nic.br cgi.br | cert.br

5º Workshop MISP

31 de julho de 2024

São Paulo, SP

"Novas" funcionalidades do MISP: 2FA e Workflow

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

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

cert.br nic.br cgi.br

TLP:CLEAR

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 de Políticas

Filiações e Parcerias:

FIRST: Membro pleno desde 2002 **TF-CSIRT Trusted Introducer:** *Accredited* desde 2020

APWG: *Research partner* desde 2004 **SEI/CMU:** Cursos autorizados desde 2003

***Honeynet Project*:** Mantém o capítulo do Brasil desde 2003

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

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

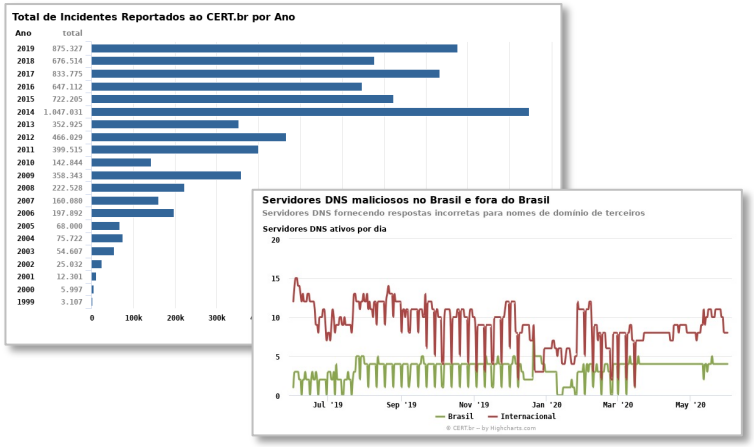
Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
  - Ponto de contato nacional de último recurso
  - Trabalho colaborativo com outras entidades
  - Auxílio na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Tratamento de Incidentes:
Fontes dos Dados, Métricas e Compartilhamento

TLP:CLEAR

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



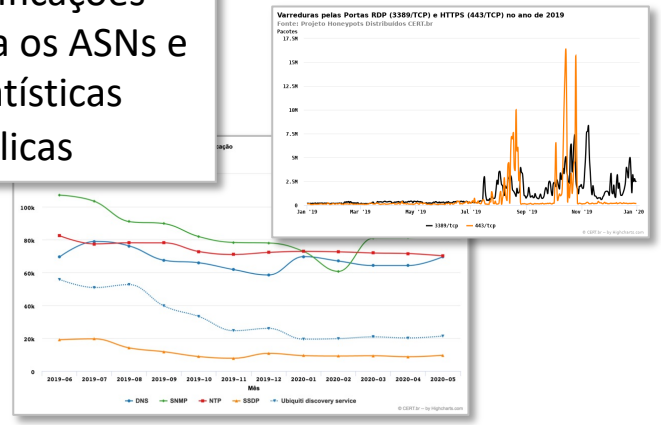
Compartilhamento via MISP

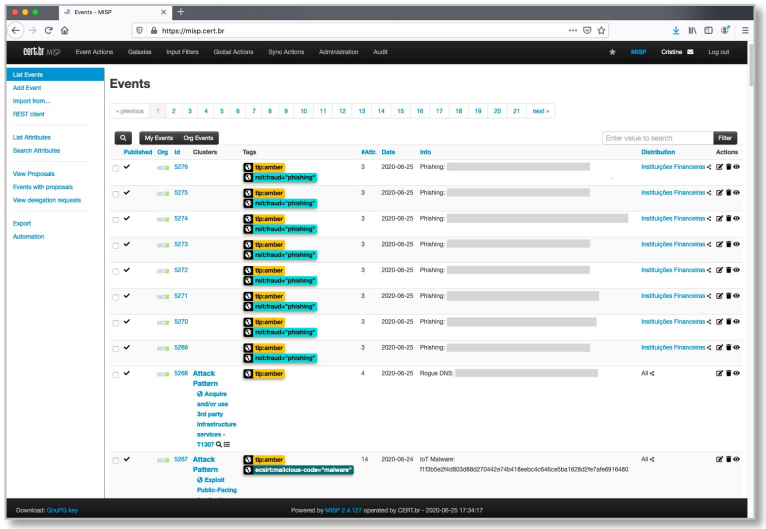
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

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://stats.cert.br/

https://cert.br/misp/

Agenda

- 2FA
  - Instalação
  - Configuração
- Workflows
  - Habilitação
  - Exemplos de uso
- Rodada de Q&A

2FA

Motivação

O que resolve:

– força bruta

– *stealers* executando na máquina do analista que capturam credenciais do MISP

O que **não** resolve:

– força bruta na API

– authkey vazada

2FA no MISP

A implementação de um segundo fator de autenticação no MISP é feita através do algoritmo: *Time-based and Single Use One-time password support (TOTP / HOTP)*

Essa funcionalidade foi implementada na versão 2.4.172 do MISP e pode ser utilizada de duas formas:

- ***TOTP* opcional** para todos os usuários (**opção default**)
- ***TOTP* mandatório** para todos os usuários

Para habilitar qualquer uma das opções, bibliotecas adicionais devem ser instaladas

Referências:
https://datatracker.ietf.org/doc/html/rfc4226
https://datatracker.ietf.org/doc/html/rfc6238
https://www.misp-project.org/2023/06/13/MISP.2.4.172.released.html

Instalando bibliotecas (1/2)

Nota: Os comandos apresentados nesse workshop são baseados no Tutorial completo para instalação e *hardening* do MISP em sistemas Ubuntu:

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

– Crie as variáveis de ambiente utilizando os seguintes comandos (faça adaptações nos diretórios, se necessário):

```
# export PATH_TO_MISP=/var/www/MISP
# export WWW_USER=www-data
# export SUDO_WWW='sudo -H -u www-data'
# export CAKE='/var/www/MISP/app/Console/cake'
```

Instalando bibliotecas (2/2)

O MISP necessita de duas bibliotecas adicionais, instaladas via *composer*, que são:

- `spomky-labs/otphp`
- `bacon-qr-code`

- Instale as bibliotecas com o seguinte comando:

```
# cd ${PATH_TO_MISP}/app
# ${SUDO_WWW} php composer.phar require spomky-labs/otphp
# ${SUDO_WWW} php composer.phar require bacon/bacon-qr-code
```

Habilitando o TOTP (1/4)

Após a instalação das bibliotecas, o TOTP já é disponível por padrão no MISP

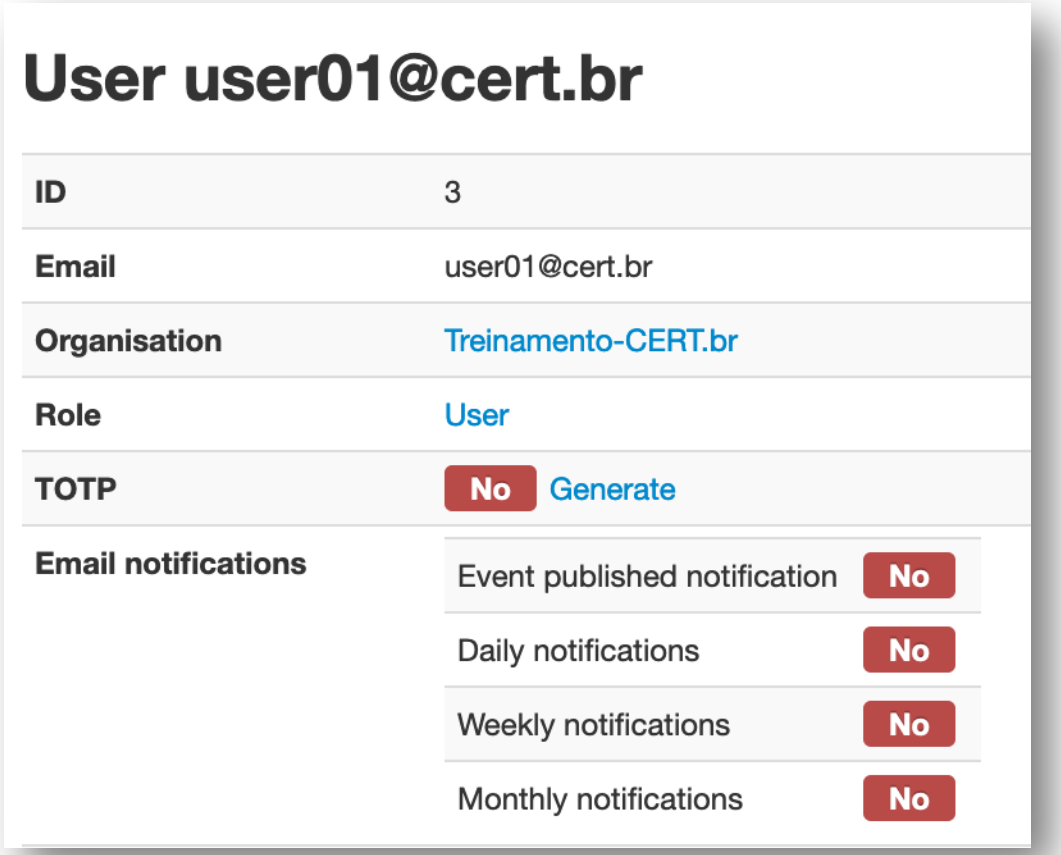
Ao logar no MISP:

– Localize no canto direito da barra superior o nome do seu usuário e clique nele

– Ou então acesse diretamente o link:

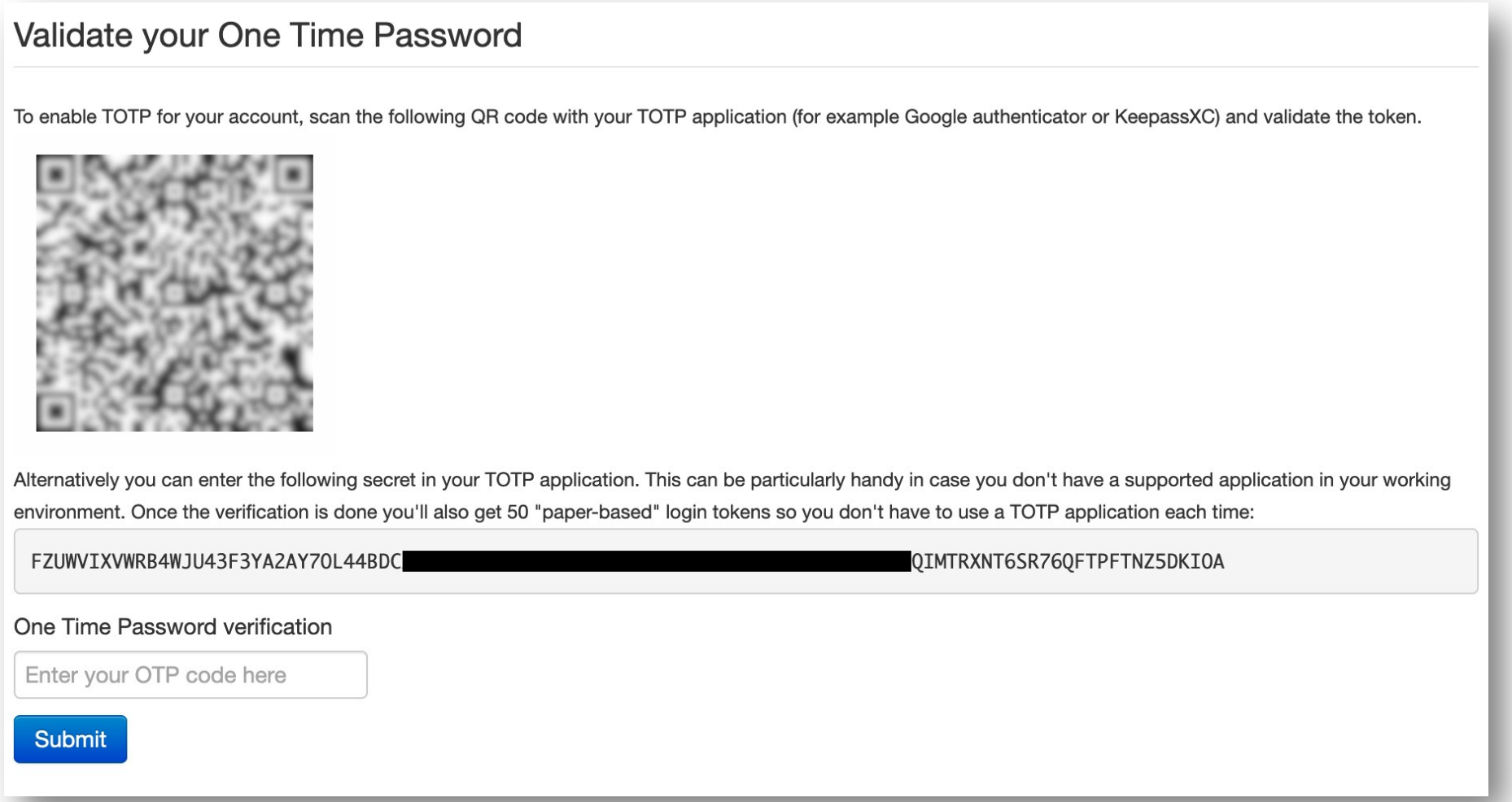
`https://<sua_url_misp>/users/view/me`

– Na opção **`TOTP`**, clique em **`Generate`**



Habilitando o TOTP (2/4)

– Utilizando um aplicativo para dispositivos móveis, escaneie o QR code apresentado:

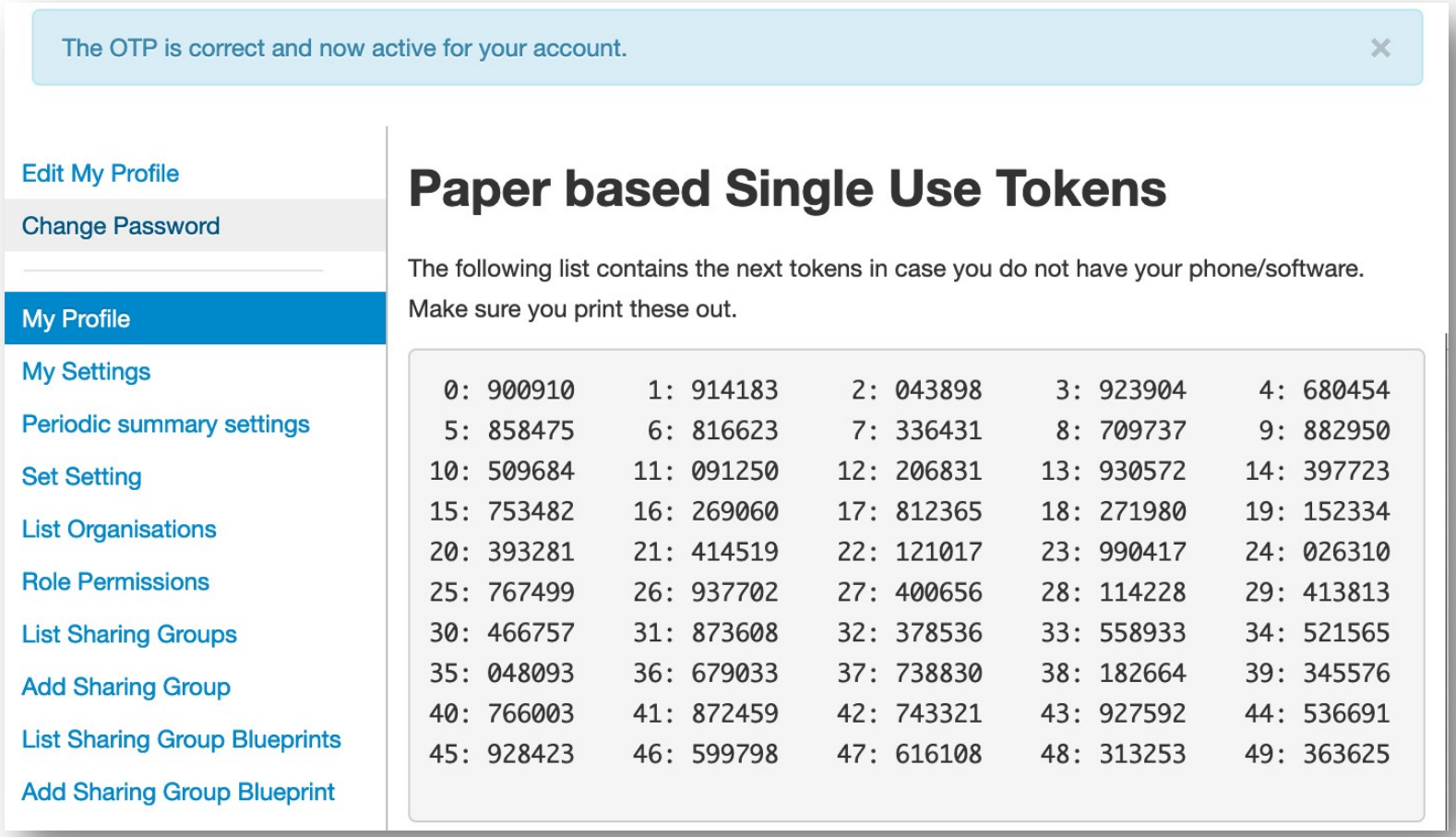


Habilitando o TOTP (3/4)

A tela seguinte exibe a mensagem que o TOTP foi habilitado com sucesso, e logo abaixo, exibe os "**`Paper based Single Use Tokens`**":

