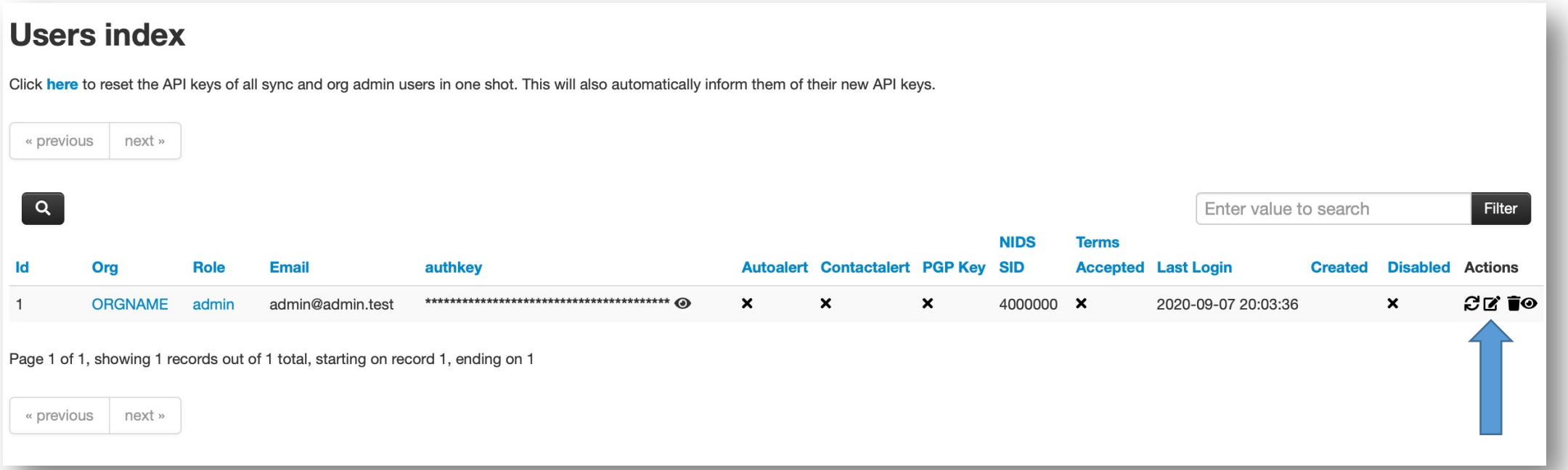
# Alteração do *e-mail* do usuário `admin` (1/2)

É recomendado alterar o *e-mail* do usuário **`admin@admin.test`**

Para isso:

– clique em "**`Administration – List Users`**"

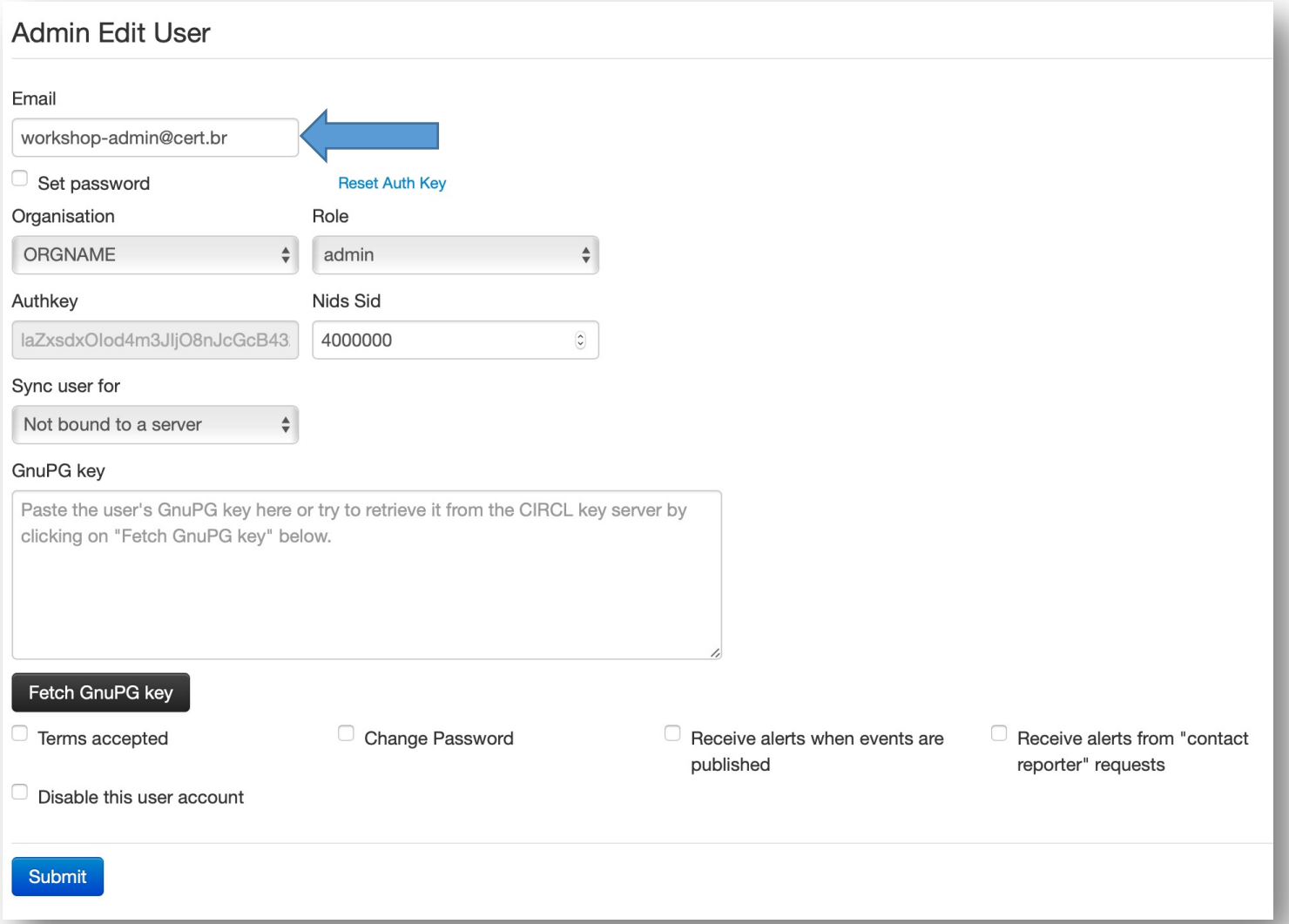
– na página "**`Users index`**" localize o usuário **`admin@admin.test`** e clique no ícone editar



# Alteração do *e-mail* do usuário admin (2/2)

Na janela "**`Admin Edit User`**" altere o *e-mail* do usuário **`admin`**

Após alterar o *e-mail*, clique em **`Submit`**



# IMPORTANTE:

TLP:WHITE

## Configuração da Organização que Gerencia a Instância

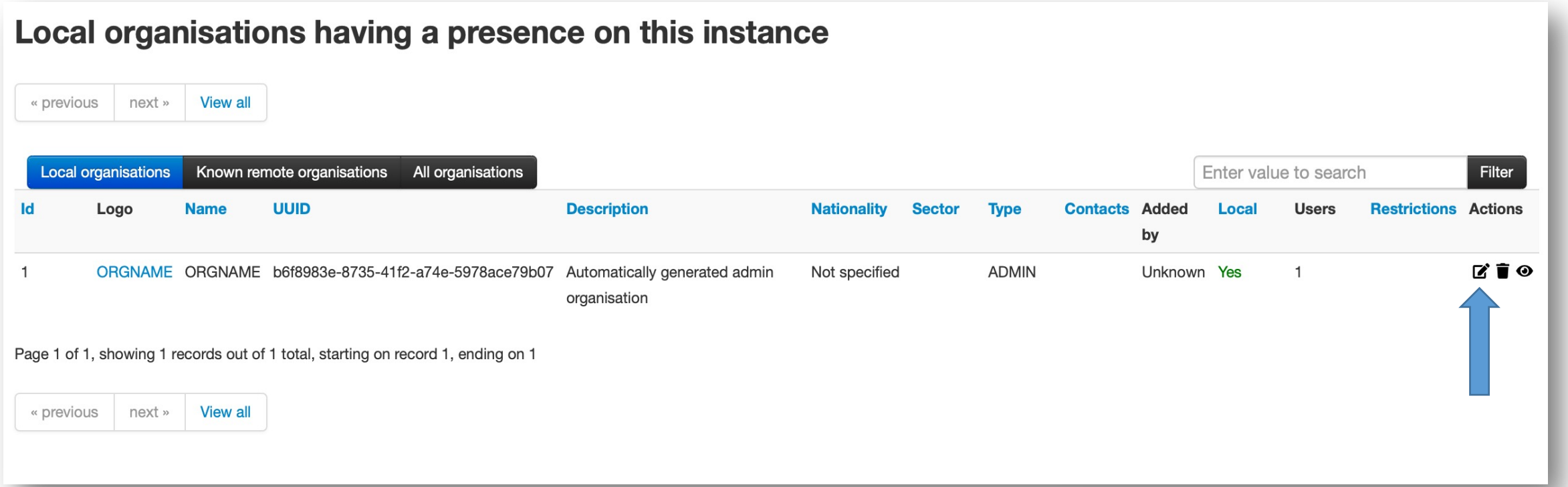
- Organização com “**`Id 1`**”
  - é a organização principal da instância (**`host organisation`**)
  - é convenção que tenha o “**`Id 1`**”

- O **`UUID`** da “**`host organisation`**”
  - identifica sua organização
  - vai ser enviado para outras instâncias
  - se for conhecida por outros, precisa ser utilizada novamente em caso de reinstalação
    - anote esse **`UUID`** em local seguro

