AN INTRODUCTION TO WORKFLOWS IN MISP

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP Project https://www.misp-project.org/

MISP PROJECT



An Introduction to Workflows in MISP

5

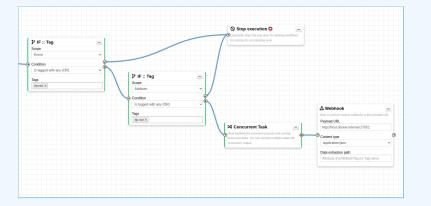
2024-04-

AN INTRODUCTION TO WORKFLOWS IN MISP MISP - THREAT SHARING CIRCL / TOAM MISP Project



CONTENT OF THE PRESENTATION

- MISP Workflows fundamentals
- Getting started
- Design of the system & how it can be extended



An Introduction to Workflows in MISP

Content of the presentation

CONTENT OF THE PRESENTATION

MISP Workflows fundamentals
 Getting started
 Design of the system & how it can be extended



5

2024-04

WHAT PROBLEMS ARE WE TRYING TO TACKLE

An Introduction to Workflows in MISP

└─What problems are we trying to tackle



- Prevent publication of events not meeting some criterias
 Prevent querying thrid-party services (e.g. virustotal) with
- sensitive information
 Send notifications in a chat rooms
- And much much more.

Workshop organized by the Canadian Cyber Cente



Initial idea came during GeekWeek7.5¹

Needs:

- Prevent default MISP behaviors
- Hook specific actions to run callbacks

Use-cases:

- Prevent publication of events not meeting some criterias
- Prevent querying thrid-party services (e.g. virustotal) with sensitive information
- Send notifications in a chat rooms
- And much much more..

¹Workshop organized by the Canadian Cyber Center

-04-15

2024-

WORKFLOW - FUNDAMENTALS

An Introduction to Workflows in MISP

2024-04-15

WORKFLOW - FUNDAMENTALS

SIMPLISTIC OVERVIEW OF A WORKFLOW IN ACTION

SIMPLISTIC OVERVIEW OF A WORKFLOW IN ACTION

An Introduction to Workflows in MISP 두 └─Workflow - Fundamentals

2024-

Simplistic overview of a Workflow in action

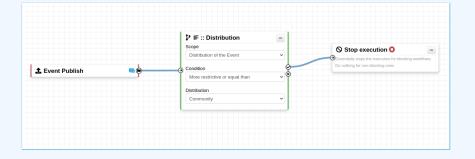
1. An action happens in MISP

- 2. If there is an enabled Workflow for that action, run it 3. If all went fine, MISP continue to perform the action
- au went nne, MISP continue to perform the action
 The operation can potentially be cancelled by himsking
 - operation can potentiatly be cancetted by block ules

- 1. An **action** happens in MISP
- 2. If there is an **enabled** Workflow for that **action**, run it
- 3. If all went fine, MISP continue to perform the action
 - The operation can potentially be cancelled by blocking modules

TERMINOLOGY

- workflow: Sequence of all operations (nodes) to be executed. Basically the whole graph.
- **execution path**: A path composed of nodes
- **trigger**: Starting point of a workflow. Triggers are called when specific actions happen in MISP
 - ► A trigger can only have one workflow and vice-versa



An Introduction to Workflows in MISP

└─ Terminology

15

2024

 workflow: Sequence of all operations (nodes) to be executed. Basically the whole graph. execution path. A path composed of nodes trigger: Starting point of a workflow. Triggers are called when specific actions happen in MISP A trigger can only have one workflow and vice-versa



WORKFLOW EXECUTION PROCESS

Typical execution process:

- 1. An action happens in MISP
- 2. The workflow associated to the trigger is ran
- 3. Execution result?
 - success: Continue the action
 - failure | blocked: Cancel the action

Example for Event publish:

- 1. An Event is about to be published
- 2. MISP executes the workflow listening to the event-publish trigger
 - **success**: Continue the publishing action
 - failure | blocked: Stop publishing and log the reason

An Introduction to Workflows in MISP

└─Workflow execution process

WORKFLOW EXECUTION PROCESS

ypical execution proces

- 1. An action happens in MISP
- 2. The workflow associated to the trigger is ra
- 5. Execution result?
- success: Continue the action
 failure | blocked: Cancel the action