Guarde esses tokens em um local seguro

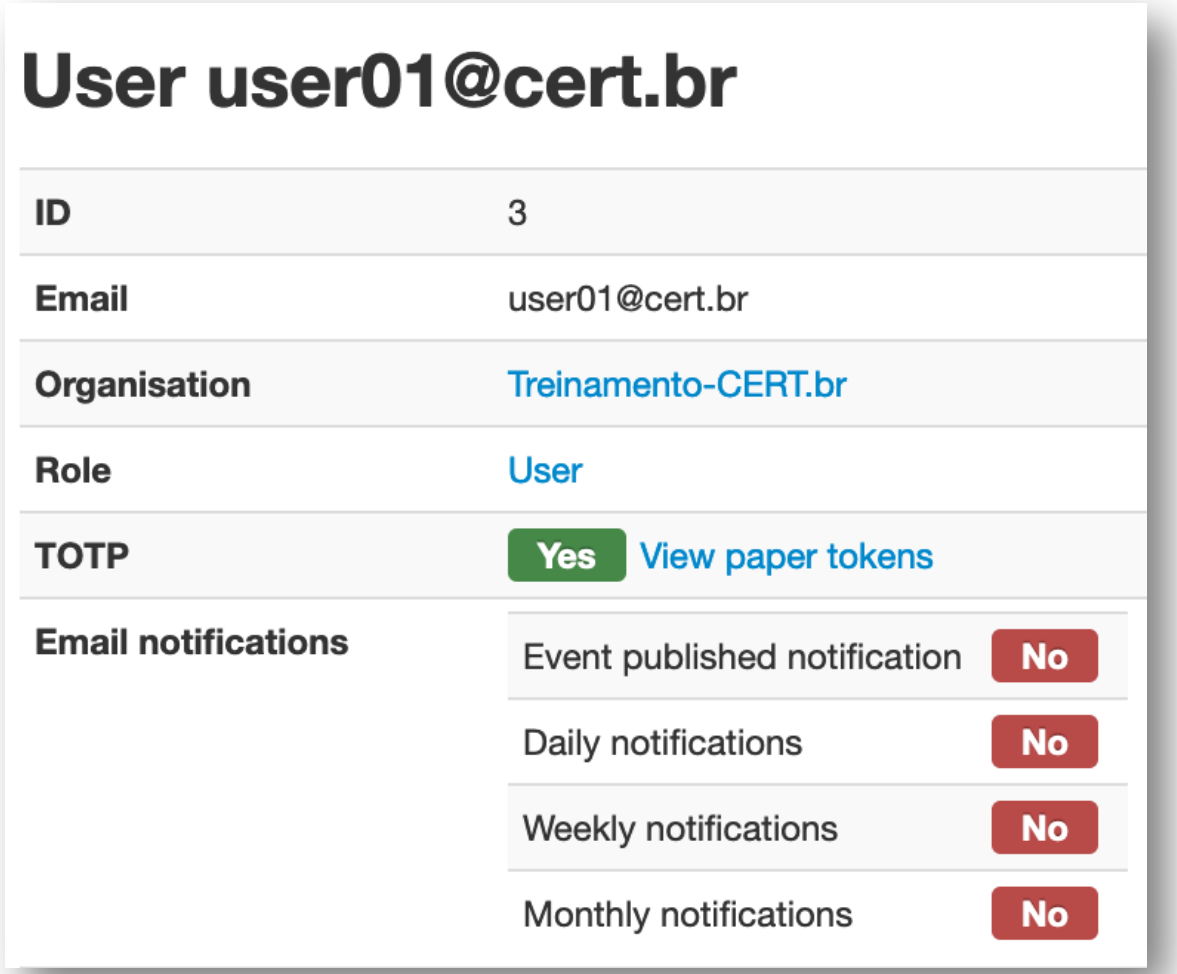
- Imprima ou guarde cifrado em arquivo
- Eles podem ser úteis se você perder o acesso ao dispositivo com token



Habilitando o TOTP (4/4)

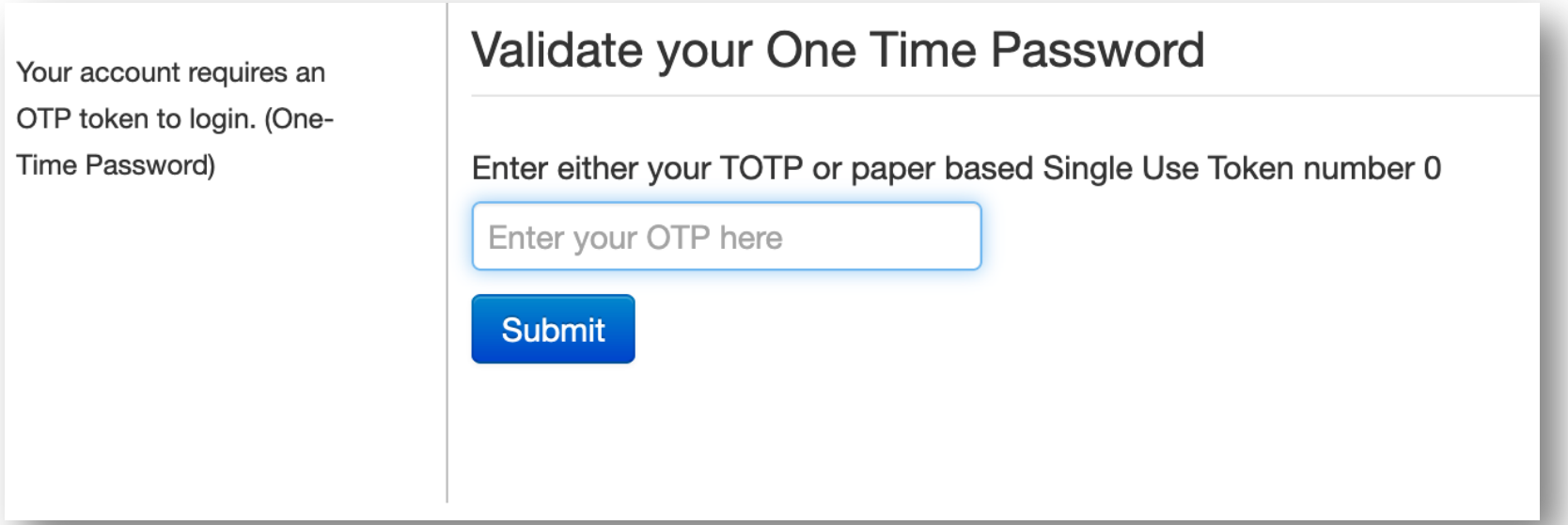
– Clique novamente no seu usuário e verifique que o TOTP foi habilitado

– Observe que é possível rever os tokens de papel clicando no link "**`View paper tokens`**"



Testando o TOTP

– Depois de habilitar o TOTP, faça logout e login novamente. Após digitar usuário e senha, uma nova tela será exibida:



– Observe que neste momento existem duas possibilidades para o TOTP: o aplicativo do celular ou o token “0” dos tokens de papel

Habilitando o TOTP mandatório (1/2)

Para realmente conferir segurança ao processo de login, é necessário que o TOTP seja mandatório

Após sua habilitação, qualquer usuário que ainda não tenha TOTP será forçado a habilitá-lo no próximo login

É possível habilitar essa opção pela linha de comando ou pela interface do MISP

– Para habilitar pela linha de comando, digite:

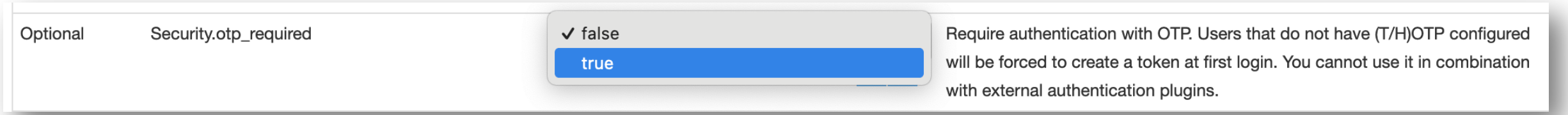
```
# ${SUDO_WWW} -- ${CAKE} Admin setSetting "Security.otp_required" true
```

Habilitando o TOTP mandatório (2/2)

Para habilitar pela interface do MISP, com um usuário administrador:

– Clique em **`Administration – Server Settings & Maintenance`**

– Na tela **`Server Settings & Maintenance`**, clique na aba **`Security`**, localize a opção **`Security.otp_required`**, clique na opção "**`false`**" e altere para "**`true`**":



Recuperação de login após perda do autenticador

Caso um usuário perca o dispositivo autenticador e não tenha o papel com os tokens, é possível recuparar o login:

– Do usuário via interface do MISP (pelo admin).