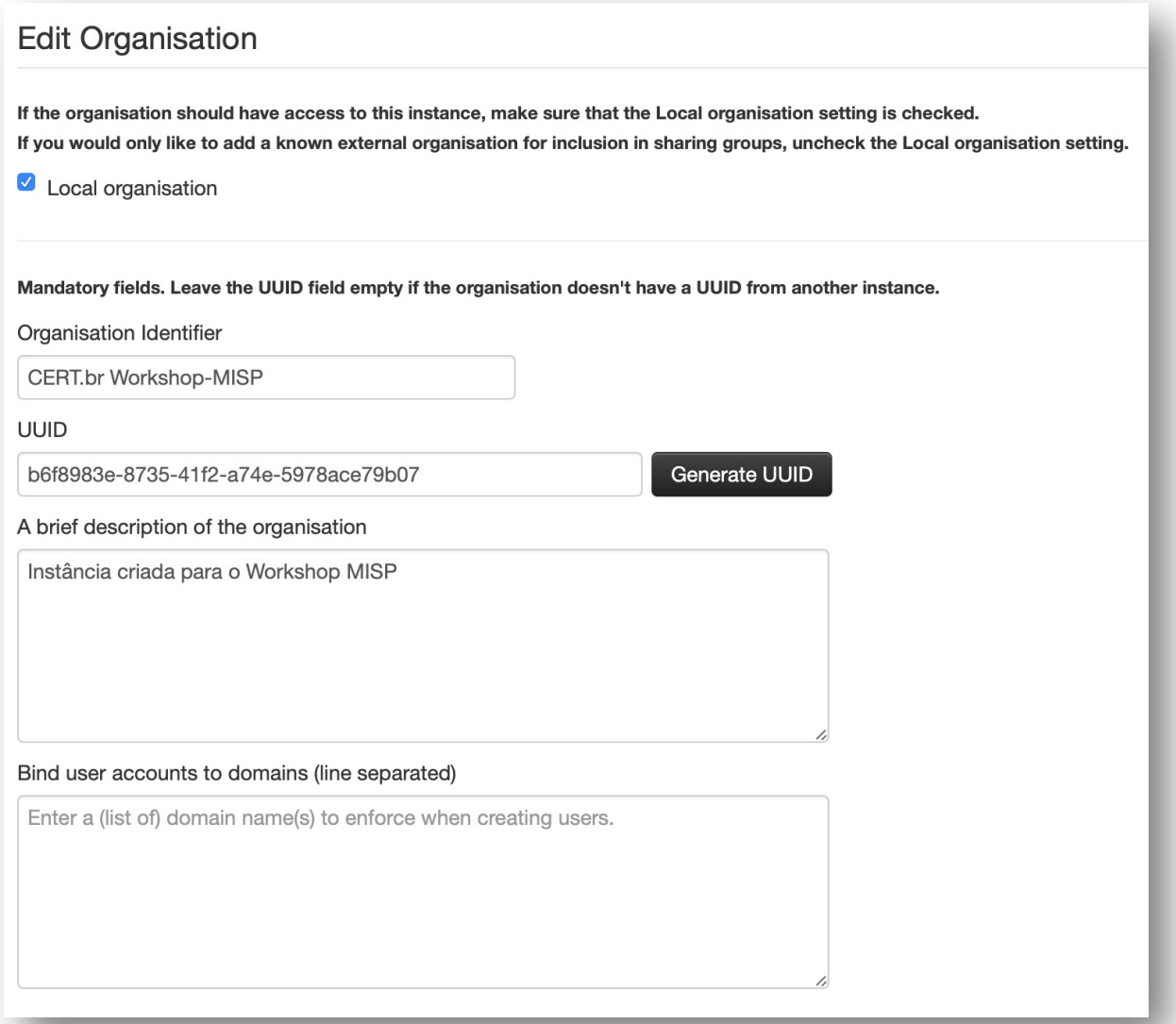
# Alterando a organização inicial (1/3)

Altere o nome da organização **`ORGNAME`** para um nome que reflita sua organização. Para isso:

- clique em "**`Administration – List Organisations`**"
- na Janela "**`Local organisations having a presence on this instance`**" identifique a organização **`ORGNAME`** e clique no ícone editar



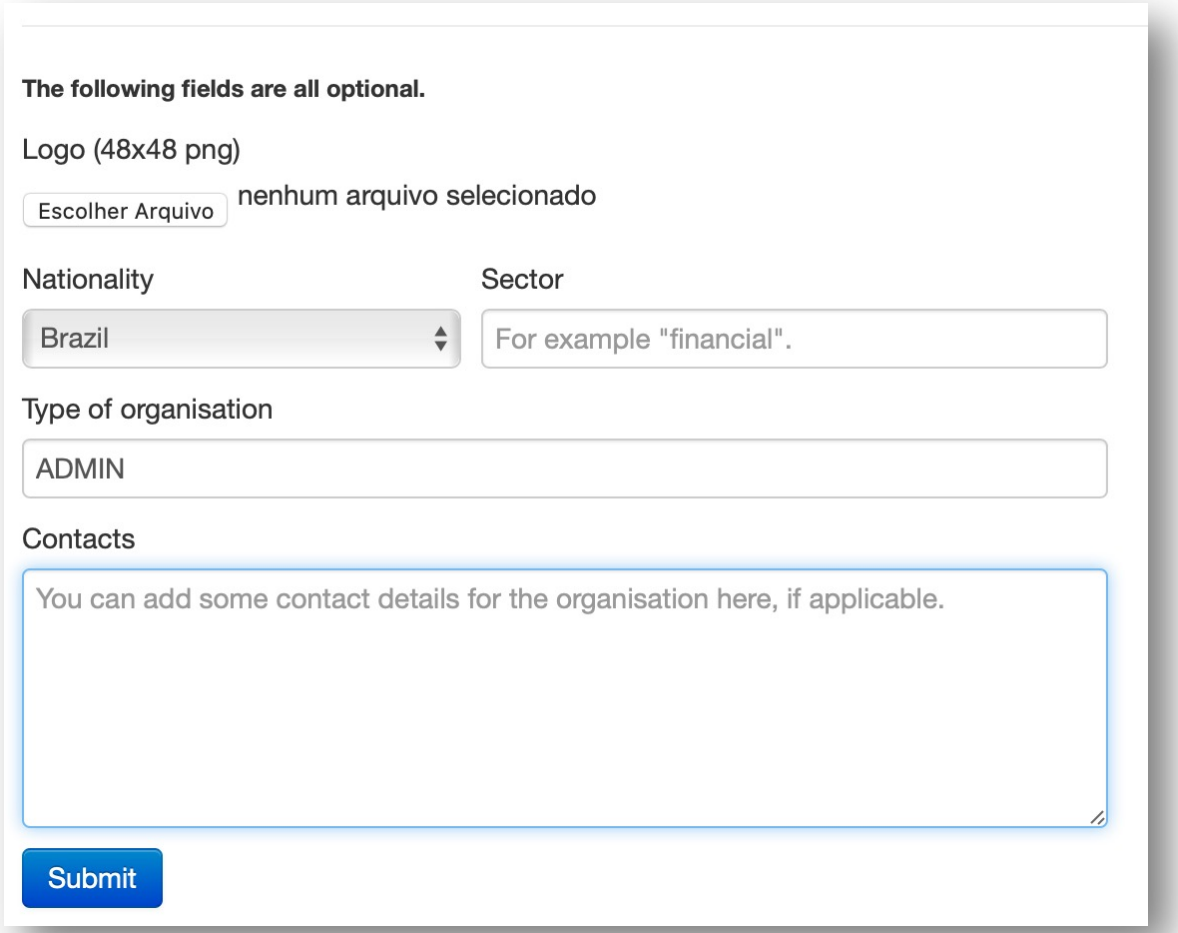
# Alterando a organização inicial (2/3)




Na janela "**`Edit Organisation`**" preencha os seguintes dados:

- Marque o *checkbox* "**`Local organisation`**", identificando a organização como local
- Em "**`Organisation Identifier`**":
  - Substitua **`ORGNAME`** pelo nome da sua organização
- Em **`UUID:`**
  - Mantenha a *string* gerada pelo sistema ou substitua pela *string* da sua organização caso já exista
- Em "**`A brief description of the organisation`**":
  - Coloque uma breve descrição da sua organização
- Em "**`Bind user accounts to domains (line separated)`**":
  - Você pode colocar uma lista de domínios permitidos para a criação dos usuários (contas de *e-mail*)

# Alterando a organização inicial (3/3)




Também é possível inserir as seguintes informações sobre uma organização:

- Logo
- Nacionalidade
- Setor
- Tipo
- Detalhes de contato

# Administrando usuários

Para utilização diária, é recomendado utilizar um usuário sem privilégios administrativos.

O usuário com privilégios de administrar o MISP deve ser utilizado apenas para tarefas administrativas, como por exemplo:

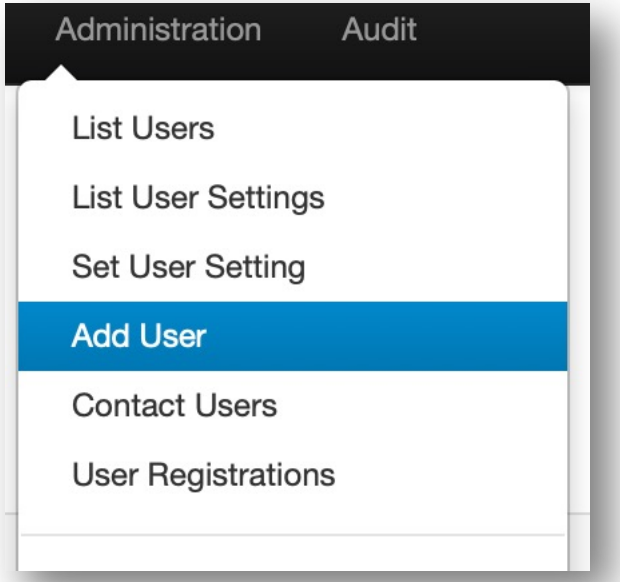
- Criar novos usuários
- Criar novas organizações
- Criar servidores de sincronia
- Atualizar o sistema
- Outras atividades administrativas

# Papéis (`roles`) dos usuários

- **`Admin`**
  - Privilégios para administrar o sistema
- **`Org admin`**
  - Privilégios para administrar a organização
- **`User`**
  - Podem criar eventos mas não publicá-los
- **`Publisher`**
  - Criam e publicam eventos dentro de uma organização
- **`Sync User`**
  - Utilizado para sincronia com outras instâncias MISP
- **`Read Only`**
  - Podem apenas ler eventos dentro de uma organização

