MISP playbooks,
Proving the value of cyber threat intelligence and ICS-CSIRT.io

Hack.LU - Lightning Talks

cudeso.be
We Secure You
https://www.cudeso.be
koen.vanimpe@cudeso.be

TLP:CLEAR

Koen Van Impe

- **Freelancer**
  - Incident response, threat intelligence, security monitoring
- **Open source contributions**
  - MISP modules, taxonomies, automation and integration with DFIR tools, …
  - MISP “tip-of-the-week”
  - MISP-Playbooks
- **OSINT threat feed**
  - botvrij.eu

✉ koen.vanimpe@cudeso.be

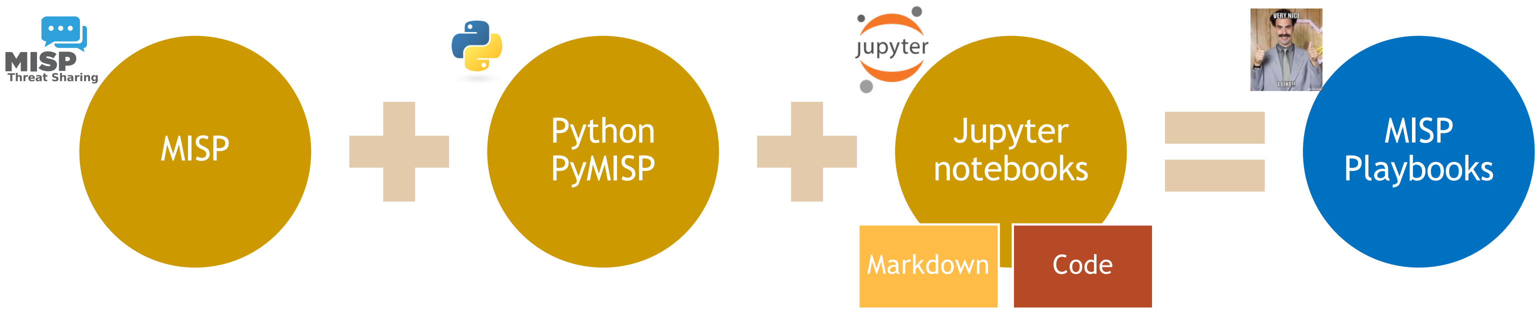
https://www.cudeso.be

https://www.vanimpe.eu

https://github.com/cudeso

MISP playbooks

https://github.com/misp/misp-playbooks



MISP playbooks address common use-cases encountered by **SOCs**, **CSIRTs** or **CTI** teams to detect, react and analyse specific intelligence received by MISP.

- The MISP playbooks are built with Jupyter notebooks and contain
  - **Documentation** in **Markdown** format, including text and graphical elements
  - **Computer code** in **Python**, primarily **PyMISP** to interact with MISP and other sources for enrichment and notification

