Intro to MISP

James Acris

Capability: Threat Intelligence

- Threat Intelligence
  - Timely and relevant indicators that something weird is happening, so look out for it.
  - Can be both given and received.
  - Varies in granularity
- Takes the form of IOCs (indicators of compromise)
- In general, best threat intel comes from our community
- Much of it is untapped

Traditionally

- Threat intel comes in the form of:
  - Email from relevant sources
  - Advisories/reports from regulatory bodies, etc.
  - Public sources, e.g. news articles
- All sorts of formats
  - In order to hunt for these in your infrastructure, requires manual intervention.
- Need to sort through noise to find useful threat intel.

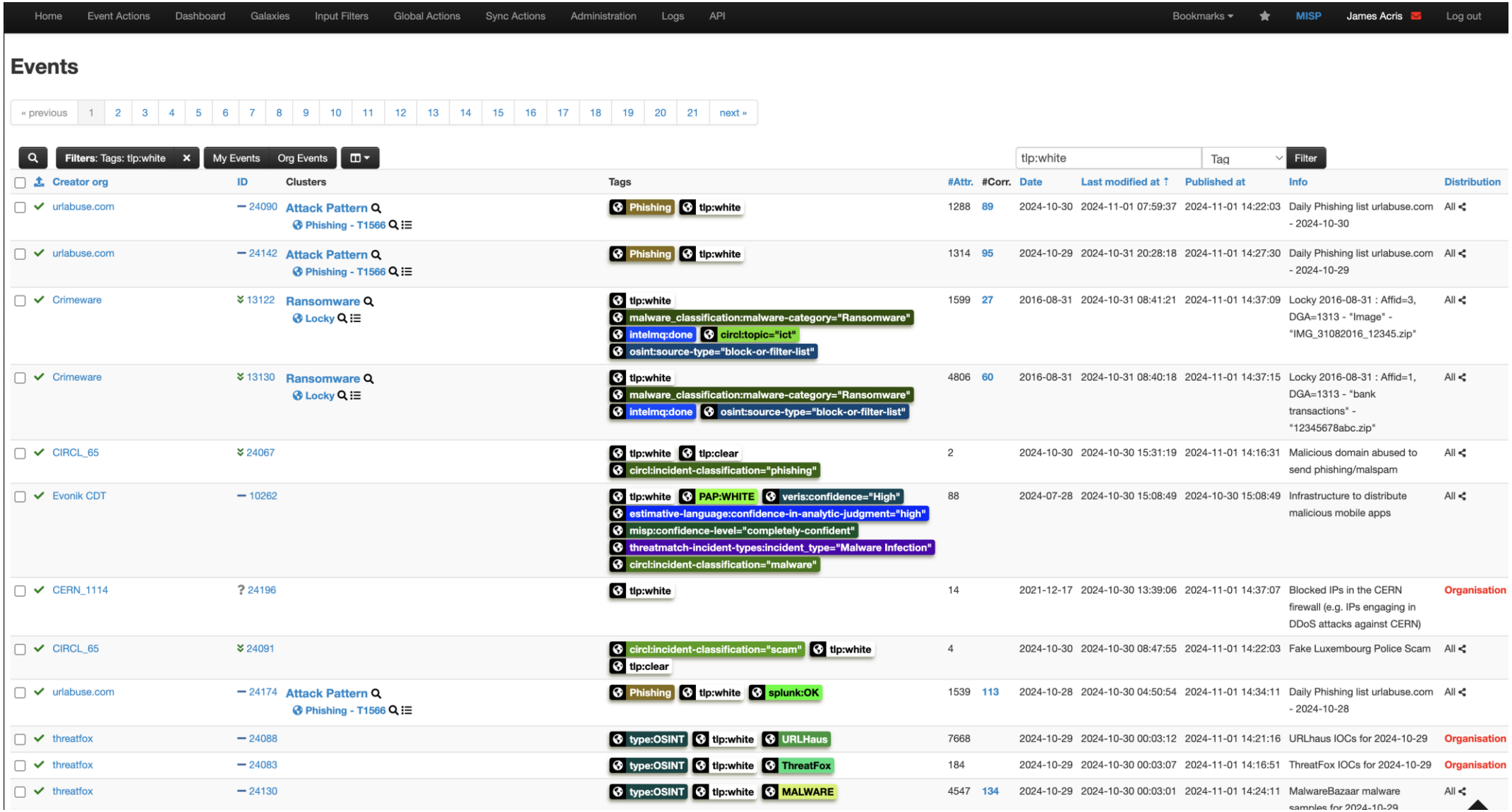
Why MISP?