# Criando usuários (1/3)

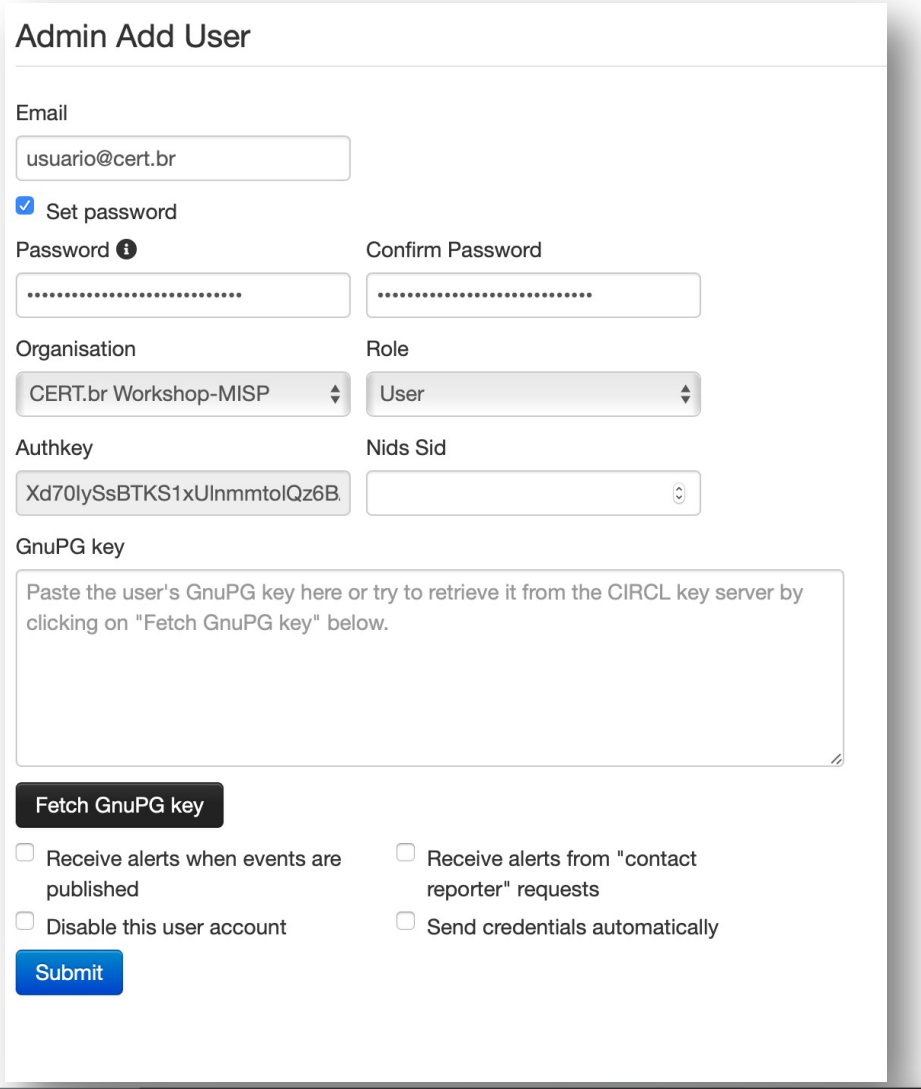
Para criar um novo usuário, clique em "**`Administration – Add User`**"



# Criando usuários (2/3)

Na janela "**`Admin Add User`**", preencha os seguintes campos:

- **`Email`**
  - Endereço de *e-mail* do usuário
- Marque o *checkbox* "**`Set password`**"
  - Digite e confirme a senha do usuário
- **`Organisation`**
  - Escolha a organização deste usuário
- **`Role`**
  - Escolha o papel do usuário
- **`Authkey`**
  - Gerada automaticamente pelo sistema
- **`Nids Sid`**
  - Utilizado pelo IDS




[CONTINUA NO PRÓXIMO *SLIDE*]

# Criando usuários (3/3)

- **`GnuPG key`**
  - Caso esteja utilizando chaves PGP, digite a chave do usuário ou clique no botão "**`Fetch GnuPG key`**"
- **`Receive alerts when events are published`**
  - Se selecionada, esta opção colocará o usuário em uma lista onde ele vai receber *e-mails* para cada evento publicado
- **`Receive alerts from "contact reporter" requests`**
  - Se selecionada, esta opção colocará o usuário em uma lista onde ele vai receber *e-mails* sempre que outro usuário tentar entrar em contato reportando eventos daquela organização
- **`Disable this user account`**
  - Se selecionada, esta opção desabilita a conta do usuário
  - Os desenvolvedores do MISP recomendam utilizar esta opção ao invés de apagar um usuário
- **`Send credentials automatically`**
  - Se selecionada, esta opção enviará as credenciais do usuário por *e-mail*

# Advanced authkeys

## Authkeys

- chaves de autenticação
- utilizadas para autenticar um usuário
  - em *scripts* de automação
  - em sincronizações entre servidores MISP

## Advanced authkeys

- introduzidas na versão 2.4.135 do MISP
- permitem que usuários gerem suas próprias **authkeys** com informações adicionais, como
  - comentário
  - data de expiração
  - IP autorizado para fazer o acesso
- opção "**Read Only**"
  - permite que usuários possam fazer apenas leitura de eventos
  - introduzida na versão 2.4.147 do MISP

# Verificando se as `advanced authkeys` estão habilitadas

Para verificar se as **`advanced authkeys`** estão habilitadas:

- clique em "**`Administration – Server Settings & Maintenance`**"
- na janela "**`Server Settings & Maintenance`**" clique na aba "**`Security Settings`**"
  - procure por "**`Security.advanced_authkeys`**", essa opção deve estar marcada como "**`True`**"

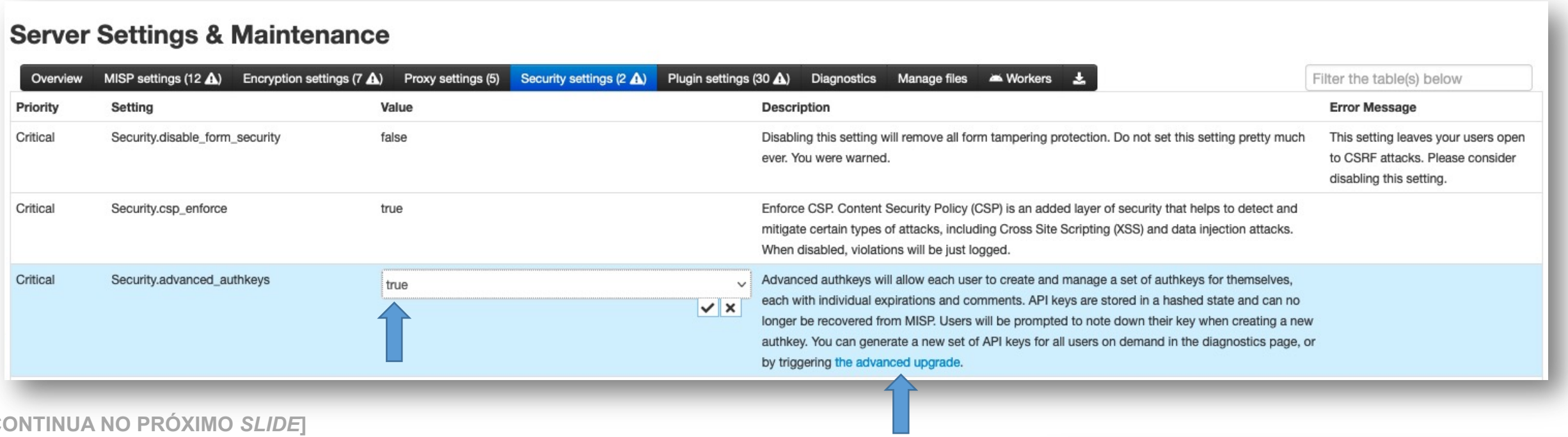
Observações:

- A opção de **`advanced authkeys`** não vem habilitada por padrão na instalação do MISP.
- A partir da versão 1.3, o Tutorial do CERT.br para instalação de MISP em Sistemas Ubuntu habilita as **`advanced authkeys`** durante o processo de instalação do MISP
  https://cert.br/misp/tutorial-ubuntu/

# Habilitando `advanced authkeys` (1/3)

Se as **`advanced authkeys`** não estiverem habilitadas:

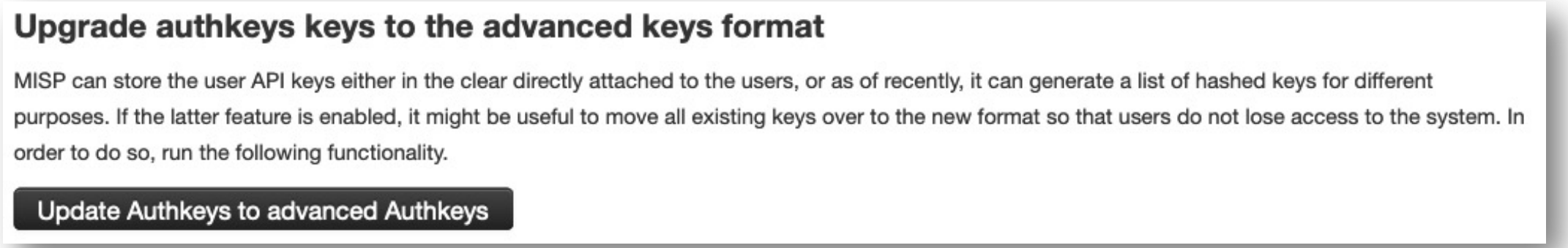
- Mude o valor de "**`Security.advanced_authkeys`**" de "**`False`**" para "**`True`**"
- Caso já existam usuários nesta instância, faça o processo de migração das **`authkeys`**
  - Para isso clique em "**`the advanced upgrade`**" ou acesse a URL: `https://<fqdn>/servers/serverSettings/diagnostics#advanced_authkey_update`



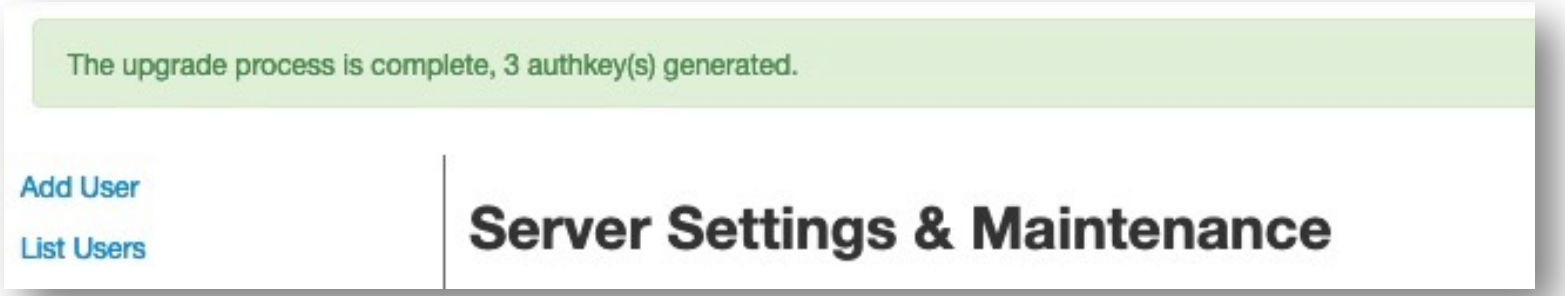

[CONTINUA NO PRÓXIMO *SLIDE*]

# Habilitando `advanced authkeys` (2/3)

– Inicie o processo de migração clicando em "**`Update Authkeys to advanced Authkeys`**"