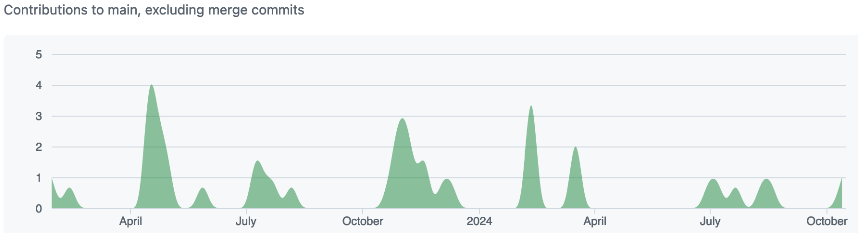
MISP playbooks

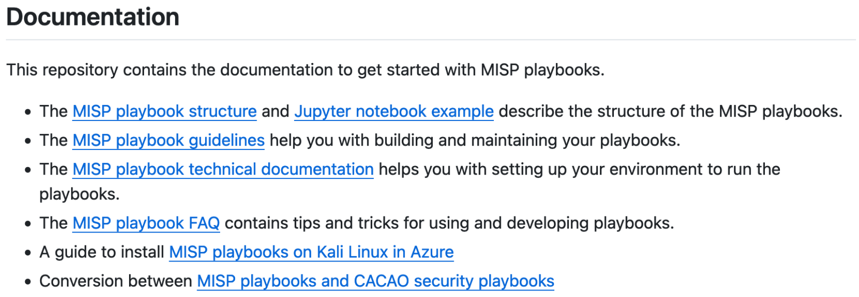
https://github.com/misp/misp-playbooks

- Published on GitHub
  - https://github.com/MISP/MISP-playbooks

- Guidance and technical **documentation**
  - Structure of playbooks
  - Recommendations to write your own playbooks
  - Setting up the environment (JupyterLab)
  - Conversion **scripts** to CACAO security playbooks

- 24 playbooks


Contributions to main, excluding merge commits


Documentation

This repository contains the documentation to get started with MISP playbooks.

- The MISP playbook structure and Jupyter notebook example describe the structure of the MISP playbooks.
- The MISP playbook guidelines help you with building and maintaining your playbooks.
- The MISP playbook technical documentation helps you with setting up your environment to run the playbooks.
- The MISP playbook FAQ contains tips and tricks for using and developing playbooks.
- A guide to install MISP playbooks on Kali Linux in Azure
- Conversion between MISP playbooks and CACAO security playbooks

MISP playbooks

https://github.com/misp/misp-playbooks

Playbooks for MISP **users**

Investigations

- IP and domain information
- Lookup CVE details
- Query Elastic for indicators
- Verify indicators in Timesketch
- JARM fingerprints

Incidents

- Create events from Sentinel incidents
- Deal with malware investigations
  - Triage
  - Hash checks
- Phishing

CTI work

- Curation and quality assurance
- Threat actor profiling

Become better acquainted with the MISP features

- MISP objects
- Warning lists
- Timestamps in MISP

Playbooks for MISP **administrators**

User management

- Provision users and organisations

Event management

- Bulk delete of events

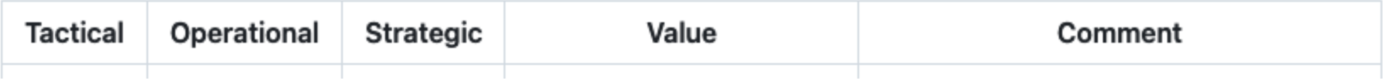
Your playbook?

- Request new playbooks via a GitHub **issue**
- Submit your own playbooks via **pull requests**

Proving the value of cyber threat intelligence

https://github.com/cudeso/proof-value-cti

- Demonstrate **value** of cyber threat intelligence (CTI) within an organisation
  - How can CTI support the organisation?
    - Tactical, operational and strategic level