– Do admin via linha de comando no SO

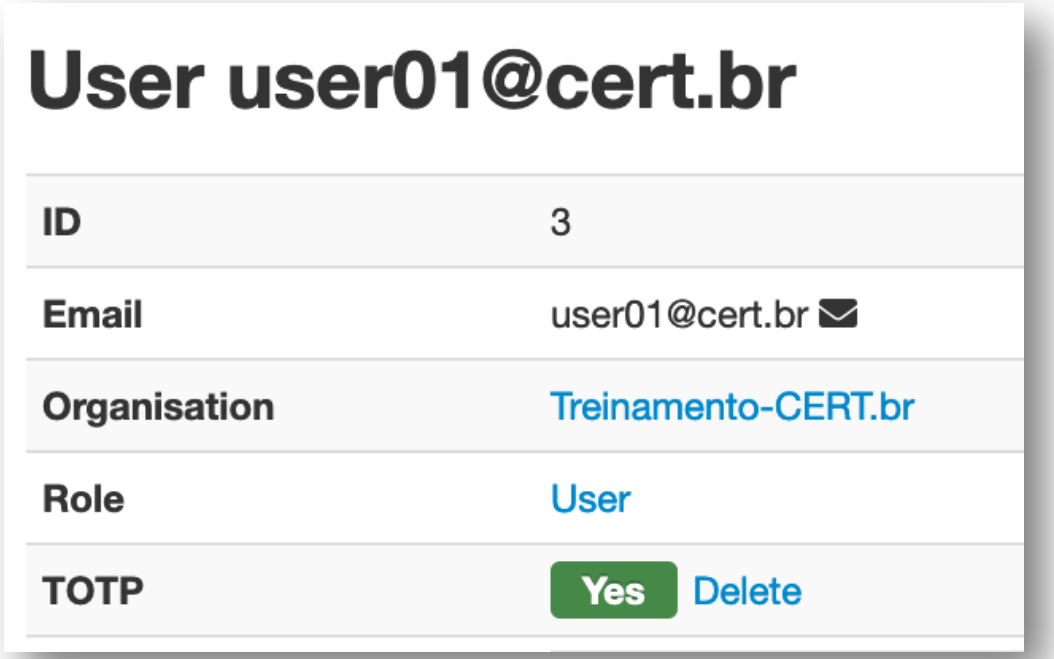
Recuperação de login de usuário

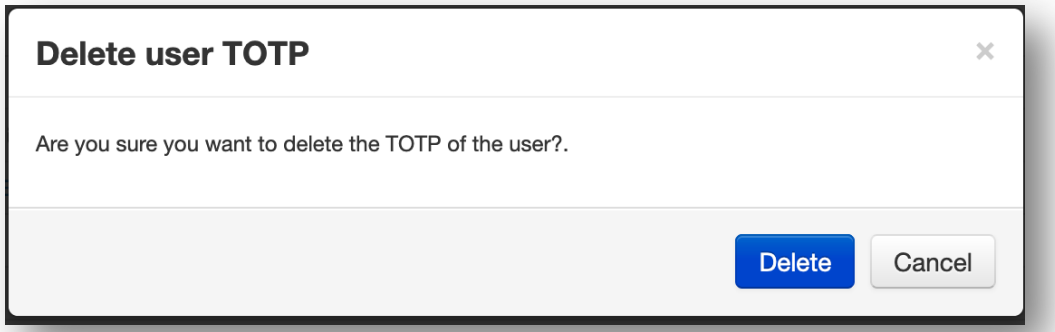
Para desabilitar o TOTP de um usuário que perdeu acesso ao dispositivo, logado como administrador:

– Clique em **`Administration -- List Users`**, selecione o usuário e clique em **`view`** (ícone representado por um olho)

– Em TOTP, clique em **`Delete`**

– Na tela “**`Delete user TOTP`**”, confirme a operação clicando no botão **`Delete`**





Recuperação de login de admin (1/2)

Para o administrador conseguir logar novamente no MISP sem o TOTP, é necessário desabilitar o TOTP do sistema todo

– Faça isso com o seguinte comando:

```
# ${SUDO_WWW} -- ${CAKE} Admin setSetting "Security.otp_disabled" true
```

– Faça o login do usuário administrador e uma vez logado no sistema, habilite novamente o TOTP com o seguinte comando:

```
# ${SUDO_WWW} -- ${CAKE} Admin setSetting "Security.otp_disabled" false
```

Recuperação de login de admin (2/2)

Após o passo anterior de desativar e re-ativar o TOTP, é necessário remover o TOTP antigo. Para isso:

- Clique no nome do usuário administrador
- Na opção **`TOTP`**, clique em **`Delete`** e confirme na tela "**`Delete user TOTP`**"
- Clique novamente no usuário administrador -- a opção **`Generate`** estará disponível
- Clique em **`Generate`** para iniciar o processo de criação de um novo token

Workflows

cert.br nic.br cgi.br

Possibilidades de uso

Prevenir alguns comportamentos padrão do MISP

Prevenir consultas para serviços de terceiros (ex: VirusTotal) que contenham dados sensíveis

Enviar notificações para aplicações como Mattermost

Enviar emails caso alguns critérios sejam atendidos

Entre outros

Pré-requisitos

- Instalar os módulos do MISP: https://github.com/MISP/misp-modules
- Plugin **`Action`** habilitado
- Opção **`MISP.background_jobs`** habilitada

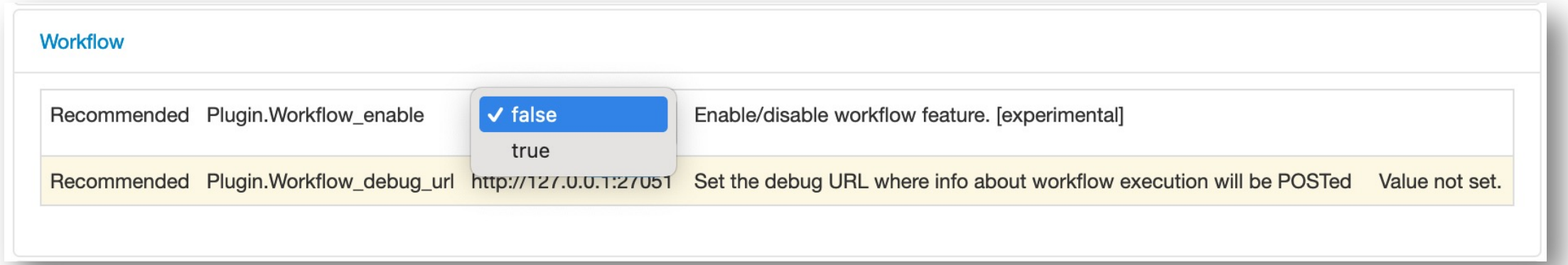
Habilitando Workflows

– Logue como administrador

– Clique em **`Administration – Server Settings & Maintenance`**

– Na tela **`Server Settings & Maintenance`** clique na aba **`Plugin`** e localize o plugin **`Workflow`**

– Altere o campo **`Plugin.Workflow_enable`** para **`true:`**



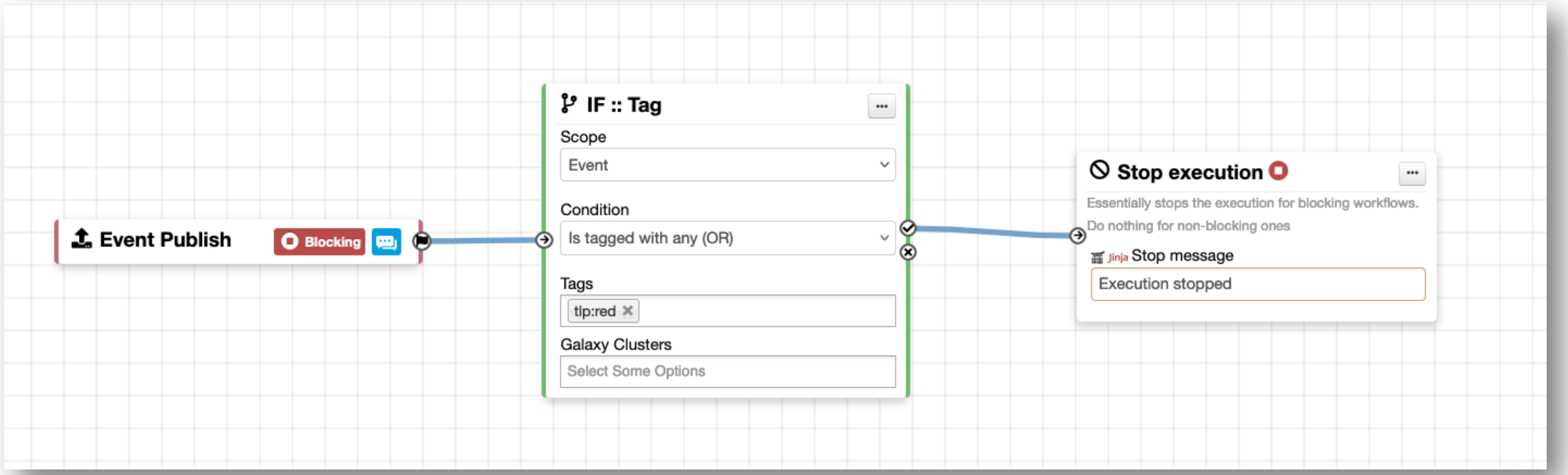
Terminologia

Workflow: sequência de operações a serem executadas no MISP

Nó (node): cada operação a ser executada dentro de um workflow

Caminho de execução (execution path): caminho composto por nós

Trigger: nó inicial de um workflow, executado quando uma atividade específica acontece



Como funciona (1/2)

1. Uma atividade ocorre no MISP
   - um novo evento é criado
   - um atributo é salvo
   - um usuário é criado
   - etc
2. Uma ou mais condições são verificadas
   - um evento possui um tag específico
   - Um evento possui uma dada distribuição
   - etc
3. Uma ou mais ações podem ser executadas
   - impedir a publicação de um evento
   - enriquecer evento
   - anexar um tag
   - etc

Como funciona (2/2)

1. Uma atividade ocorre no MISP e aciona um trigger
2. O workflow associado a este trigger é executado
   - checa se todas as condições são satisfeitas
   - executa todas as ações
3. Resultado da execução do trigger:
   - **sucesso**: ação continua
   - **falha ou bloqueio**: ação é cancelada

Exemplo

1. Um evento está prestes a ser publicado
2. O MISP executa o workflow com o trigger para publicação de evento
   - **sucesso**: continua a ação de publicação do evento
   - **falha ou bloqueio**: interrompe a publicação do evento e registra a razão

TLP:CLEAR

Triggers disponíveis

All | attribute | event | log | object | others | post | shadow-attribute | sighting | user | Blocking | Enabled | Disabled