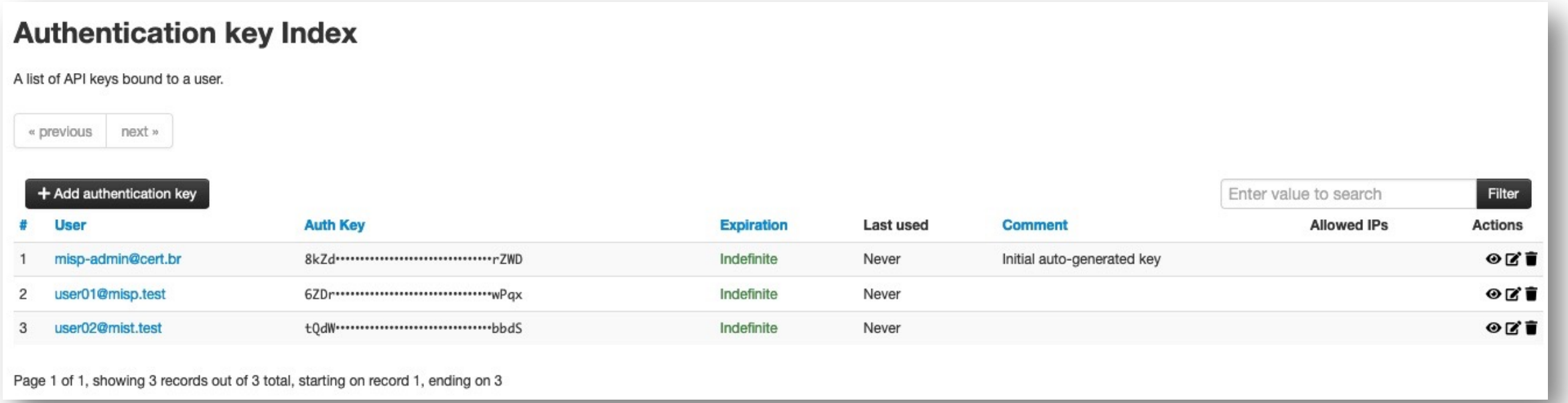

– Ao final do processo, uma mensagem será exibida no canto superior da tela:




[CONTINUA NO PRÓXIMO *SLIDE*]

# Habilitando `advanced authkeys` (3/3)

– Para verificar se o processo ocorreu sem problemas, confira se as **`authkeys`** foram geradas com sucesso clicando em "**`Administration — List Auth keys`**"



## Authentication key Index

A list of API keys bound to a user.

« previous | next »

+ Add authentication key

Enter value to search | Filter

| # | User | Auth Key | Expiration | Last used | Comment | Allowed IPs | Actions |
|---|---|---|---|---|---|---|---|
| 1 | misp-admin@cert.br | 8kZd••••••••••••••••••••••••••••••••••rZWD | Indefinite | Never | Initial auto-generated key | | |
| 2 | user01@misp.test | 6ZDr••••••••••••••••••••••••••••••••••wPqx | Indefinite | Never | | | |
| 3 | user02@mist.test | tQdW••••••••••••••••••••••••••••••••••bbdS | Indefinite | Never | | | |

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

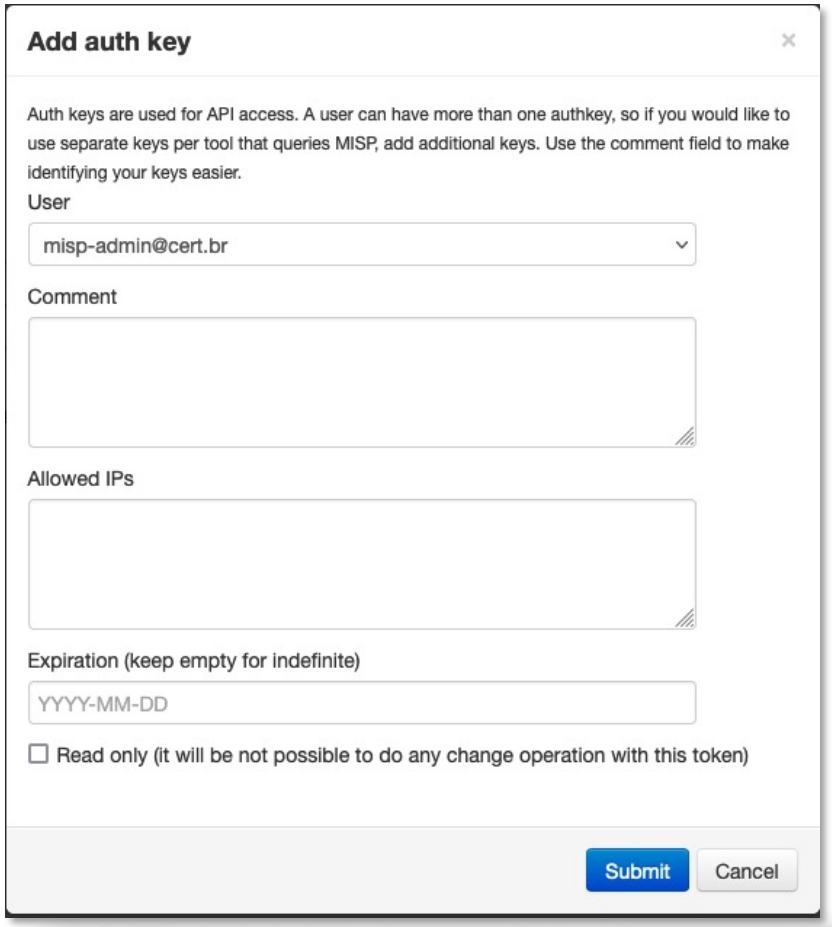
# Gerando novas `authkeys`
# Administrador (1/2)

TLP:WHITE

Para gerar uma nova **`authkey`** para qualquer usuário, o administrador do MISP deve clicar em "**`Administration — List Authkeys`**" e na janela "**`Authentication key Index`**", clicar no botão "**`+ Add authentication key`**".

Na janela "**`Add auth key`**":

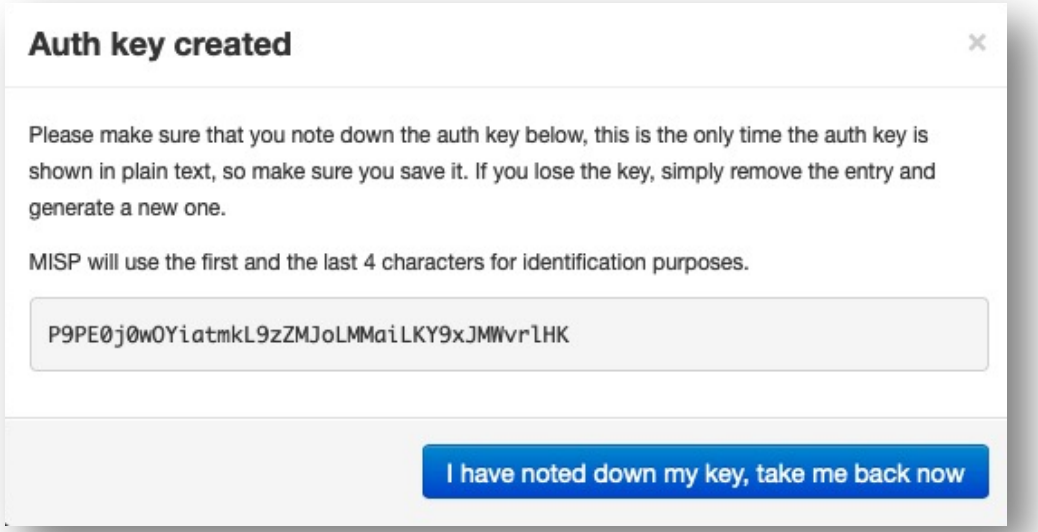
- Em "**`User`**" selecione para qual usuário a **`authkey`** será atribuída
- Em "**`Comment`**" digite um comentário para identificar esta **`authkey`**
- Em "**`Allowed IPs`**" defina por qual endereço IP este usuário pode se autenticar utilizando esta **`authkey`** ou deixe em branco para permitir qualquer endereço IP
- Em "**`Expiration`**" defina uma data para expiração da **`authkey`** ou deixe em branco para desabilitar a expiração para esta **`authkey`**
- A opção "**`Read only`**" pode ser marcada para permitir que este usuário faça apenas leitura dos eventos



# Gerando novas `authkeys`
# Administrador (2/2)



Ao finalizar a criação da **`authkey`**, a seguinte janela será exibida:




**IMPORTANTE:**

- O MISP exibe a **`authkey`** gerada apenas nesse momento, por isso, guarde-a de forma segura
- Caso o usuário perca a **`authkey`**, será necessário gerar uma nova

# Gerando novas `authkeys`
# Usuário

TLP:WHITE

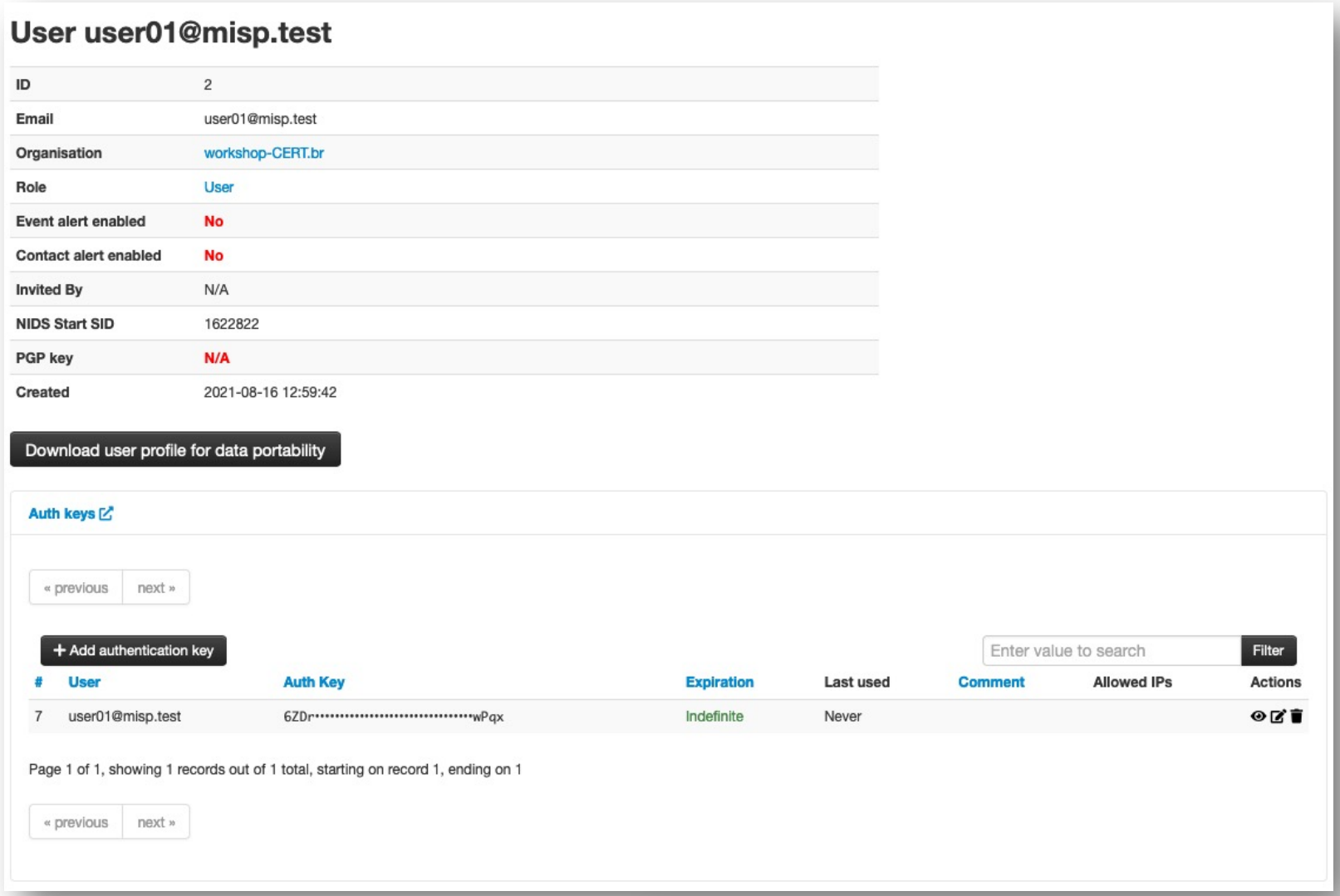
Qualquer usuário pode criar novas **`authkeys`** para ele mesmo, para isso, basta clicar em