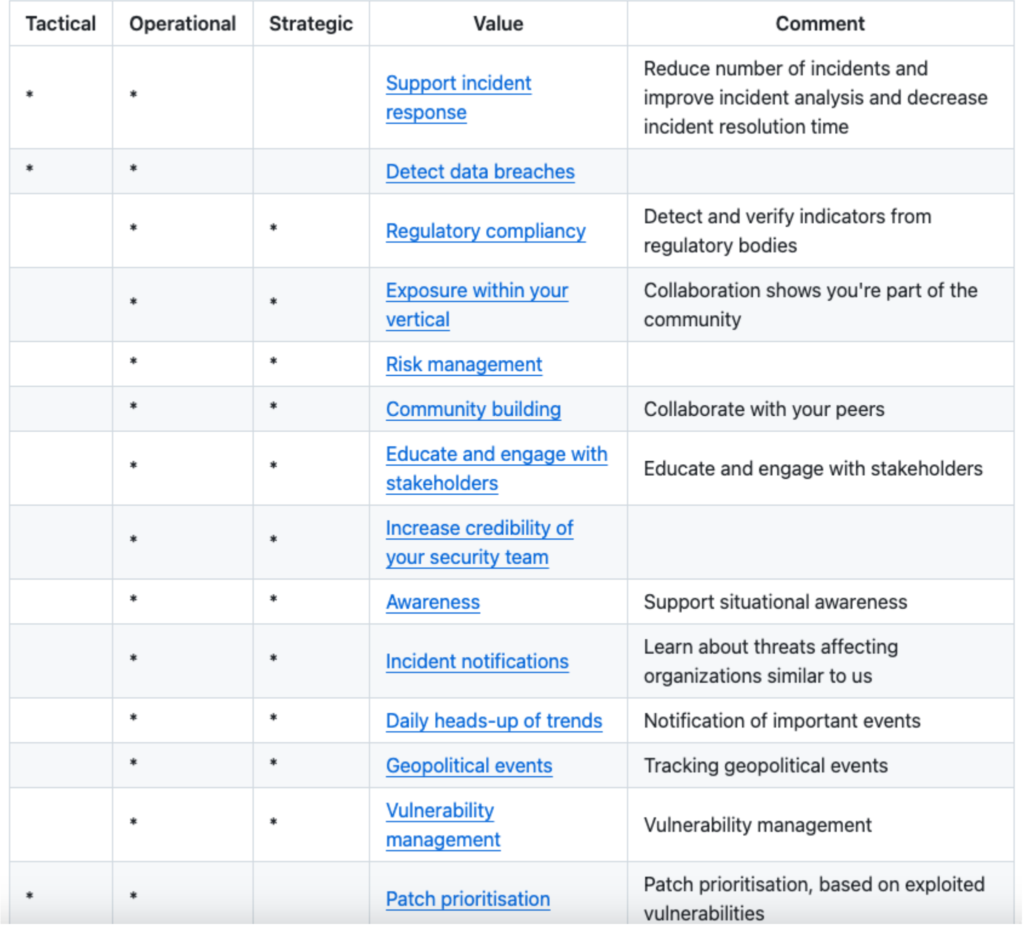
Tactical	Operational	Strategic	Value	Comment

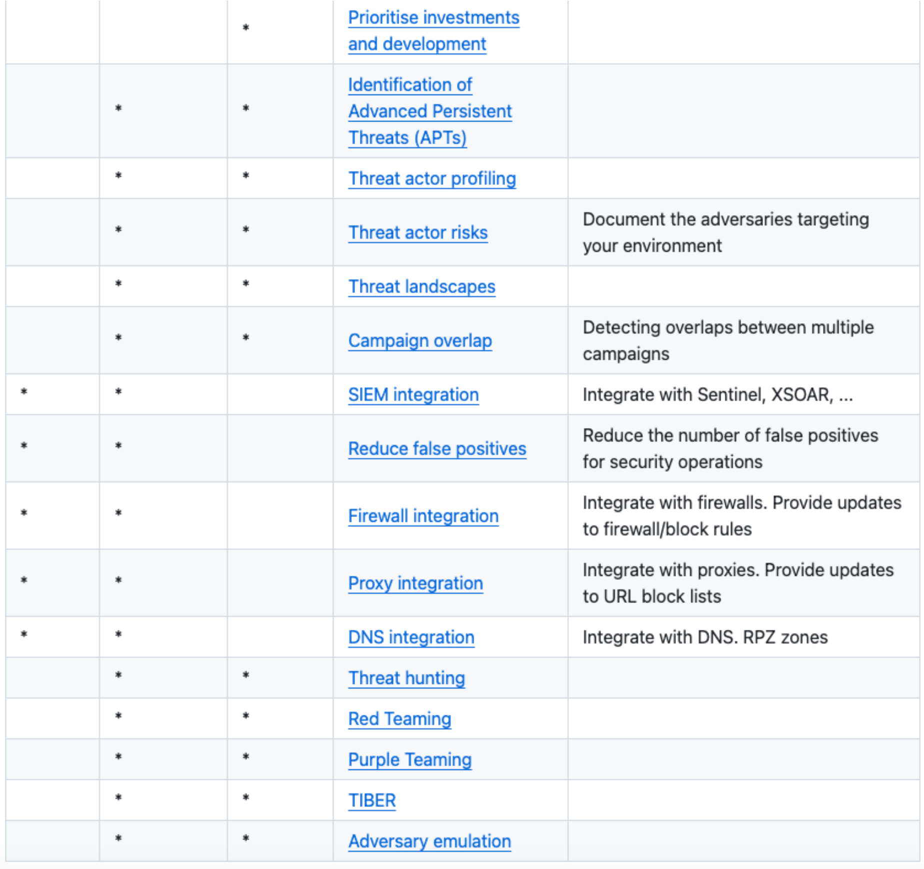
- Already a lot of resources available, but not always that easy to start with
- **Practical, pragmatic** and **collaborative**
- Not a new standard or framework
  - No intention of reinventing the wheel
  - Something simple that you can use in conversation such as "why would spend money on CTI"?
  - Organisations looking at how to operationalise CTI