Trigger name	Scope	Trigger overhead	Description	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Debug enabled	Enabled	Actions
Attribute After Save	attribute	high	This trigger is called after an Attribute has been saved in the database	2	✗	✓	3	2024-07-24 17:09:57	☐	✗	
Enrichment Before Query	others	low	This trigger is called just before a query against the enrichment service is done		✓	✓				✗	
Event After Save	event	high	This trigger is called after an Event or any of its elements has been saved in the database	11	✗	✓	2	2024-07-24 17:18:09	☐	✗	
Event After Save New	event	low	This trigger is called after a new Event has been saved in the database	2	✗	✓	4	2024-07-24 17:06:39	☐	✗	
Event After Save New From Pull	event	low	This trigger is called after a new Event has been saved in the database from a PULL operation. This trigger executes in place of `event-after-save-new`	0	✗	✓	6	2024-07-24 17:10:09	☐	✗	
Event Before Save	event	high	This trigger is called before an Event or any of its elements is about to be saved in the database	0	✓	✓	1	2024-07-24 17:06:40	☐	✗	
Event Publish	event	low	This trigger is called just before a MISP Event starts the publishing process	11	✓	✓	5	2024-07-24 17:21:30	☐	✓	
Log After Save	log	high	This trigger is called after a Log event has been saved in the database		✗	✗				✓	
Object After Save	object	high	This trigger is called after an Object has been saved in the database		✗	✓				✓	
Post After Save	post	low	This trigger is called after a Post has been saved in the database		✗	✗				✓	
Shadow Attribute Before Save	shadow-attribute	medium	This trigger is called just before a Shadow Attribute is saved in the database		✓	✓				✓	
Sighting After Save	sighting	medium	This trigger is called when a sighting has been saved		✗	✓				✓	
User After Save	user	low	This trigger is called after a user has been saved in the database		✗	✗				✓	
User Before Save	user	low	This trigger is called just before a user is save in the database		✓	✗				✓	

TLP:CLEAR

Condições disponíveis (logic modules)

All | Action | Logic | misp-module | Custom | Blocking | Enabled | Disabled

Enter value to search | Filter

Module name	Description	Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions
Blueprint logic module	Lorem ipsum dolor, sit amet consectetur adipisicing elit.	logic	×	×	×	✓	×	
Concurrent Task	Allow breaking the execution process and running concurrent tasks. You can connect multiple nodes the `concurrent` output.	logic	×	×	×	×	×	
IF :: Count	Count IF / ELSE condition block. It counts the amount of entry selected by the provided hashpath. The `then` output will be used if the encoded conditions is satisfied, otherwise the `else` output will be used.	logic	×	×	×	×	✓	
IF :: Distribution	Distribution IF / ELSE condition block. The `then` output will be used if the encoded conditions is satisfied, otherwise the `else` output will be used.	logic	×	✓	×	×	✓	
Filter :: Generic	Generic data filtering block. The module filters incoming data and forward the matching data to its output.	logic	×	×	×	×	✓	
Filter :: Remove filter	Reset filtering	logic	×	×	×	×	×	
IF :: Generic	Generic IF / ELSE condition block. The `then` output will be used if the encoded conditions is satisfied, otherwise the `else` output will be used.	logic	×	×	×	×	✓	
IF :: Organisation	Organisation IF / ELSE condition block. The `then` output will be used if the encoded conditions is satisfied, otherwise the `else` output will be used.	logic	×	✓	×	×	×	
IF :: Published	Published IF / ELSE condition block. The `then` output will be used if the encoded conditions is satisfied, otherwise the `else` output will be used.	logic	×	✓	×	×	×	
IF :: Tag	Tag IF / ELSE condition block. The `then` output will be used if the encoded conditions is satisfied, otherwise the `else` output will be used.	logic	×	✓	×	×	✓	
IF :: Threat Level	Threat Level IF / ELSE condition block. The `then` output will be used if the encoded conditions is satisfied, otherwise the `else` output will be used.	logic	×	×	×	×	✓	

TLP:CLEAR

Ações disponíveis (actions modules)

All | Action | Logic | misp-module | Custom | Blocking | Enabled | Disabled

Enter value to search | Filter

Module name	Description	Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions
Attribute comment operation	Set the Attribute's comment to the selected value	action	×	✓	×	×	✓	
Event distribution operation	Set the Event's distribution to the selected level	action	×	✓	×	×	✓	
Add Event Blocklist entry	Create a new entry in the Event blocklist table	action	×	✓	×	×	✓	
Add to warninglist	Append attributes to an active custom warninglist.	action	×	✓	×	×	✓	
Assign country	Add or remove country Galaxy Cluster based on provided data	action	×	✓	×	×	×	
Attach enrichment	Attach selected enrichment result to Attributes.	action	×	✓	×	×	×	
Attach warninglist	Attach selected warninglist result.	action	×	✓	×	×	×	
Attribute edition operation	Base module allowing to modify attribute	action	×	✓	×	×	×	
Attribute IDS Flag operation	Toggle or remove the IDS flag on selected attributes.	action	×	✓	×	×	×	
Blueprint action module	Lorem ipsum dolor, sit amet consectetur adipisicing elit.	action	×	×	×	✓	×	
Enrich Event	Enrich all Attributes contained in the Event with the provided module.	action	×	✓	×	×	×	
mattermost	Simplistic module to send message to a Mattermost channel.	action	×	×	✓	×	×	
MS Teams Webhook	Perform callbacks to the MS Teams webhook provided by the "Incoming Webhook" connector	action	×	×	×	×	×	
Publish Event	Publish an Event in the context of the workflow	action	×	×	×	×	✓	
Push to ZMQ	Push to the ZMQ channel	action	×	×	×	×	×	
Send Log Mail	Allow to send a Mail to a list or recipients, based on a Log trigger. Requires functional misp-modules to be functional.	action	×	×	×	×	✓	
Send Mail	Allow to send a Mail to a list or recipients. Requires functional misp-modules to be functional.	action	×	×	×	×	✓	
slack	Simplistic module to send messages to a Slack channel.	action	×	×	✓	×	×	
Splunk HEC export	Export Event Data to Splunk HTTP Event Collector. Due to the potential high amount of requests, it's recommanded to put this module after a `concurrent_task` logic module.	action	×	✓	×	×	×	
Stop execution	Essentially stops the execution for blocking workflows. Do nothing for non-blocking ones	action	✓	×	×	×	✓	
Tag operation	Add or remove tags on Event or Attributes.	action	×	✓	×	×	✓	
Tag Replacement Generic	Attach a tag, or substitue a tag by another	action	×	✓	×	×	×	
Tag Replacement - PAP	Attach a tag (or substitue) a tag by another for the PAP taxonomy	action	×	✓	×	×	✓	
Tag Replacement - TLP	Attach a tag (or substitue) a tag by another for the TLP taxonomy	action	×	✓	×	×	✓	
Telegram Send Alert	Send a message alert to a Telegram channel	action	×	×	×	×	×	
testaction	This module is merely a test, always returning true. Triggers on event publishing.	action	×	×	✓	×	×	
Webhook	Allow to perform custom callbacks to the provided URL	action	×	×	×	×	×	

Workflows na prática

Exemplo A

Não permitir publicação de eventos com:

- `distribution` **`is NOT`** `your organization only`
- `tag` **`==`** `TLP:RED`

Exemplo B

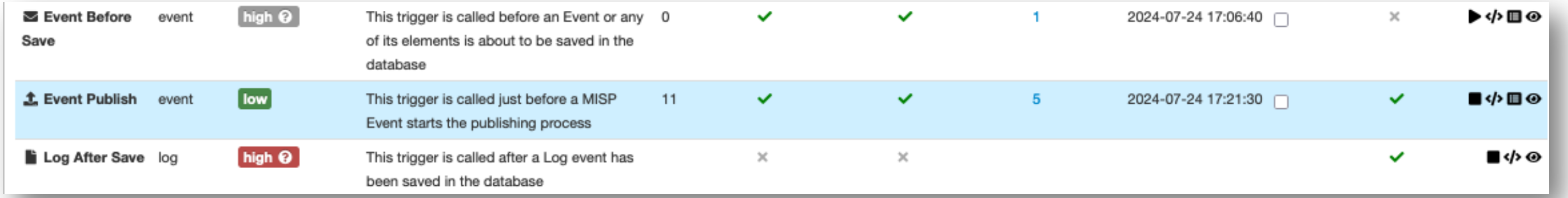
Remover flag **`IDS`** para todos atributos:

- do tipo **`datetime`**
- não afetar outros tipos

Exemplo A (1/6)