"**`Global Actions – My profile`**"

Na janela "**`User [Email do Usuário]`**", clique no link "**`Auth keys`**". Ele vai expandir e mostrar as **`authkeys`** deste usuário.

Para adicionar uma nova **`authkey`**, clique no botão

"**`+ Add authentication key`**"



# 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:WHITE

# Sincronização: `Push` vs. `Pull`

| | Push | Pull |
|---|---|---|
| Direção | **A** envia eventos para **B** | **B** busca eventos em **A** |
| Propagação de eventos | Automática<br>No momento da publicação do evento | Manual<br>Via interface do MISP ou via **`cron`** |
| Dados para configuração de sincronia | **A** manda para **B**:<br>– **`UUID`** e **`ORGNAME`**<br>**B** manda para **A**:<br>– **`URL`**, **`Authkey`**, **`UUID`** e **`ORGNAME`** | **B** manda para **A**:<br>– **`UUID`** e **`ORGNAME`**<br>**A** manda para **B**:<br>– **`URL`**, **`Authkey`**, **`UUID`** e **`ORGNAME`** |
| Criação de contas e servidores para sincronia | **B** cria:<br>- Org. local com os dados de **A**<br>– **`Sync-user`** para **A** na Org. local criada<br>**A** cria:<br>- Servidor de sincronia, com a opção **`push`** marcada, com os dados de **B** | **B** cria:<br>- Servidor de sincronia, com a opção **`pull`** marcada, com os dados de **A**<br>**A** cria:<br>- Org. local com os dados de **B**<br>– **`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**

- Os desenvolvedores do MISP recomendam que a sincronia entre servidores seja feita via **`push`** para garantir que os eventos sejam compartilhados assim que forem publicados
- 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

TLP:WHITE

# Relembrando:
# 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:

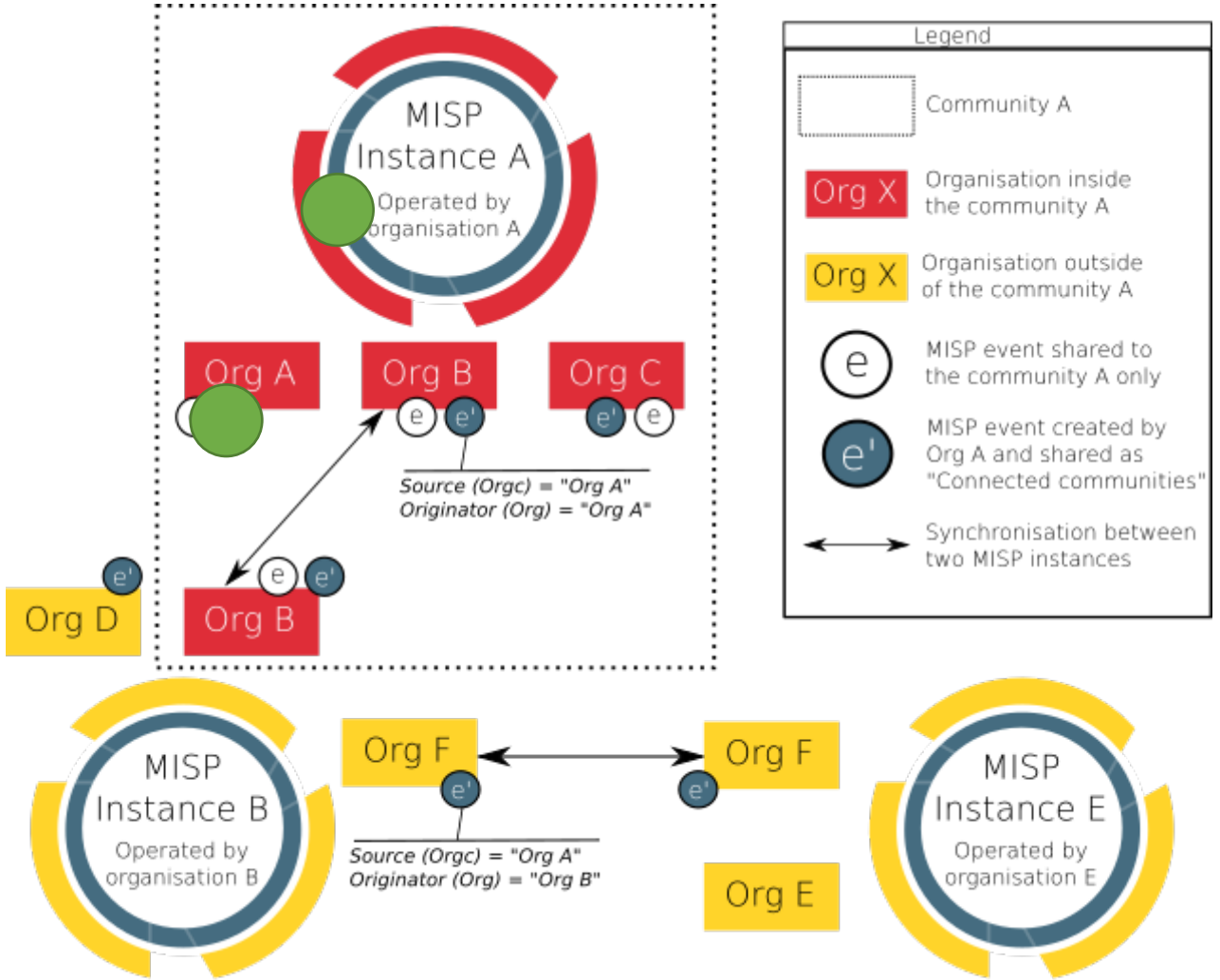
- **`Your organisation only`**
  - Apenas usuários da sua organização recebem os eventos