Example for Event publis

- 1. An Event is about to be published
- MISP executes the workflow listening to event-publish trigger
 - success: Continue the publishing action
 failure | blocked: Stop publishing and log the reas

04-15

2024-

BLOCKING AND NON-BLOCKING WORKFLOWS

An Introduction to Workflows in MISP

2024-

Blocking and non-blocking Workflows

Currently 2 types of workflow

- Blocking: Completion of the action can be prevented
 If a blocking module blocks the action
- If a blocking module raises an exception
- Non-blocking: Workflow execution outcome has no impact b Blocking modules can still stop the execution

Currently 2 types of workflows:

- **Blocking**: Completion of the action can be prevented
 - ► If a **blocking module** blocks the action
 - ► If a **blocking module** raises an exception
- Non-blocking: Workflow execution outcome has no impact
 - **Blocking modules** can still stop the execution

EXECUTION CONTEXT

An Introduction to Workflows in MISP 2024-04-15 Workflow - Fundamentals

-Execution context

· Workflows can be triggered by any users Workflows can be triggered by actions done via the UI or API However, the user for which the workflow executes has: Ensures data is processed regardless of ownership and

- Workflows can be triggered by any users
- Workflows can be triggered by actions done via the **UI** or **API**
- However, the user for which the workflow executes has:
 - The site-admin permission
 - Is from the MISP.host_org_id
- Ensures data is processed regardless of ownership and access: no ACL

CLASSES OF WORKFLOW MODULES

Actions

3 classes of modules

- **action**: Allow to executes functions, callbacks or scripts
 - Can stop execution
 - e.g. Webhook, block the execution, perform enrichments, ...
- **logic**: Allow to redirect the execution flow.
 - IF condition, fork the blocking execution into a non-blocking one, ...
- **blueprint**: Allow to reuse composition of modules
 - Can save subworkflows and its module's configuration

An Introduction to Workflows in MISP

15

2024-0

└─Classes of Workflow modules

Actions	P Logic	el Blasprints	
3 classes of modules			
action: Allow to exec		ions, callbacks o	or scripts
 Can stop executio e.g. Webhook, blo 		ution perform er	richments
a logic: Allow to redire	ect the exe	cution flow.	
 IF condition, fork 	the blockin	g execution into a	non-blocki
one,			

Lueprint: Allow to reuse composition of modules
 Can save subworkflows and its module's configuration

SOURCES OF WORKFLOW MODULES

3 sources of action modules

Built-in **default** modules

- Part of the MISP codebase
- app/Model/WorkflowModules/action/[module_name].php

User-defined custom modules

- ► Written in PHP
- Can extend existing default modules
- Can use MISP's built-in functionalities (restsearch, enrichment, push to zmq, ...)
- **Faster and easier to implement new complex behaviors**
- app/Lib/WorkflowModules/action/[module_name].php

An Introduction to Workflows in MISP

4-15

C

2024-

└─Sources of Workflow modules

sources of action modules Built-in default modules

- Built-in default modules
 Built of the MISP codeb
- Part of the MISP codebase
 app/Nodel/WorkflowModules/action/[module_name]
- User-defined custom modules
 - Written in PHP
 - Can extend existing default modules
 Can use MISP's built-in functionalities (rest
 - enrichment, push to zmq, ...)
 - Faster and easier to implement new complex behaves a complex behaves a complex flow of the second sec

Sources of Workflow modules

3 sources of action modules

- Modules from the enrichment service
 - Default and custom modules
 - ► From the *misp-module* misp-module^{®®}
 - Written in Python
 - Can use any python libraries
 - New misp-module module type: action
 - \rightarrow Both the PHP and Python systems are plug-and-play

An Introduction to Workflows in MISP

└─Sources of Workflow modules



Both the PHP and Python systems are plug-and-play

2024-04-15

TRIGGERS CURRENTLY AVAILABLE

An Introduction to Workflows in MISP

└─Triggers currently available

urrent			ers can be hoo		g blo	king	ι	_	
	-	800	Particular Scalar des antimiser sonant						••••
a beistene bien	-		The tage is a fee (and only a propagate in party of a fee 3.4 ms	-			10+1+54		
A Real Property lies	-		The type is solve the article that has seen in						••••
i ben haden			The same is a first part of the a staff Concerns.						
a Real dia lass	~	000	Participants and other and they have been as only in the latter of the l						
A Real Property lies	-		The same is also also also also also also al				******		
the Workson		•	The tage is added to a set for the section in the section of the s						
	-		The lage A set of the						••••

Currently 8 triggers can be hooked. 3 being **blocking**.