- Automates much of this process
- All threat intel comes in the same format
- Can choose to receive threat intel from trusted, reliable, relevant sources
- Can interface with many tools (APIs, emails, python, CLI)
  - Including zeek

About MISP

- Developed by CIRCL (Luxembourg CSIRT) & others
- Used within our community
  - CERN
  - JISC
  - Grid sites

Science and Technology Facilities Council



Science and Technology Facilities Council

Daily Phishing list urlabuse.com - 2024-10-30

Event ID	24090
UUID	1d64a8e1-f566-4a63-81c7-2177f56c5120
Creator org	urlabuse.com
Protected Event (experimental)	Event is in unprotected mode.
Tags	Phishing tlp:white
Date	2024-10-30
Threat Level	Medium
Analysis	Ongoing
Distribution	All communities
Published	Yes 2024-11-01 14:22:03
#Attributes	1288 (429 Objects)
First recorded change	2024-10-30 09:14:08
Last change	2024-11-01 07:59:37
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Pivots | Galaxy | Event graph | Event timeline | Correlation graph | ATT&CK matrix | Event reports | Attributes | Discussion

24090: Daily Phishi...

Galaxies

Attack Pattern

Phishing - T1566

« previous 1 2 3 4 5 6 7 8 next » view all

Related Events

Order by date

- Daily Phishing list urlabuse.com - 2024-10-29 — 2024-10-29 — 9
- Phishing URL findings — 2024-10-29 — 1
- Phishing URL findings — 2024-10-28 — 1
- Daily Phishing list urlabuse.com - 2024-10-28 — 2024-10-28 — 7
- Daily Phishing list urlabuse.com - 2024-10-27 — 2024-10-27 — 2
- Daily Phishing list urlabuse.com - 2024-10-26 — 2024-10-26 — 2
- Daily Phishing list urlabuse.com - 2024-10-25 — 2024-10-25 — 4
- Daily Phishing list urlabuse.com - 2024-10-24 — 2024-10-24 — 3
- Daily Phishing list urlabuse.com - 2024-10-23 — 2024-10-23 — 4
- Daily Phishing list urlabuse.com - 2024-10-21 — 2024-10-21 — 2

Show (79 more)

Warning: Potential false positives (show)

Top 1000 website from Alexa

Scope toggle | Decay score | Context | Related Tags | Filtering tool | Expand all Objects | Collapse all Attributes