    **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

# Tipo de distribuição:
# `Your organisation only`

TLP:WHITE

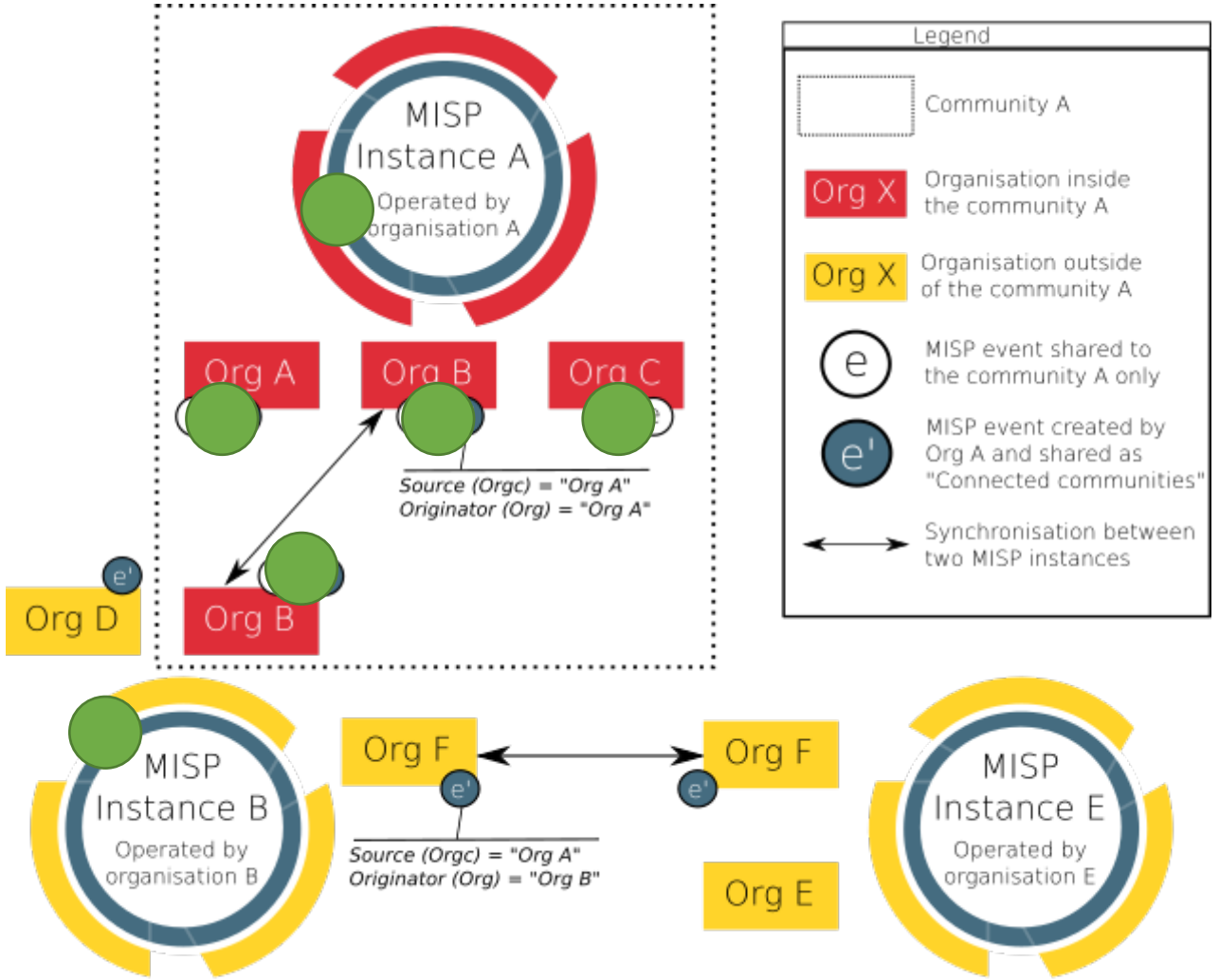



Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

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

# Tipo de distribuição:
# `This community only`

TLP:WHITE

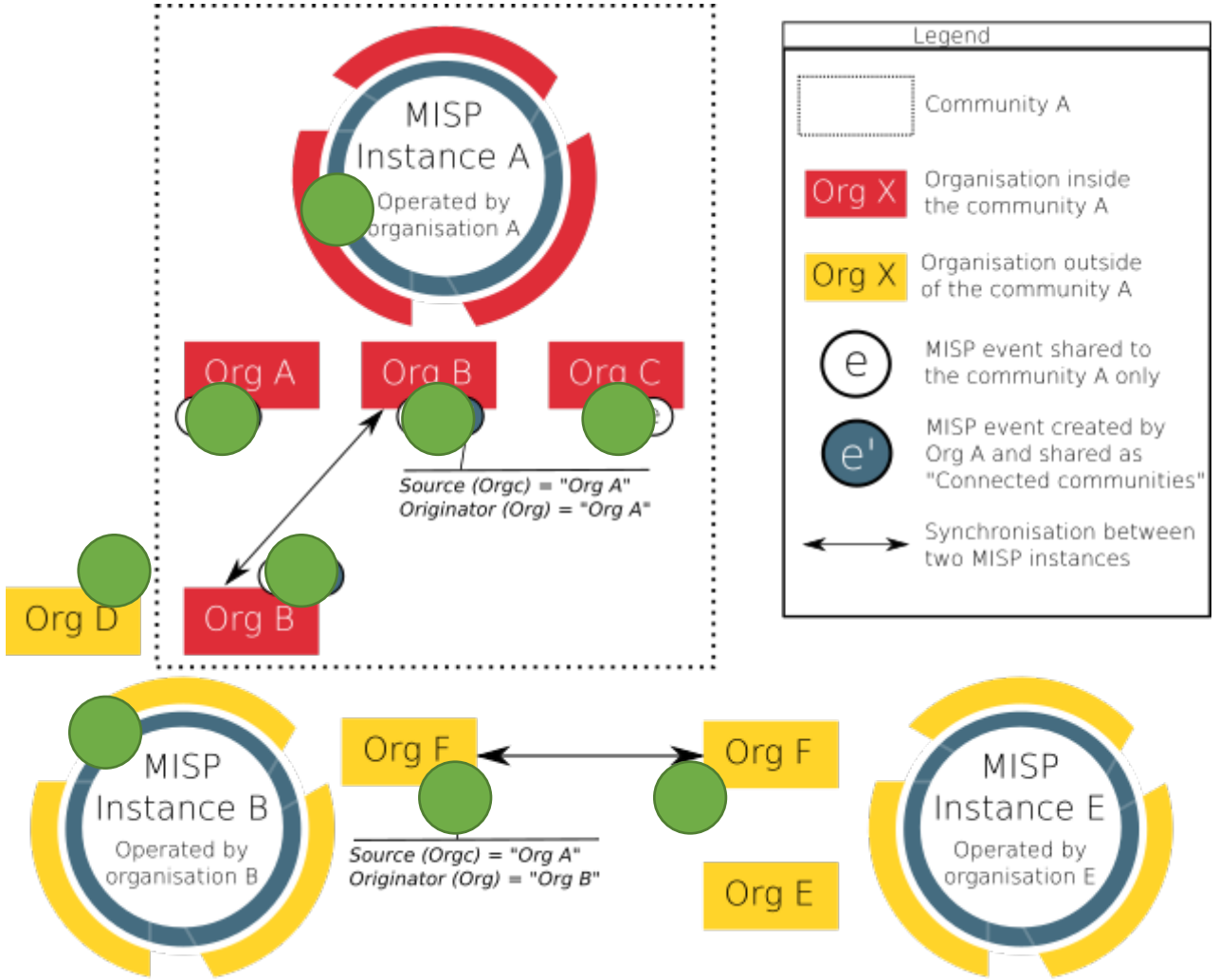



Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

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

# Tipo de distribuição:
# **Connected communities**

TLP:WHITE

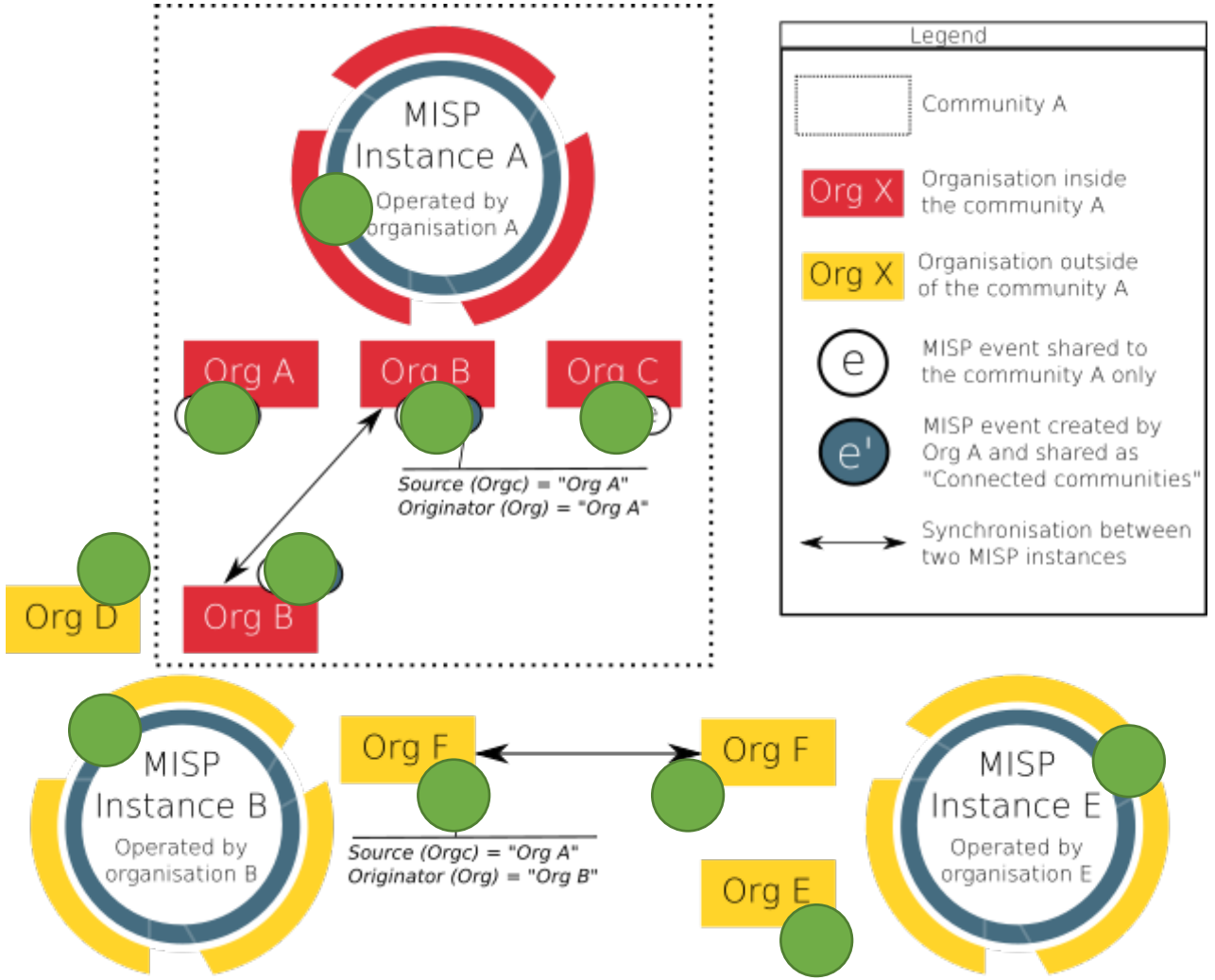



Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

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

# Tipo de distribuição:
# `All communities`

TLP:WHITE



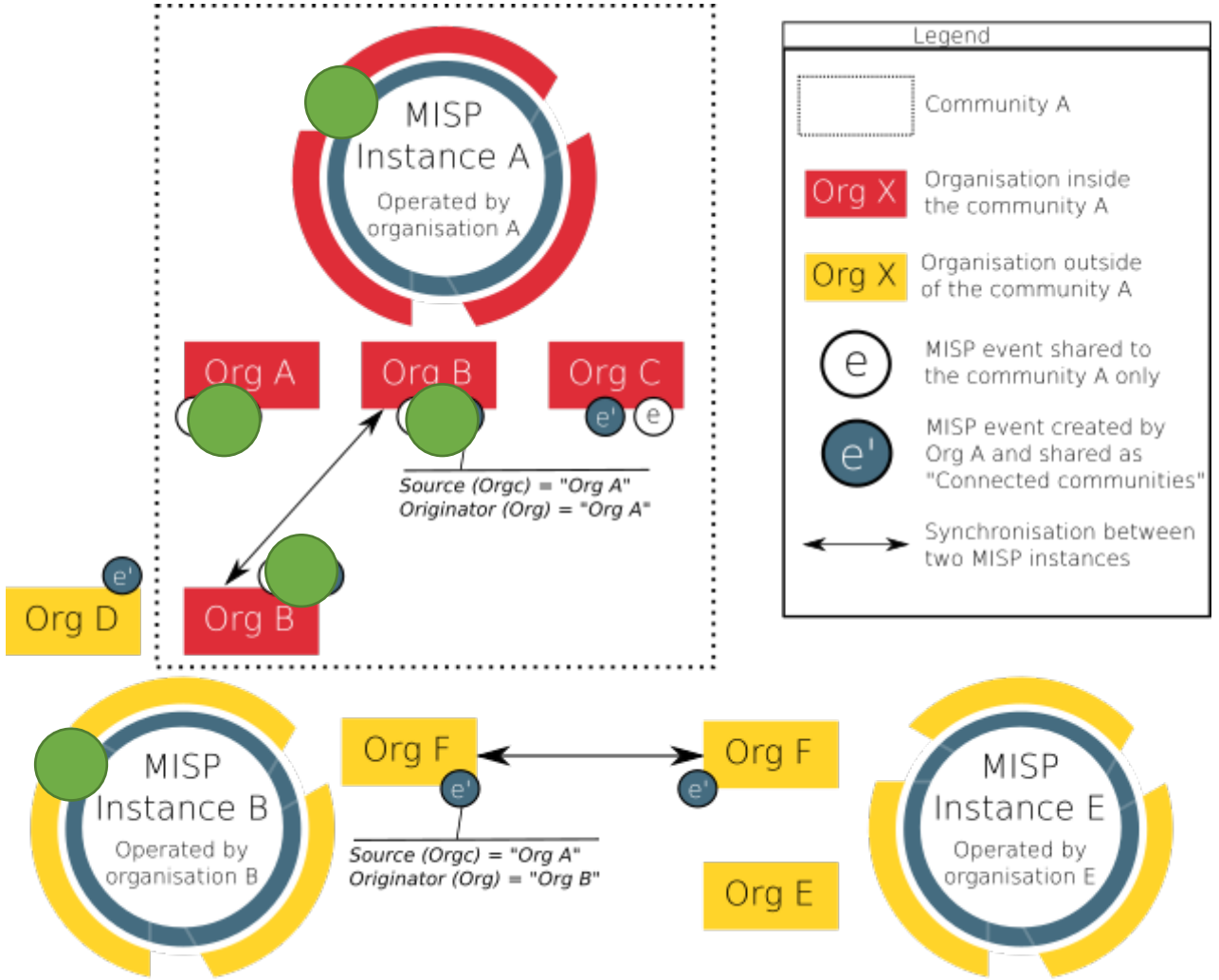

Representa a visibilidade de um evento publicado na Instância A, conforme o tipo de distribuição

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

# Tipo de distribuição: **Sharing group**

TLP:WHITE

**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

# Configuração da instância que receberá os eventos

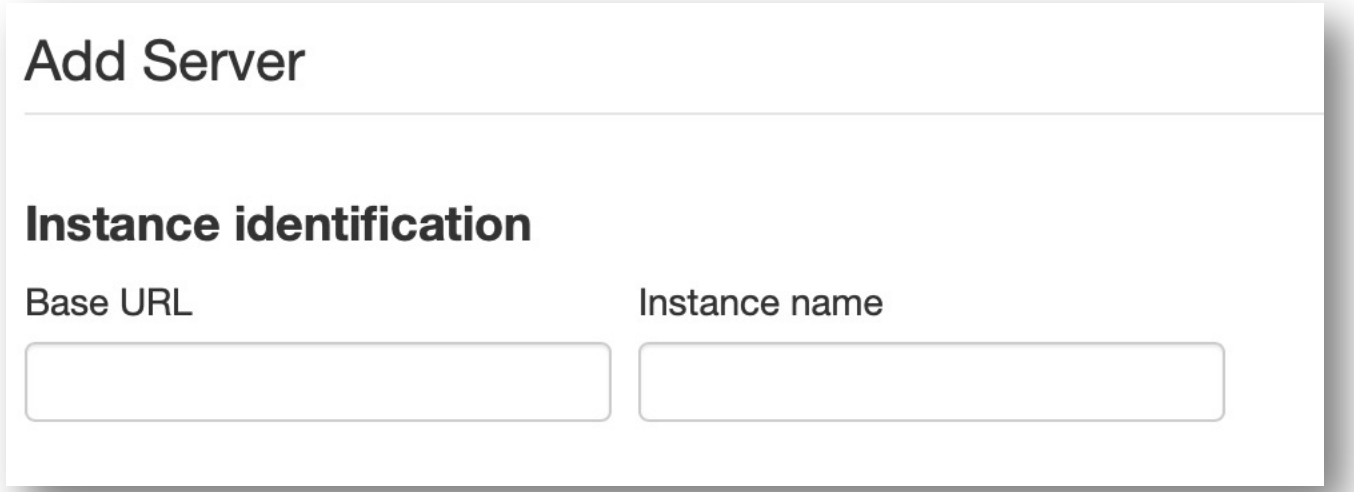
Crie na instância que receberá eventos:

- Uma **organização local**
  - com o **mesmo nome e o mesmo `UUID`** da organização que enviará os eventos
  - crie um usuário do tipo "**`sync-user`**" nesta organização