		00				0				
Trigger name	Scope	Trigger overhead	Description	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Enabled	Actions
Attribute After Save	attribute	high 😧	This trigger is called after an Attribute has been saved in the database	58	×	~	160	2022-07-29 06:58:11	*	∎∲⊟©
* Enrichment Before Query	others	low	This trigger is called just before a query against the enrichment service is done	841	~	~	162	2022-07-29 08:32:32	*	∎⋪∎∅
Event After Save	event	medium 😧	This trigger is called after an Event has been saved in the database	11	×	×	175	2022-07-29 08:37:23	*	∎⋪∎∅
1 Event Publish	event	low	This trigger is called just before a MISP Event starts the publishing process	1	~	~	180	2022-07-29 12:14:10	~	∎⋪∎∅
& Object After Save	object	high 😧	This trigger is called after an Object has been saved in the database	35	×	~	161	2022-07-28 13:59:37	×	▶⋪∎∅
Post After Save	post	low	This trigger is called after a Post has been saved in the database	36	×	×	176	2022-07-28 13:59:51	*	∎⋪∎⊕
🎒 User After Save	user	low	This trigger is called after a user has been saved in the database	55	×	×	159	2022-07-28 14:00:03	*	∎⋪∎∅
≗ + User Before Save	user	low	This trigger is called just before a user is save in the database	42	~	×	158	2022-07-28 14:00:32	*	∎∲≣∅

04-15

2024

WORKFLOW - GETTING STARTED

An Introduction to Workflows in MISP

2024-04-15

WORKFLOW - GETTING STARTED

GETTING STARTED WITH WORKFLOWS (1)

Review MISP settings:

Make sure MISP.background_jobs is turned on
 Make sure workers are up-and-running and healthy
 Turn the setting Plugin.Workflow_enable on

Overview MI	SP settings (20 🛕)	Encryption set	tings (7 🛕) 🛛 Prox	y settings (5)	Security settings (8 \land)	Plugin settings (465 🕰)	SimpleBackgroundJobs settings (1	1 🗛) Di
Enrichment							Filter the table(s) below	
Import								
Export								
Action								
Critical	Plugin.Action_servic	es_enable	true	Enabl	e/disable the action service	15		
Recommended	Plugin.Action_servic	es_url	http://host.docker.i	nternal The u	rl used to access the action	services. By default, it is a	ccessible at http://127.0.0.1:6666	
Recommended	Plugin.Action_servic	es_port	6677	The p	ort used to access the activ	on services. By detault, it is	accessible at 127.0.0.1:6666	
Recommended	Plugin.Action_timeo	ut	10	Set a	timeout for the action servi	ces		Value not set.

4. [optional:misp-module] Turn the setting Plugin.Action_services_enable on

Overview	MISP settings (20 🛦)	Encryption settings (7 🛦)	Praxy settings (5)	Security settings (8 🛕)	Plugin settings (465 🛕)	SimpleBackgroundJobs settings (11 \Lambda)	Diagno
Enrichmen						Filter the table(s) below	
Import							
Export							
Action							
Cortex							
Sightings							
Workflow							
Recomme	nded Plugin.Workflow_er	nable	true Enable	aldisable workflow feature			

An Introduction to Workflows in MISP

15

2024-

 \Box Getting started with workflows (1)

1. Make s 2. Make s	are workers are	ground_jobsi up-and-running in.Workflow_o	and healt
	term of some time to be	is heavy? hereasts been	Contraction of the
4. footion	almisp-module	e] Turn the settin vices_enable	on on
Plugi	STREET, SQUARE, SQUARE		
Plugi	Concession in succession	(* heavy) haven't been	and the second s
Plugi	-	The local balances in the second	
Plugi	-		
Plugi	-		10.000
Plugi		r 🛊 - Kangalag (🛊 - Sangalag (🛊 - Sangalag (24.0000
Plugi		r 🛊 - Kangang (🛓 Sangang (🖢 Sangang	(1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.

