

# CyCAT

The Cybersecurity Resource Catalogue

**Lightning Talk. Alexandre Dulaunoy, Saâd Kadhi**

13th CSIRTs Network Meeting - 3 March 2021

TLP:WHITE



# CyCAT?

What, Who, Why





# Welcome to the jungle

- Cyberattacks are continuously **increasing**, in number, complexity and variety
- To defend their constituencies, defenders have launched **several** initiatives
- **Numerous** tools, products, frameworks and methodologies to prevent, detect and respond to these threats
- **Not always properly tested, not always easy to locate**, produced in a highly decentralised fashion
- And the **rhythm is accelerating**
- With little consideration to **prior art** (mainly due to lack of knowledge?)

# Where should I start?

- I need to defend my constituency
- What tools, rules, playbooks, controls,... exist out there?
- Which ones are the **most relevant** for my context & for my current maturity?
- Which ones **work best** for my needs?
- Which ones have been **sufficiently tested**?
- Which ones supersede, augment or **conflict with** existing ones?
- Which 'resource producers' tend to make **quality** products for my needs?

# Enters CyCAT

- CyCAT = **CY**bersecurity Resource **CAT**alogue
- **Non-profit** initiative trying to solve a (cyber)age-old problem
- **Map + document**, in a single formalism, and **catalogue** all the available...
- Cybersecurity tools, rules, playbooks, controls...
- **Contextualised** to facilitate searching and selection
- Resource interlinking to support the creation of coherent 'packages'
- 'Packages' = **plug-and-play** solutions for less-mature entities



# The CyCAT System

## High-level concepts





# CyCAT as a system

- **API**-backed website that can be fed, queried and **curated** by the community
- Building on the success of initiatives such as CVE and elegant solutions such as MISP's UUID
- Resource owners will be able to apply for their own **namespaces** within CyCAT and add their products (FOSS or commercial)
- Products will have their **UUID + metadata** (e.g. *stable/experimental, latest/deprecated, capability:memory-scan=experimental, capability:file-scan=stable*)
- Supported by a **taxonomy**

## Publisher namespace #

A publisher can be any organisation, project or individual requesting a publisher to CyCAT.

Field name	Description	Required
name	Name of the publisher (full name)	✓
short-name	Name of the publisher (short name)	✓
description	Description of the publisher	✓
cycat-oid	assigned CyCAT OID	✓
link	Internet link referencing the publisher	✓
timestamp	Last update of the publisher record (unix timestamp)	✓
maintainer	owner, external, cycat	-