- Envie para os administradores da instância que enviará os eventos os seguintes dados da sua instância:
  - **`URL`**
  - **`Organisation Identifier`**
  - **`UUID`**
  - **`Authkey`** do usuário "**`sync-user`**"

# Configuração da instância que enviará os eventos (1/3)

Na instância que enviará os eventos, crie um servidor de sincronia:

- Na tela principal do MISP, clique em "**`Sync Actions - List Servers`**"
- Na tela "**`Servers`**", localize o link "**`New Servers`**"
- Na tela "**`Add Server`**" entre com a seguinte informação:
  - Em "**`Instance Identification`**" coloque os dados da **instância que receberá** os eventos:
    - **`Base URL:`** URL da instância
    - **`Instance Name:`** nome da organização

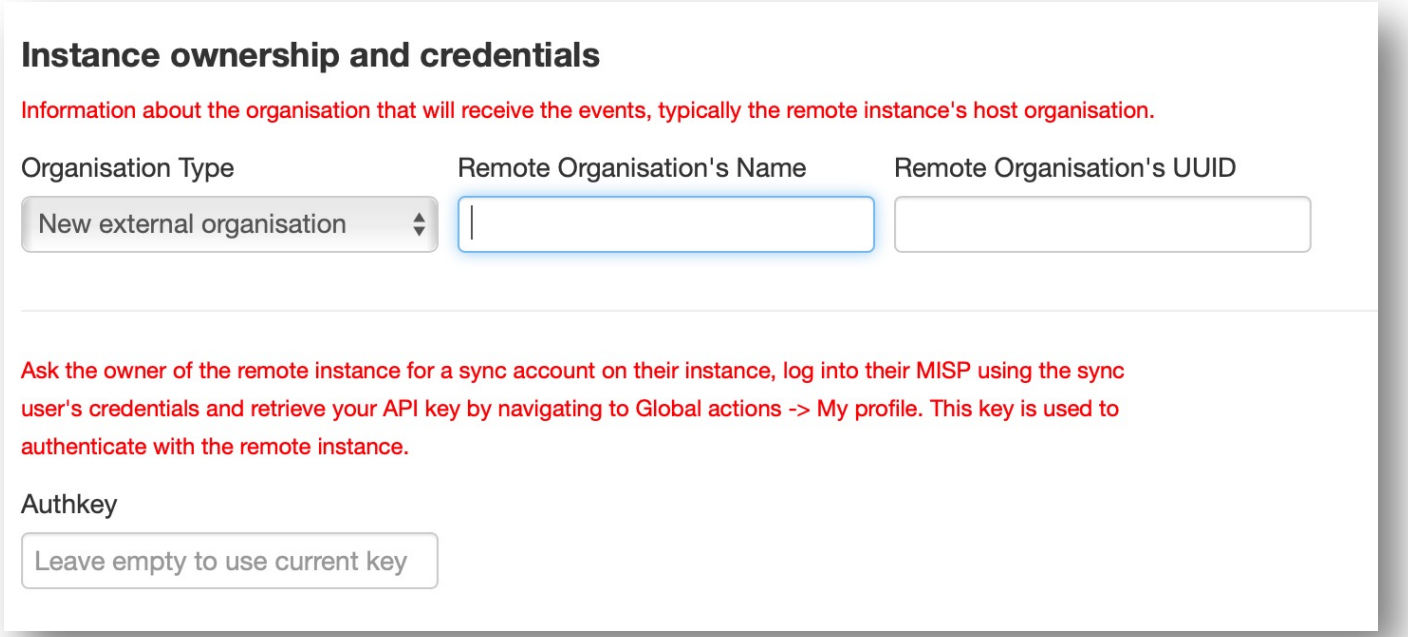



[CONTINUA NO PRÓXIMO *SLIDE*]

# Configuração da instância que enviará os eventos (2/3)

[CONTINUAÇÃO DO *SLIDE* ANTERIOR]

- Em "**`Instance ownership and credentials`**" coloque os dados da instância que receberá os eventos:
  - **`Organisation Type:`** Selecione o tipo de organização, geralmente "**`New external organisation`**"
  - **`Remote Organisation's Name:`** "**`Organisation Identifier`**" informado
  - **`Remote Organisation's UUID:`** o "**`UUID`**" informado
  - **`Authkey:`** Preencha com a **`authkey`** do **`sync-user`** informado