GETTING STARTED WITH WORKFLOWS (2)

An Introduction to Workflows in MISP

04-15

2024-0

Getting started with workflows (2)

GETTING STARTED WITH WORKFLOWS (2)

f you wish to use action modules from misp-module, make use to have: The latest update of misp-module > There should be an action_mod module type in

misp-modules/misp_modules/modules
Restarted your misp-module application

is command should show all "action" modules arl == http://szy.co.st6666/modules | \ '.[] | select (.meta."module-type"]] | contains("action")) | met .mame, version: .meta.version]'

If you wish to use action modules from misp-module, make sure to have:

- The latest update of misp-module
 - There should be an action_mod module type in misp-modules/misp_modules/modules
- Restarted your misp-module application

1 # This command should show all 'action' modules
2 \$ curl -s http://127.0.0.1:6666/modules | \
3 jq '.[] | select(.meta."module-type"[] | contains("action")) |
4 {name: .name, version: .meta.version}'

GETTING STARTED WITH WORKFLOWS (3)

An Introduction to Workflows in MISP 두 └─Workflow - Getting started

Getting started with workflows (3)

- 1. Go to the list of modules
- Administration > Workflows > List Modules
- Make sure default modules are loaded
- 3. [optional:misp-module] Make sure misp-module module:
- are loaded

1. Go to the list of modules

- Administration > Workflows > List Modules
- or /workflows/moduleIndex
- 2. Make sure **default** modules are loaded
- 3. [optional:misp-module] Make sure **misp-module** modules are loaded

2024-

CREATING A WORKFLOW WITH THE EDITOR

- 1. Go to the list of triggers Administration > Workflows
- 2. Enable and edit a trigger from the list
- 3. Drag an action module from the side panel to the canvas
- From the trigger output, drag an arrow into the action's input (left side)
- 5. Execute the action that would run the trigger and observe the effect!

Trigger name	Scope	Trigger overhead	Description	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Enabled	Actions
C Attribute After Save	atribute	high 0	This trigger is called after an Attribute has been saved in the database	58	×	×	160	2022-07-29 06:58:11	*	•••••
* Enrichment Before Query	others	kow	This trigger is called just before a query against the enrichment service is done	841	*	~	162	2022-07-29 08:32:32	*	∎∲≣⊚
Event After Save	event	medium	This trigger is called after an Event has been saved in the database	11	×	×	175	2022-07-29 08:37:23	*	■\$0
1 Event Publish	event	kow	This trigger is called just before a MISP Event starts the publishing process	1	*	~	180	2022-07-29 12:14:10	*	■\$
& Object After Save	object	high 0	This trigger is called after an Object has been saved in the database	35	×	~	161	2022-07-28 13:59:37	×	▶ \$ ₽∎€
Post After Save	post	kow	This trigger is called after a Post has been saved in the database	36	×	×	176	2022-07-28 13:59:51	×	•\$\$
🎝 User After Save	user	law	This trigger is called after a user has been saved in the database	55	×	×	159	2022-07-28 14:00:03	*	∎¢∎⊛
A* User Before Save	user	low	This trigger is called just before a user is save in the database	42	×	×	150	2022-07-28 14:00:32	*	•\$



An Introduction to Workflows in MISP

04-15

2024-

Creating a workflow with the editor

	rigg	n module fr ger output,						
cute the	act	ion that wo	ulo	l ru	n the	triș	ger ai	nd o
	-							100

	-							1000
\$1900 PR	-							
		NAME AND ADDRESS OF TAXABLE PARTY.						