Publisher examples: mitre, circl, misp

## Project namespace #

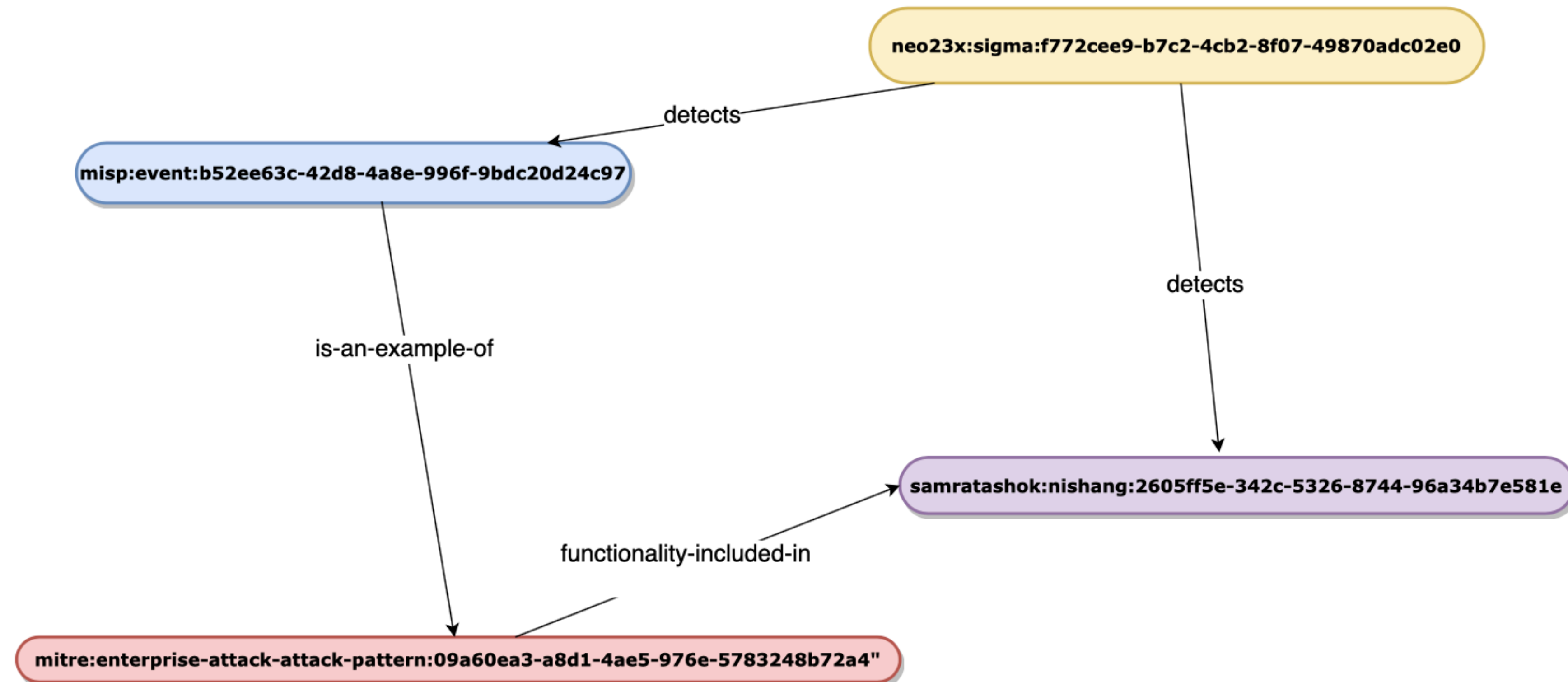
A publisher can request one or more project to CyCAT associated to the publisher namespace.

Field name	Description	Required
name	Name of the project (full name)	✓
short-name	Name of the project (short name)	✓
description	Description of the project	✓
cycat-oid	assigned CyCAT OID	✓
link	Internet link referencing the project	✓
license	License(s) of the project in SPX identifier (array)	✓
type	<a href="#">Taxonomy type</a> of the project from CyCAT taxonomy	✓
scope	<a href="#">Taxonomy scope</a> of the project from CyCAT taxonomy	✓
timestamp	Last update of the project record (unix timestamp)	✓
maintainer	owner, external, cycat	-



## URL example #

An CyCAT example with nishang, an offensive powershell #



```
% uuidgen --sha1 -n "690b3b43-d689-481c-aa61-5351963a36f2" -N "samratashok:nishang:"  
2605ff5e-342c-5326-8744-96a34b7e581e
```



# The Initiative

And why we need your help






# Current status and next steps

- CyCAT was launched on 1 February 2021
- By Freddy Dezeure, Alexandre Dulaunoy, Andras Iklody and Saâd Kadhi
- We received excellent suggestions and questions from key community contributors: Patrick Bareiss, John Lambert, Thomas Patzke, John Wunder, Daniil Yugoslavskiy...
- **Still open for initial feedback and peer review** until 31 March 2021
- Then we'll set out to build the alpha version of the system
- We expect to launch it during the next EU ATT&CK Community workshop, co-organised by Freddy Dezeure, CIRCL and CERT-EU, on 1 June 2021

# CyCAT needs you

- This is an **ambitious** project
- And 4 well-intentioned people won't be able to succeed...
- .. without your help and the help of the **community** they love and care for
- There are still many questions we need to address and some difficult problems we need to solve
- Publisher, defender, both? Read the White Paper, look at the taxonomy, go through the FAQ and **contribute**
- Got questions or suggestions?  [info@cycat.org](mailto:info@cycat.org)