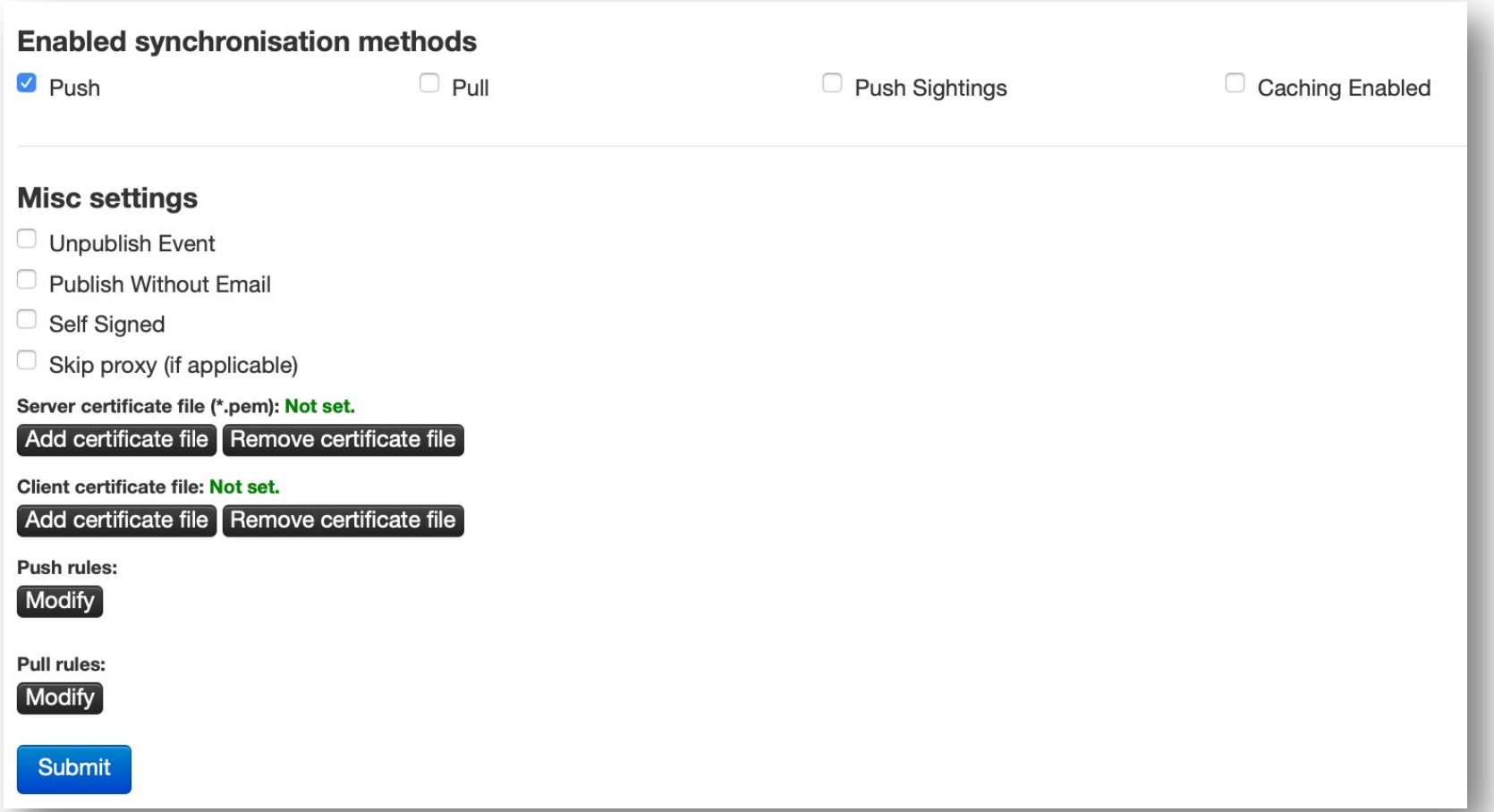

[CONTINUA NO PRÓXIMO *SLIDE*]

# Configuração da instância que enviará os eventos (3/3)

[CONTINUAÇÃO DO *SLIDE* ANTERIOR]

- Em "**`Enabled synchronisation methods`**":
  - Marque a opção "**`Push`**"

- Ao final clique em **`Submit`**



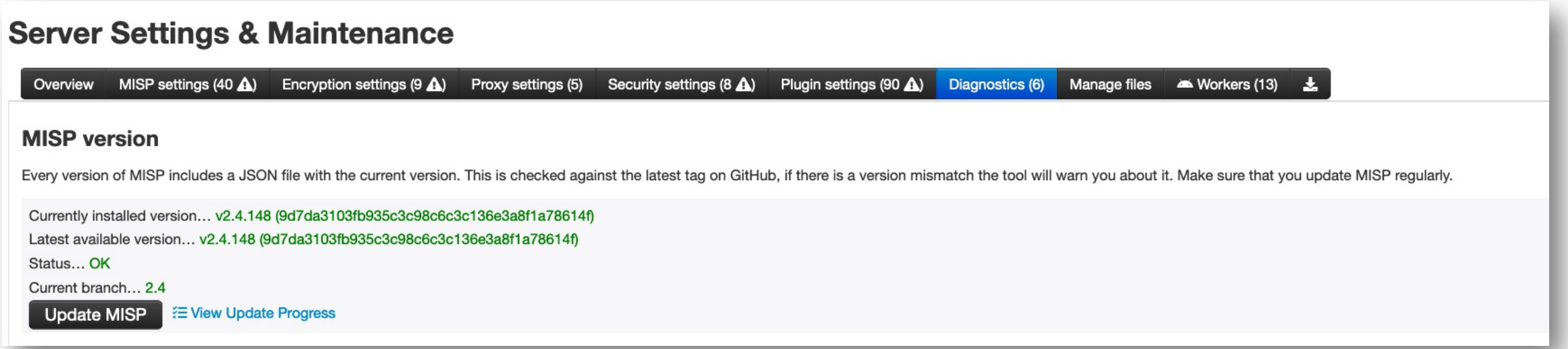
# Atualização do MISP (1/2)

É importante manter o MISP sempre atualizado.

- Para verificar se existem atualizações disponíveis, na janela principal do MISP clique em "**`Administration — Server Settings & Maintenance`**"
- Na tela "**`Server Settings & Maintenance`**" clique em "**`Diagnostics`**"
- Verifique se existem atualizações disponíveis ou se o MISP está atualizado

# Atualização do MISP (2/2)

- Caso necessite de atualizações, clique no botão "**`Update MISP`**"
- Aguarde até a atualização terminar
- Recarregue a página e verifique se o MISP foi atualizado



# Uso do MISP de Maneira Automatizada

cert.br nic.br cgi.br

# Recomendações para automatização

Ter um usuário específico para essa finalidade.

Começar “pequeno”.

# REST API

O MISP tem uma REST API que possibilita, entre outros:

- gerenciar eventos (adicionar, atualizar e remover)
- gerenciar atributos
- gerenciar **`tags`**
- gerenciar organizações
- gerenciar usuários
- submeter **`sightings`**
- obter estatísticas de atributos/**`tags`**

Referências: https://www.circl.lu/doc/misp/automation/

# Exemplo de consulta utilizando `curl`

TLP:WHITE

## Busca por eventos publicados no último dia (saída JSON)

```
curl -s \
  -d '{"returnFormat":"json","publish_timestamp":"1d"}' \
  -H "Authorization: <sua_authkey>" \
  -H "Accept: application/json" \
  -H "Content-type: application/json" \
  -X POST https://<FQDN>/events/restSearch
```

# Exemplo de consulta utilizando `curl`

## Busca por um evento pelo seu `ID` (saída CSV)

TLP:WHITE

```
curl -s \
  -d '{"returnFormat":"csv","eventid":"<id_do_evento>"}' \
  -H "Authorization: <sua_authkey>" \
  -H "Content-type: application/json" \
  -X POST https://<FQDN>/events/restSearch
```

# Exemplo de consulta utilizando `curl`

TLP:WHITE

## Busca de eventos com atributos específicos (saída JSON)

Retorna eventos

- com atributos do tipo URL
- publicados no último dia
- com a **`tag rsit:fraud="phishing"`**

```
curl -s \
  -d '{"returnFormat":"json","type":"url","date":"1d","tags":["rsit:fraud=\"phishing\""]}' \
  -H "Authorization: <sua_authkey>" \
  -H "Accept: application/json" \
  -H "Content-type: application/json" \
  -X POST https://<FQDN>/attributes/restSearch | \
  jq -c '.response.Attribute[].value'
```

# PyMISP

O PyMISP é uma biblioteca em Python utilizada para acessar o MISP através da sua REST API.

Para utilizar o PyMISP é necessário ter uma **`authkey`** em uma instância MISP.

Referências:

- https://www.misp-project.org/misp-training/a.2-pymisp.pdf
- https://www.circl.lu/doc/misp/pymisp/
- https://pymisp.readthedocs.io/en/latest/

# PyMISP
# **Funcionalidades**

TLP:WHITE

Interação:

- Adicionar, consultar, atualizar, apagar e publicar eventos
- Adicionar, consultar e atualizar
  - **`tags`** e **`sightings`**
  - atributos de
    - arquivos: *hashes, registry keys, patterns, pipe, mutex*
    - rede: endereço IP, *hostname*, domínio, URL, etc
    - *e-mail*: origem, destino, assunto, anexos, etc
    - dentre outros
- Fazer *upload* / *download* de binários
- Pesquisar por palavras-chave
- Consultar adições ou alterações em um determinado período (1h, 1d, 7d, etc):
  - eventos
  - meta-dados
  - atributos

Tarefas Administrativas:

- Gerenciar
  - usuários
  - organizações
  - servidores de sincronia
- Exportar estatísticas
- Gerenciar feeds
- Consultar *status* e versões

# PyMISP
# **Instalação**

É possível instalar o PyMISP pelo utilitário **`pip`** ou diretamente do seu repositório no GitHub.

Para instalar o PyMISP pelo **`pip`**, digite o comando:

```
pip install pymisp
```

Para instalar o PyMISP pelo GitHub, digite os comandos:

```
git clone https://github.com/MISP/PyMISP.git && cd PyMISP
python setup.py install
```

# PyMISP
## Arquivo `keys.py`

É uma convenção para facilitar o gerenciamento de **`authkeys`** e URLs utilizadas por múltiplos *scripts*

```
#!/usr/bin/env python3

misp_url = 'https://<FQDN>'
misp_key = ‘<AUTHKEY>' # MISP auth key found on the MISP web interface
misp_verifycert = True
```

TLP:WHITE

# Exemplo de Código para Publicação de um Evento (1/2)

```
#!/usr/bin/env python3

from pymisp import ExpandedPyMISP, MISPEvent, MISPAttribute
from keys import misp_url, misp_key, misp_verifycert

if __name__ == '__main__':
    # create misp instance
    misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert)

    # create event
    my_event = MISPEvent()

    my_event.info = 'Phishing: www.example.org'

    # threat IDs: 1 = High / 2 = Medium / 3 = Low / 4 = Undefined
    my_event.threat_level_id = 1
    # analysis IDs: 0 = Initial / 1 = Ongoing / 2 = Completed
    my_event.analysis = 1
    # distribution IDs: 0 = Your Organization only / 1 = This community only /
    # 2 = Connected communities / 3 = All communities
    my_event.distribution = 1

    # add basic information to event
    my_event = misp.add_event(event=my_event, pythonify=True)
```

[CONTINUA NO PRÓXIMO *SLIDE*]

# PyMISP
# Exemplo de Código para Publicação de um Evento (2/2)

TLP:WHITE

[CONTINUAÇÃO DO *SLIDE* ANTERIOR]

```
    # add event tag
    # tag IDs: 1 = tlp:red / 2 = tlp:amber / 3 = tlp:green / 4 = tlp:white
    misp.tag(my_event, '2')

    # the phishing URL
    phishing_url = 'http://www.example.org/phishing_page.html'

    # add event atribute
    url_Attribute = MISPAttribute()
    url_Attribute.category = 'Network activity'
    url_Attribute.type = 'url'
    url_Attribute.value = phishing_url
    url_Attribute.comment = 'Phishing URL'
    url_Attribute.to_ids = True
    misp.add_attribute(my_event.id, attribute=url_Attribute, pythonify=True)

    # publish event
    misp.publish(event=my_event.id)

    print(my_event.to_json())

# EOF
```

# Sobre o CERT.br

cert.br nic.br cgi.br

TLP:WHITE

# 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/

# Contato sobre MISP

misp@cert.br

https://cert.br/misp/

Notificações de incidentes: cert@cert.br

@certbr

nic.br cgi.br

www.nic.br | www.cgi.br