WORKING WITH THE EDITOR

Operations not allowed:

- Execution loop are not authorized
 - Current caveat: If an action re-run the workflow in any way



An Introduction to Workflows in MISP

04-15

2024-

└─Working with the editor

WORKING WITH THE EDITOR

Operations not allowed: Execution loop are not authorized Current careat- if an action remon the workflow in any way



WORKING WITH THE EDITOR

An Introduction to Workflows in MISP 두 └─Workflow - Getting started

└─Working with the editor

WORKING WITH THE EDITOR

Operations not allowed: Multiple connections from the same output

Securities order output and confinition for unon



Operations not allowed:

- Multiple connections from the same output
 - **•** Execution order not guaranted and confusing for users



2024-

WORKING WITH THE EDITOR

An Introduction to Workflows in MISP

└─Working with the editor



Deprations showing a warning: Blocking modules after a concurrent tasks module Blocking modules in a non-blocking workflow

	 H Concerned Task	 O line security O	
********	 And and the Art of the second second	 Scaling is an including one	

Operations showing a warning:

- Blocking modules after a concurrent tasks module
- **Blocking** modules in a **non-blocking** workflow

		Concurrent Task	Stop execution O
Event Publish	O Blocking 🥅 🖗	Allow breaking the execution process and running concurrent tasks. You can connect multiple nodes the 'concurrent' output.	Essentially stops the execution for blocking workflows. Do nothing for non-blocking ones

2024-04-15

WORKFLOW BLUEPRINTS

Blueprints allow to **re-use parts** of a workflow in another one
 Blueprints can be saved, exported and **shared**

Debugging webhook	v1656059209
Default: ×	
Blueprint Content: 1 node	
Webhook module pre-configured for del purposes	bugging

Blueprints origins:

- From the "official" misp-workflow-blueprints repository
- 2. Created or imported by users

An Introduction to Workflows in MISP

└─Workflow blueprints

2024-04-15

Debugging webhook	+1000000
Defail: #	
Ekseptet Contest: Lande	
A 1	
Intelligion mediale pre-configured for delarg	

WORKFLOW BLUEPRINTS: CREATE

Select one or more modules to be saved as blueprint then click on the save blueprint button

Trigger index Workflow: publis!	Save Save Saved Last saved tharps 15 days ago		
Actions PLogic Bueprint Since Blueprint Workflow part 1	Add Workflow Blueprint	×	Cupicate Dobte A Bioprete •
Workflow part 1 clitteel discent ame statisticate Biogram Content: 3 modes 0 1 0 2 Test	Name of the workflow blueprint Description Concise description of the workflow blueprint		
Workflow part 2 with a super long text addulate text 40% and 6 accounts Bulkepric Contents 7 modes ************************************	Parallel Task		Profile a DPC (P) Text on the second
Debugging webhook stillstorert-aksi dial-bloktzeadit Buegens Cortent: 1 node i 1 Vichhock module pre-configured for debug purposes			
part3 Process the effective objective objective Blueprint Cortent: 2 modes Disprint Cortent: 2 modes tot Mattermost module	a las film a las promotos bas por motos bas por motos bas por motos bas film a las film		
Mattermost module configuration edute-kase-4034616 ketzets170x0 Blueprint Content: 1 node	Submit	Cancel	

An Introduction to Workflows in MISP

04-15

2024

└─Workflow blueprints: Create

WORKFLOW BLUEPRINTS: CREATE

Select one or more modules to be saved as blueprint then click on the save blueprint button



20

HASH PATH FILTERING

Some modules have the possibility to filter or check conditions using CakePHP's path expression.

```
1 $path_expression = '{n}[name=fred].id';
2 $users = [
3 {'id': 123, 'name': 'fred', 'surname': 'bloggs'},
4 {'id': 245, 'name': 'fred', 'surname': 'smith'},
5 {'id': 356, 'name': 'joe', 'surname': 'smith'},
6 ];
7 $ids = Hash::extract($users, $path_expression);
8 // => $ids will be [123, 245]
```



```
2024-04-15
```

An Introduction to Workflows in MISP

└─ Hash path filtering

	dules have the possibility to filter or check s using CakePHP's path expression.
2 Susers + [3 ['id': 12] 4 ['id': 24] 5 ['id': 350 6]:	<pre>as = '(n)[nemestred].id'; , 'nemes': 'fred', 'surrames': 'bioggs'], , 'nemes': 'rice', 'surrames': 'smith'], , 'nemes': 'lice', 'surrames': 'smith'], atract(Suren, Spath-spression);</pre>
	PF::deseric in two

MODULE FILTERING

Some action modules accept filtering conditions
 E.g. the enrich-event module will only perform the enrichment on Attributes having a tlp:white Tag