– Clique em **`Administration – Workflows`**

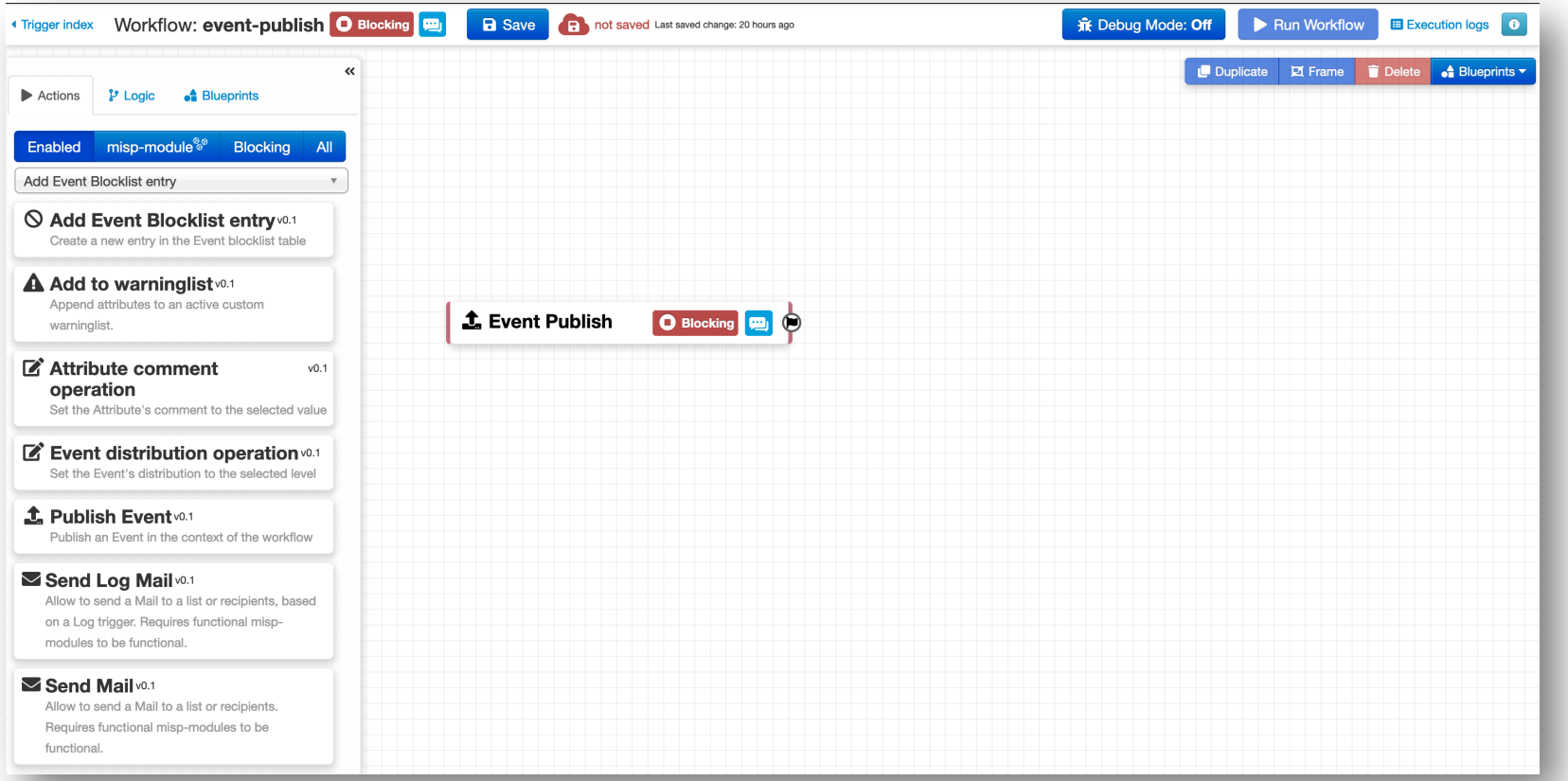
– Na janela **`Triggers`**, localize o trigger **`Event Publish`** e dê dois clique em cima dele:



Event Before Save	event	high	This trigger is called before an Event or any of its elements is about to be saved in the database	0	✓	✓	1	2024-07-24 17:06:40	✗
Event Publish	event	low	This trigger is called just before a MISP Event starts the publishing process	11	✓	✓	5	2024-07-24 17:21:30	✓
Log After Save	log	high	This trigger is called after a Log event has been saved in the database		✗	✗			✓

Exemplo A (2/6)

O editor de workflows será aberto:

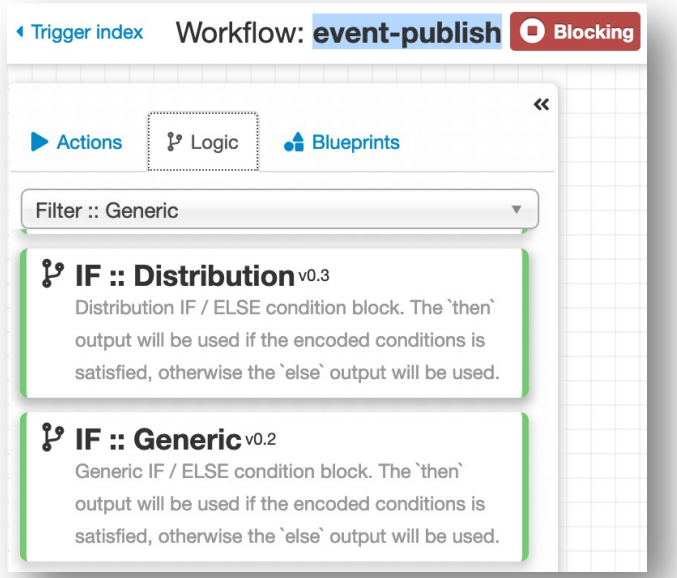


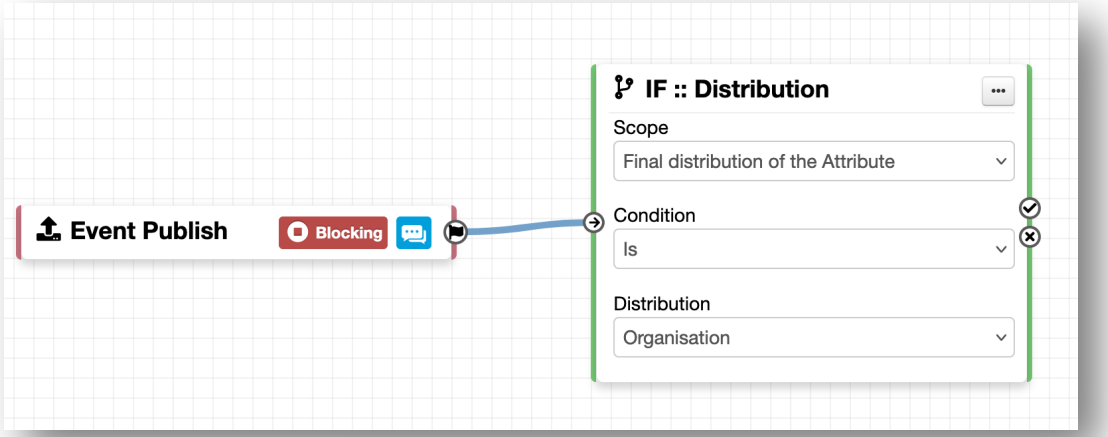
Exemplo A (3/6)

– Na janela **`editor de workflow`**, no menu de escolha de módulos, clique em **`Logic`** e procure pelo módulo **`IF :: Distribution`**

– Clique e arraste para o centro do editor, deixando ao lado do trigger **`Event Publish`**

– Clique na bandeira preta do trigger **`Event Publish`** e arraste para a seta do módulo **`IF :: Distribution`**

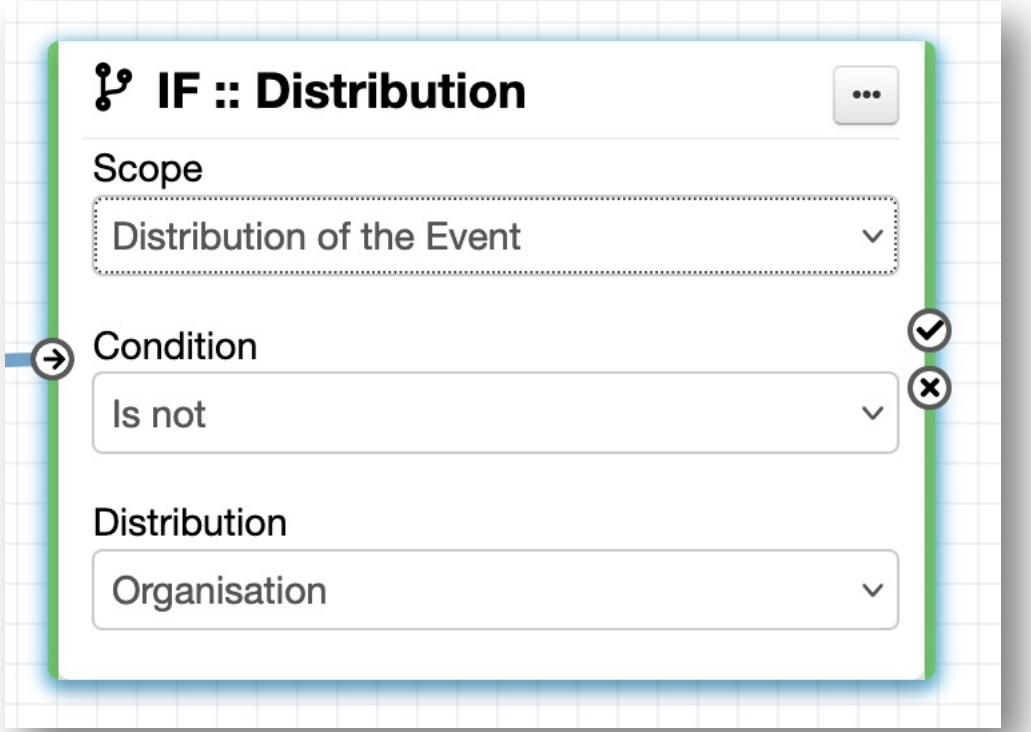




Exemplo A (4/6)