- Published an initial list of ideas on GitHub
  - https://github.com/cudeso/proof-value-cti
  - Room for improvement
    - Store "value" descriptions in ~~YAML files~~ ('DFIQ.org'). Or JSON?
      - +: generate "human" readable and "machine" readable output

Proving the value of cyber threat intelligence

https://github.com/cudeso/proof-value-cti

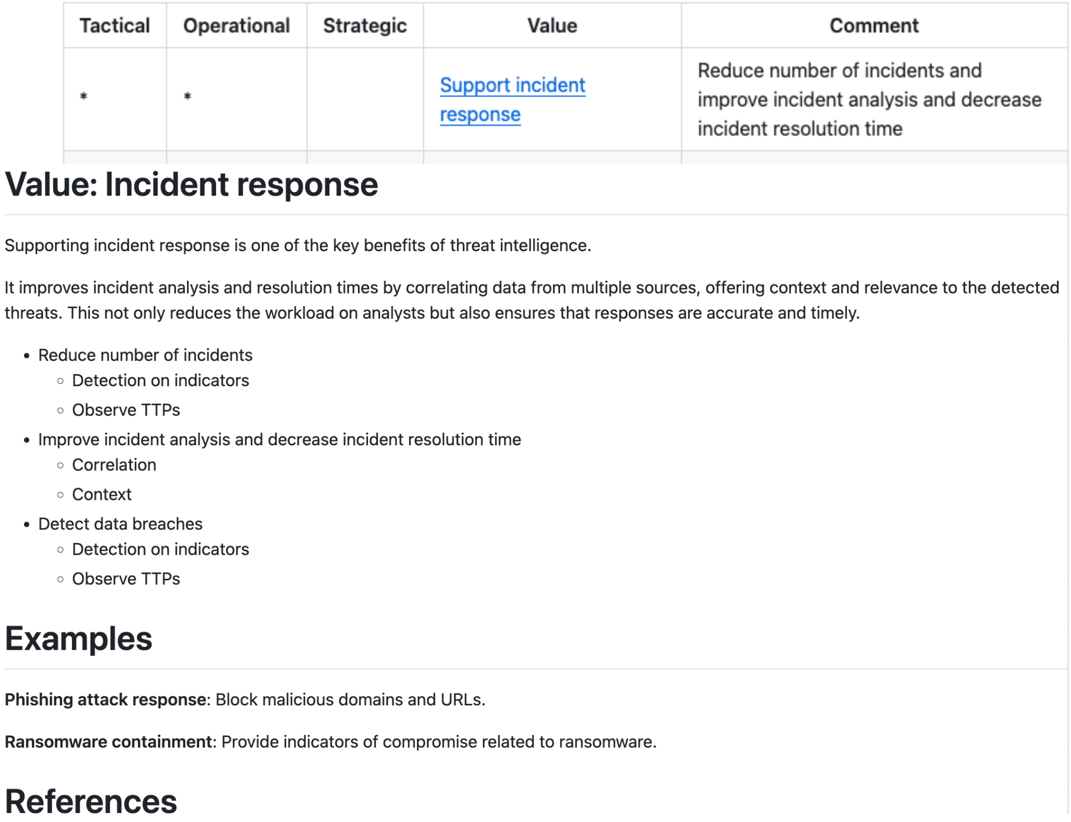




Tactical	Operational	Strategic	Value	Comment
*	*		Support incident response	Reduce number of incidents and improve incident analysis and decrease incident resolution time
*	*		Detect data breaches	
	*	*	Regulatory compliancy	Detect and verify indicators from regulatory bodies
	*	*	Exposure within your vertical	Collaboration shows you're part of the community
	*	*	Risk management	
	*	*	Community building	Collaborate with your peers
	*	*	Educate and engage with stakeholders	Educate and engage with stakeholders
	*	*	Increase credibility of your security team	
	*	*	Awareness	Support situational awareness
	*	*	Incident notifications	Learn about threats affecting organizations similar to us
	*	*	Daily heads-up of trends	Notification of important events
	*	*	Geopolitical events	Tracking geopolitical events
	*	*	Vulnerability management	Vulnerability management
*	*		Patch prioritisation	Patch prioritisation, based on exploited vulnerabilities
		*	Prioritise investments and development	
	*	*	Identification of Advanced Persistent Threats (APTs)	
	*	*	Threat actor profiling	
	*	*	Threat actor risks	Document the adversaries targeting your environment
	*	*	Threat landscapes	
	*	*	Campaign overlap	Detecting overlaps between multiple campaigns
*	*		SIEM integration	Integrate with Sentinel, XSOAR, ...
*	*		Reduce false positives	Reduce the number of false positives for security operations
*	*		Firewall integration	Integrate with firewalls. Provide updates to firewall/block rules
*	*		Proxy integration	Integrate with proxies. Provide updates to URL block lists
*	*		DNS integration	Integrate with DNS. RPZ zones
	*	*	Threat hunting	
	*	*	Red Teaming	
	*	*	Purple Teaming	
	*	*	TIBER	
	*	*	Adversary emulation	

Proving the value of cyber threat intelligence

https://github.com/cudeso/proof-value-cti



Tactical	Operational	Strategic	Value	Comment
*	*		Support incident response	Reduce number of incidents and improve incident analysis and decrease incident resolution time

Value: Incident response

Supporting incident response is one of the key benefits of threat intelligence.

It improves incident analysis and resolution times by correlating data from multiple sources, offering context and relevance to the detected threats. This not only reduces the workload on analysts but also ensures that responses are accurate and timely.