Module Filtering	:	×
Element selector		
Attribute.{n}		
Value		
tlp:white		
Operator		
In	`	-
Hash Path		
AttributeTag.{n}.Tag.name		
	Save Close	

2024-04-15

An Introduction to Workflows in MISP

└─Module filtering

Module Filtering	
Enners alledar	
ALL DOCUMENTS OF THE DOCUMENTS	
Value	
By affile	
faunty	
in the second se	
100.000	
Ambus has being bill tag same	

DATA FORMAT IN WORKFLOWS



- All triggers will inject data in a workflow
- In some cases, there is no format (e.g. User after-save)
- In others, the format is **compliant with the MISP Core format**
- In addition to the RFC, the passed data has additional properties
 - Attributes are always encapsulated in the Event or Object
 - Additional key _AttributeFlattened
 - Additional key _allTags
 - Additional key inherited for Tags

An Introduction to Workflows in MISP

2024-04-15

L Data format in Workflows

DATA FORMAT IN WORKFLOWS



 All triggers will inject data in a workflow
 In some cases, there is no format (e.g. User after-save)
 In others, the format is compliant with the MISP Core for
 In addition to the RPC, the passed data has additional properties
 Attributes are always encapsulated in the Event Object
 Attributes are always encapsulated in the Event of Object

LOGIC MODULE: CONCURRENT TASK

- Special type of logic module allowing multiple connections
 Allows breaking the execution flow into a concurrent tasks to be executed later on by a background worker
- As a side effect, blocking modules cannot cancel ongoing operations



04-15 2024-

An Introduction to Workflows in MISP

Logic module: Concurrent Task

LOGIC MODULE: CONCURRENT TAS

 Special type of logic module allowing multiple connections
 Allows breaking the execution flow into a concurrent tasks to be executed later on by a background worker
 As a side effect, blocking modules cannot cancel ongoing operations



DEBUGGING WORKFLOWS: LOG ENTRIES

Workflow execution is logged in the application logs:

- /admin/logs/index
- Or stored on disk in the following file:
 - /app/tmp/logs/workflow-execution.log
- Use the webhook-listener.py tool
 - /app/tools/misp-workflows/webhook-listener.py

Logs		»					
Email	s Authen	ication issue	es MISP Update res	ults Setti	ng changes	Warnings and e	rrors
id †	Email	Org	Created	Model	Model ID	Action	Title
49146	SYSTEM	SYSTEM	2022-08-01 07:34:40	Workflow	162	execute_workflow	Finished executing workflow for trigger `enrichment-before-query` (162). Outcome: success
49144	SYSTEM	SYSTEM	2022-08-01 07:34:39	Workflow	162	execute_workflow	Started executing workflow for trigger 'enrichment-before-query' (162)

An Introduction to Workflows in MISP

4-15

2024-

Lebugging Workflows: Log Entries

							in the application logs:
		· /a		igs/		ex	
	Or	stor	ed on di	ŵ ii	s the	e follos	ving file:
							w-execution.log
							. py tool
	•						lows/webhook-listener.p
Log	•						
Log	•	/a					
Log	•	/a					
Log	•	/a					
Log	-	- /a	pp/tool	.s/#	isp	workf	lows/webhook-listener.p
Log	5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	- /a		s/8	isp	workf	

DEBUGGING WORKFLOWS: DEBUG MODE



n Debug Mode: On can be turned on for each workflows

- Each nodes will send data to the provided URL
 - Configure the setting: Plugin.Workflow debug url
- Result can be visualized in
 - offline: tools/misp-workflows/webhook-listener.py
 - **online**: requestbin.com or similar websites

LIVE	PAUSE	Q Type to search
Today		
2:25:10 pm	POST	/end?outcome=blocked
2:25:09 pm	POST	<pre>/exec/stop-execution?result=success</pre>
2:25:09 pm	POST	<pre>/exec/tag-if?result=success</pre>
2:25:08 pm	POST	/init?type=blocking