Enter value to search

Date	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions

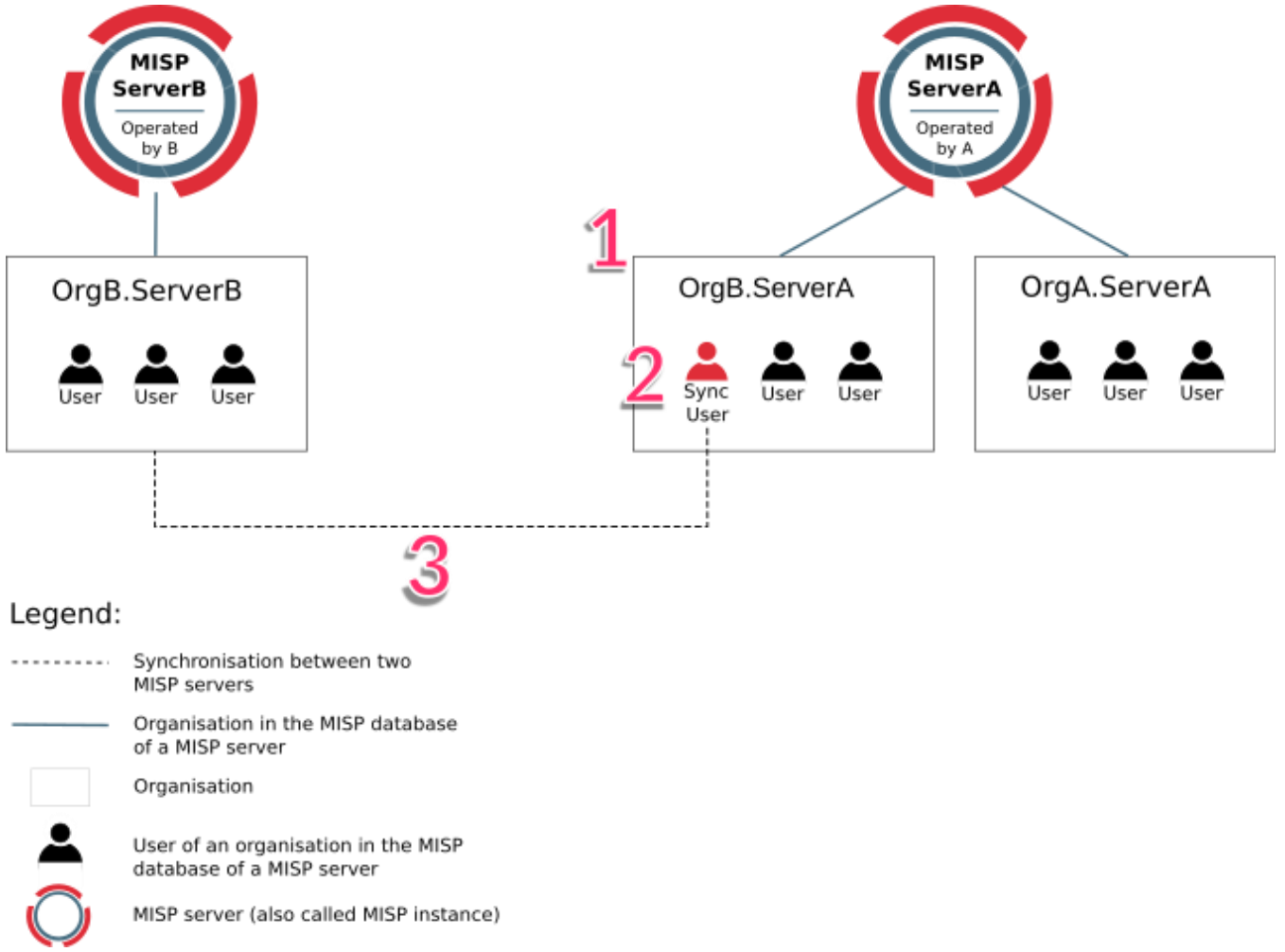
« previous | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | next » | view all

Scope toggle | Decay score | Context | Related Tags | Filtering tool | Expand all Objects | Collapse all Attributes | Enter value to search

Date	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2024-10-30	085...891	**Object name:** phishing **References:** 0		**hostname** :: hostname `lafrposter.xyz` Hide 4 Attributes			Phishing					Inherit			
2024-10-30	df6...fa1	Network activity	**hostname:** hostname	lafrposter.xyz	phishing:action="take-down"		Host name or IP address of the phishing attack	☑			☑	Inherit	(0/0/0)		
2024-10-30	eed...cd9	Network activity	**url:** url	http://lafrposter.xyz	phishing:action="take-down"		Source URL	☑			☑	Inherit	(0/0/0)		
2024-10-30	e80...86e	Other	**target:** text	La Poste			Target of the attack	☑	Too many correlations.		☐	Inherit	(0/0/0)		
2024-10-30	7bd...855	Other	**takedown-time:** datetime	2024-10-30T21:25:27.996737			domain deleted	☐			☐	Inherit	(0/0/0)		
2024-10-30	cb4...187	**Object name:** phishing **References:** 0		**hostname** :: hostname `worker-restless-shape-3288.hblaine.workers.dev` Hide 3 Attributes			Phishing					Inherit			
2024-10-30	995...fe5	Network activity	**hostname:** hostname	worker-restless-shape-3288.hblaine.workers.dev			Host name or IP address of the phishing attack	☑			☑	Inherit	(0/0/0)		
2024-10-30	95e...ddc	Network activity	**url:** url	http://worker-restless-shape-3288.hblaine.workers.dev			Source URL	☑			☑	Inherit	(0/0/0)		
2024-10-30	020...88f	Other	**target:** text	Microsoft			Target of the attack	☑	Too many correlations.		☐	Inherit	(0/0/0)		