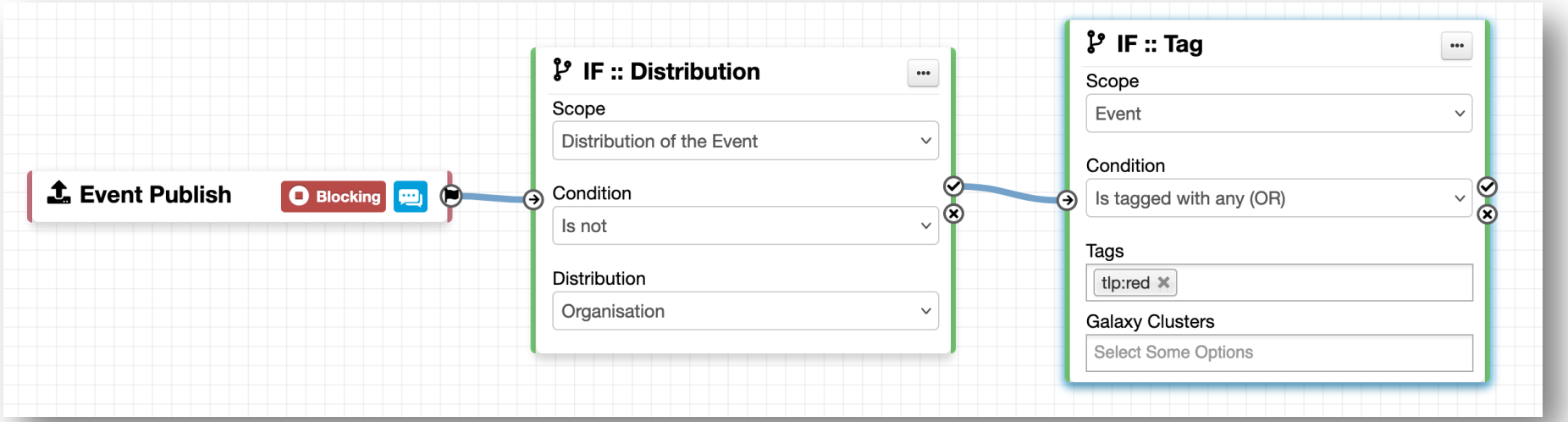
– Configure o módulo **`IF :: Distribution`** para ficar da seguinte forma:

- Scope – **`Distribution of the Event`**
- Condition – **`Is not`**
- Distribution - **`Organisation`**



Exemplo A (5/6)

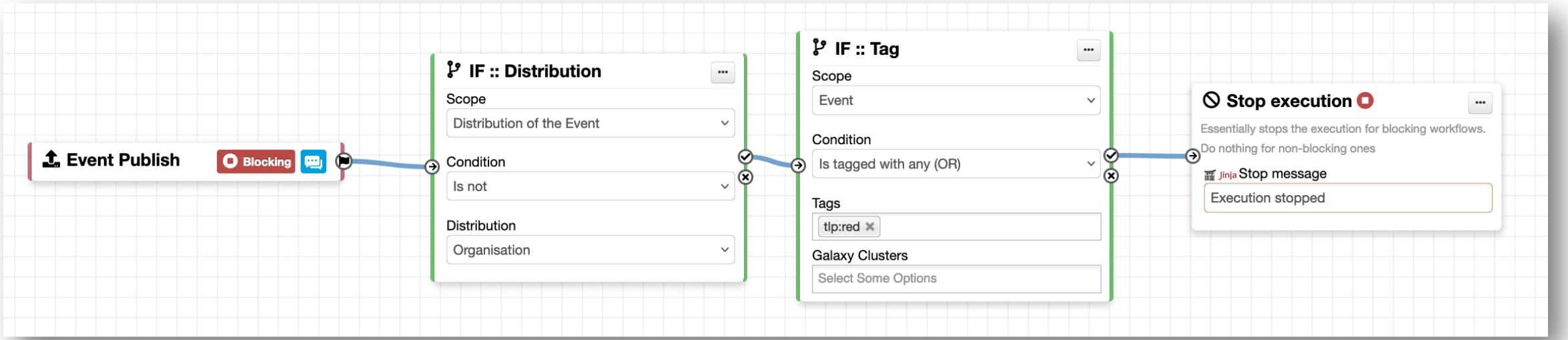
- No menu de escolha de módulos, ainda na opção **`Logic`**, escolha o módulo **`IF :: Tag`** e arraste para o **`editor de workflow`**
- No módulo **`IF :: Distribution`**, clique no ícone que representa **`condition satisfied`** e conecte na entrada do módulo **`IF :: Tag`**
- Configure o módulo **`IF :: Tag`** da seguinte forma:
  - Scope – **`Event`**
  - Condition – **`Is tagged with any (OR)`**
  - Tags: **`tlp:red`**



Exemplo A (6/6)

– Por fim, no menu de escolha de módulos, selecione a opção **`Actions`**, escolha o módulo **`Stop execution`** e arraste para o **`editor de workflow`**

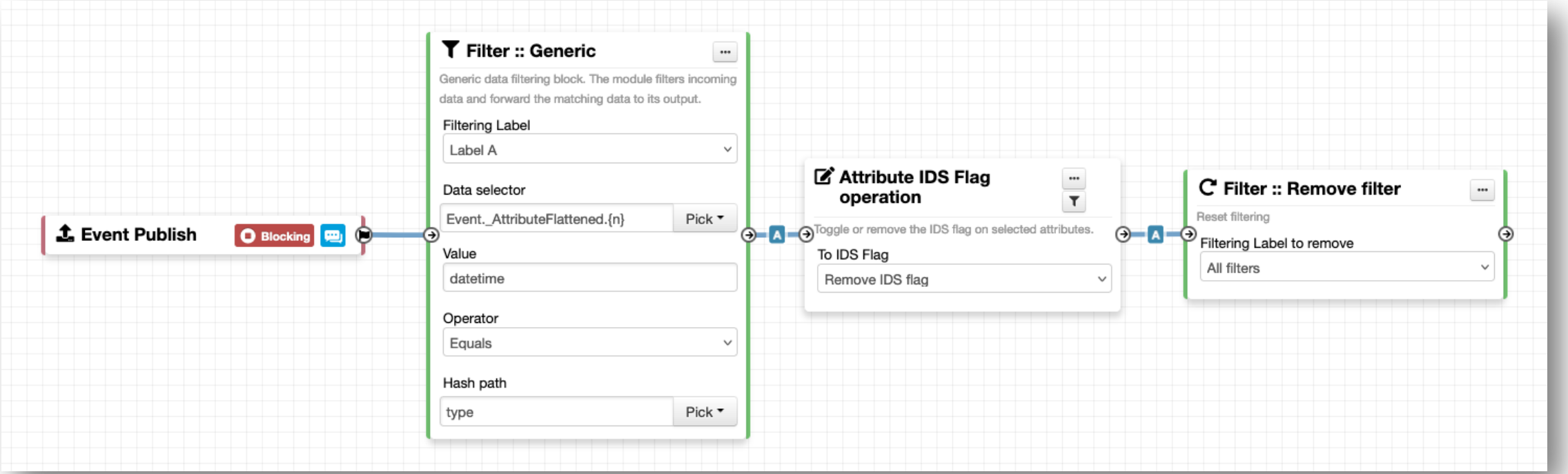
– No módulo **`IF :: Tag`**, clique no ícone que representa **`condition satisfied`** e conecte na entrada do módulo **`Stop execution`**



Exemplo B (1/4)

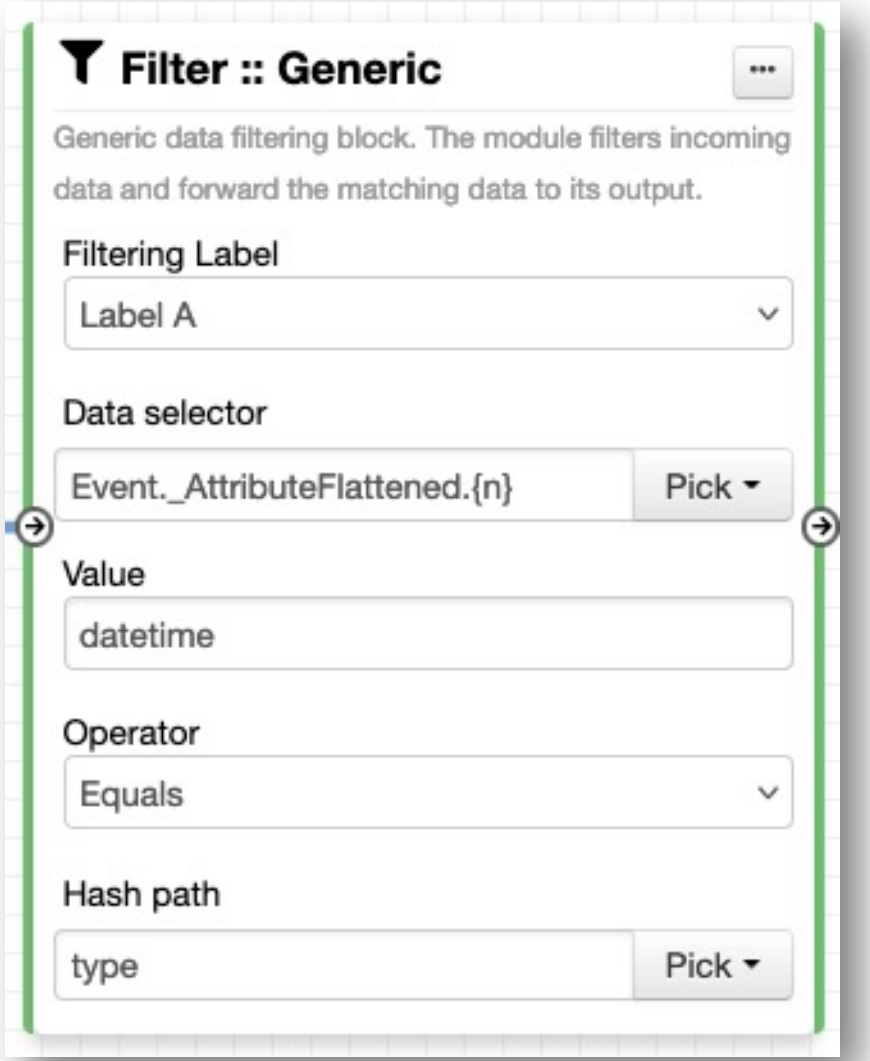
– Os seguintes módulos foram utilizados:

- `Filter :: Generic`
- `Attribute IDS Flag operation`
- `Filter :: Remove filter`



Exemplo B (2/4)

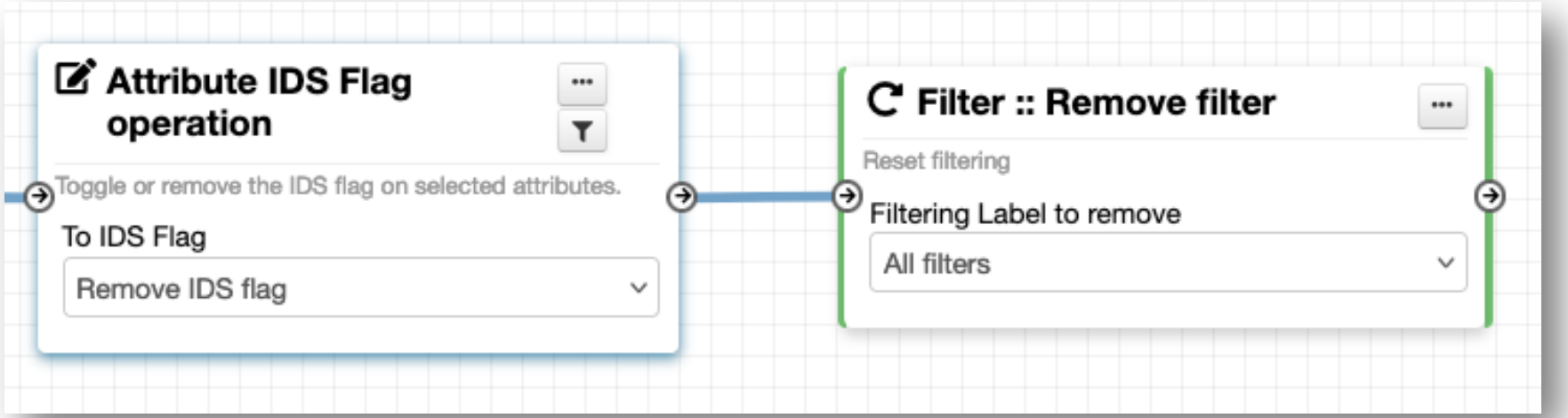
– Utilize o módulo **`Filter :: Generic`**
Permite filtrar dados que serão passados para uma ação
- Filtering Label – **`Label A`**
- Data selector – **`Event._AttibuteFlattened.{n}`** possibilita que todos os atributos sejam selecionados, mesmo se estiverem dentro de objetos
- Value – **`datetime`**
- Operator – **`Equals`**
- Hash path – **`type`**



Exemplo B (3/4)

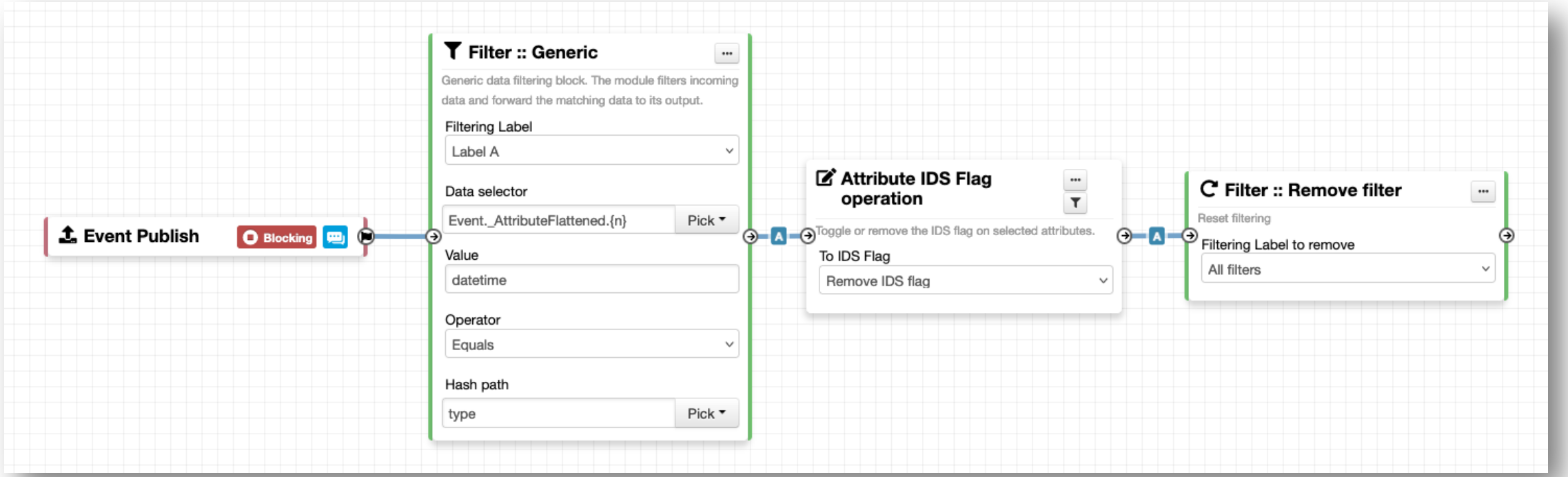
– Utilize o módulo **`Attribute IDS Flag operation`**
  - To IDS Flag – **`Remove IDS flag`**

– Utilize o módulo **`Filter :: Remove filter`**
  - Filtering Label to remove – **`All filters`**
    Remove os filtros utilizados no **`execution path`**, permitindo utilização de outros filtros posteriores



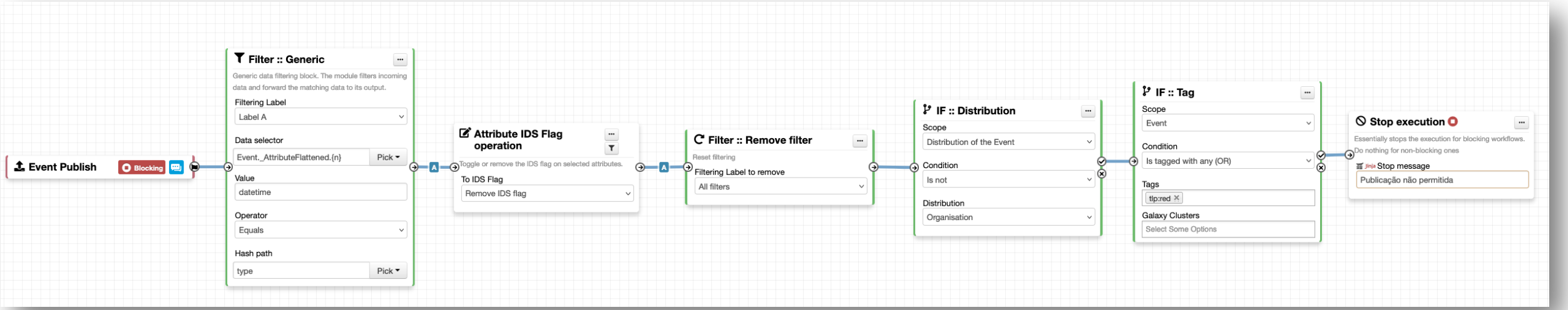
Exemplo B (4/4)

– Conecte todos os módulos e salve:



Encadeando os exemplos

Existe a possibilidade de encadear vários módulos, criando workflows mais complexos:



Referências para workflows

- https://www.misp-project.org/misp-training/a.12-misp-workflows.pdf
- https://www.misp-project.org/misp-training/handout/a.12-misp-workflows_handout.pdf
- https://www.youtube.com/watch?v=OyLE2g4zii0
- https://www.youtube.com/watch?v=BsggY7-X_6o

Q&A

cert.br nic.br cgi.br

Obrigado

@ marcus@cert.br

@ mhp@cert.br

@ Notificações para: cert@cert.br

𝕏 @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br