An Introduction to Workflows in MISP Workflow - Getting started

04-15

2024-

-Debugging Workflows: Debug mode

	G Wo			
Each no Cont Result c F offii	des wi Igure 1 In be Ne: to Ne: re	ll sen he se visua pls/n quest	can be turned on for each wo id data to the provided URL tting: Plugin.workflow_dob lized in nisp-workflows/webhook-1 bin.com or similar websites Direction.	ug_url
	Teday			
	111-11-1	POST	/end/textreme-blocked	
	1.11.10.00	POST	/ener/stage execution/vesafilesaccess	
	11111	POST	/exec/tag-iffrend/t-saccess	
	111.00.00	P951	/inititype-blocking	

LEARNING BY EXAMPLES

An Introduction to Workflows in MISP

LEARNING BY EXAMPLES

WORKFLOW EXAMPLE 1

An Introduction to Workflows in MISP 두 └─Learning by examples

└─Workflow example 1

2024-0

	277.5%		
	har	21mm 20	
Liters Polish .			

 The Event-Publish trigger uses the MISP core format
 The IF::Tag module checks if at least one of the Attribute has the tlp::hite tag
 If it does, the Push-to-ZNQ module will be executed



- 1. The Event-Publish trigger uses the MISP core format
- 2. The IF::Tag module checks if at least one of the Attribute has the tlp:white tag
- 3. If it does, the Push-to-ZMQ module will be executed

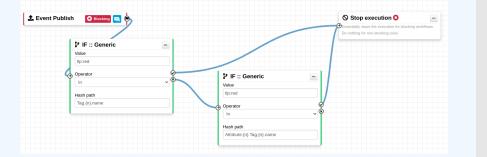
WORKFLOW EXAMPLE 2

An Introduction to Workflows in MISP 2024-04-15 -Learning by examples

-Workflow example 2







■ If an event has the tlp:red tag or any of the attribute has it, the publish process will be cancelled

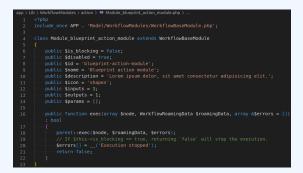
EXTENDING THE SYSTEM

An Introduction to Workflows in MISP

2024-04-15

EXTENDING THE SYSTEM

CREATING A NEW MODULE IN PHP



- app/Lib/WorkflowModules/action/[module_name].php
- Module configuration are defined as public variables
- The exec function has to be implemented.
 - ► If it returns **true**, execution will proceed
 - If it returns false
 - And the module is blocking, the execution will stop and the operation will be blocked

An Introduction to Workflows in MISP

04-15

2024-

└─Creating a new module in PHP

ł	
ł.	

 app/Lib/WorkflowModules/action/[module_name].php Module configuration are defined as public variables The exec function has to be implemented. If it returns true, execution will proceed If it returns false A of the module is blocking, the execution will step and the

29

CREATING A NEW MODULE IN PYTHON

23 # Boolean is used to simply signal that the execution has finished. 24 # For blocking modules the actual boolean value determines whether we break execution
24 # for brocking modules the actual borean value betermines whether we break execution 25 returns = 'boolean'
26 27 moduleinfo = {'version': '0.1', 'author': 'Andras Iklody',
27 modulemno = { version : 0.1 ; autor : Amonas incory a 28 hockedeedeed 'description': "This module is merely a test, always returning true. Triggers on event publishing.".
20 control of the stription is into module is merely a test, atways returning true. Higgers on event publishing, p 29 control of the stription is into module is merely a test, atways returning true. Higgers on event publishing, p
32 def-handler(q-False):
33 voi finance (q. 1929)
34 ····································
35 ··· result ison.loads(q) ·#>noga
36] ··· output = result - insert - your magic here!
37 ····································
<pre>41 > def introspection(); -</pre>
64

 Module configuration are defined in the moduleinfo and moduleconfig variables
 The handler function has to be implemented.

Blocking logic is the same as other modules

An Introduction to Workflows in MISP

└─Creating a new module in Python

	and a spenning statement and a second of statement of statements a
	And a second s
	Consignation of the second state of the second
111111	All and a second
	I mention photo, that he and the second of the dust of advantation and a sub-second
	Annue - Ann - Annue -
1	And the second s
- 1	
	and I have been a set of the set

 Module configuration are defined in the module info and module config variables
 The handler function has to be implemented.
 Blocking logic is the same as other modules

04-15

2024-0