Sharing in MISP

- Publicly available threat feeds
  - A good start but limited in relevance
- Syncs with other MISP servers
  - More relevant intel if from the community
- Distribution settings (set by publisher)
  - Your organisation only
  - This community only
  - Connected communities
  - All communities
  - Sharing group

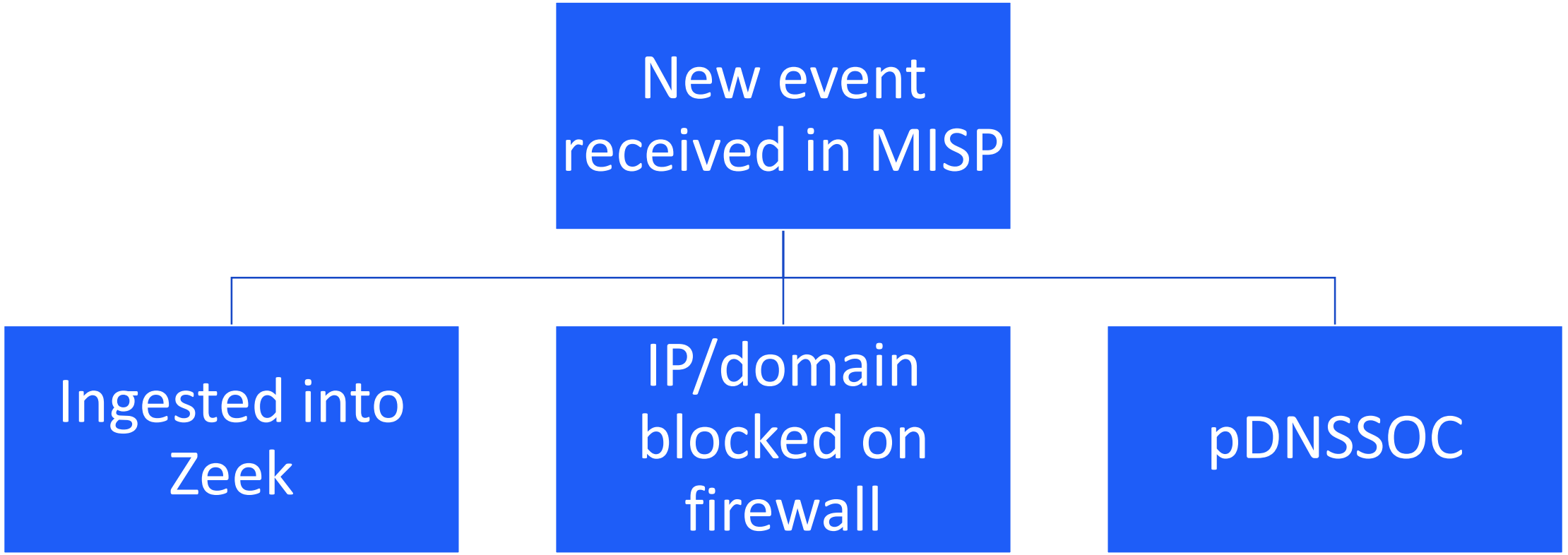


Science and Technology Facilities Council

Automation

- pDNSSOC
- Zeek IDS export
  - Can configure alerts within zeek if IOCs from MISP are found
- REST API
  - Built-in reference
- Export to JSON/XML

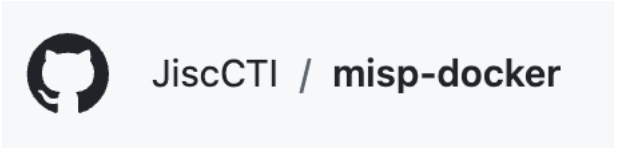
Use cases



Science and Technology Facilities Council

How to get started?

- Deploy your own
- JISC Docker deployment:
  - github.com/JiscCTI/misp-docker
  - Provides a great out-of-the box configuration
  - Easy to configure alternative Auth methods



Science and Technology Facilities Council

Science and Technology Facilities Council

Thank you

Facebook: Science and Technology Facilities Council

Twitter:@STFC_matters

YouTube: Science and Technology Facilities Council