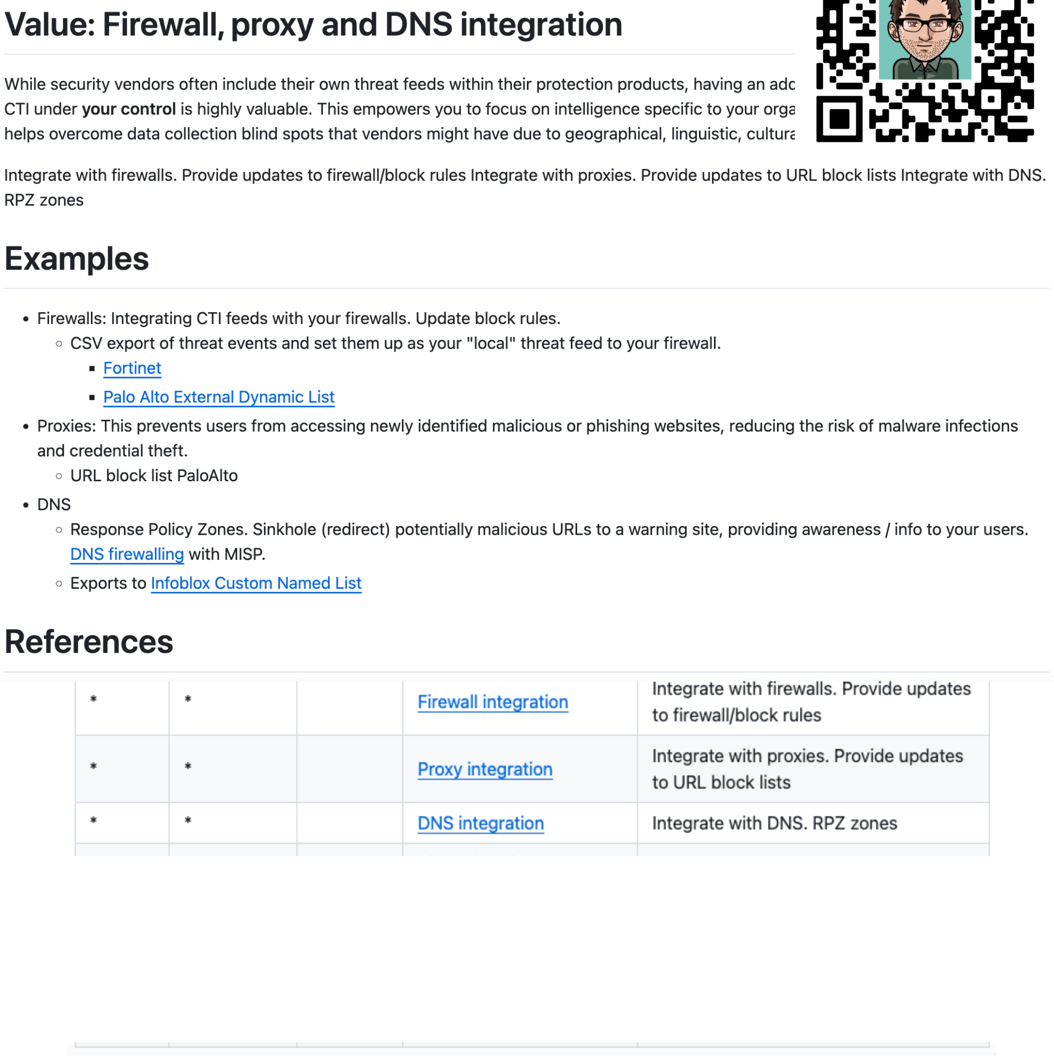
- Reduce number of incidents
  - Detection on indicators
  - Observe TTPs
- Improve incident analysis and decrease incident resolution time
  - Correlation
  - Context
- Detect data breaches
  - Detection on indicators
  - Observe TTPs

Examples

Phishing attack response: Block malicious domains and URLs.

Ransomware containment: Provide indicators of compromise related to ransomware.

References



Value: Firewall, proxy and DNS integration

While security vendors often include their own threat feeds within their protection products, having an adc CTI under **your control** is highly valuable. This empowers you to focus on intelligence specific to your orga helps overcome data collection blind spots that vendors might have due to geographical, linguistic, cultura

Integrate with firewalls. Provide updates to firewall/block rules Integrate with proxies. Provide updates to URL block lists Integrate with DNS. RPZ zones

Examples

- Firewalls: Integrating CTI feeds with your firewalls. Update block rules.
  - CSV export of threat events and set them up as your "local" threat feed to your firewall.
    - Fortinet
    - Palo Alto External Dynamic List
- Proxies: This prevents users from accessing newly identified malicious or phishing websites, reducing the risk of malware infections and credential theft.
  - URL block list PaloAlto
- DNS
  - Response Policy Zones. Sinkhole (redirect) potentially malicious URLs to a warning site, providing awareness / info to your users. DNS firewalling with MISP.
  - Exports to Infoblox Custom Named List

References

*	*		Firewall integration	Integrate with firewalls. Provide updates to firewall/block rules
*	*		Proxy integration	Integrate with proxies. Provide updates to URL block lists
*	*		DNS integration	Integrate with DNS. RPZ zones

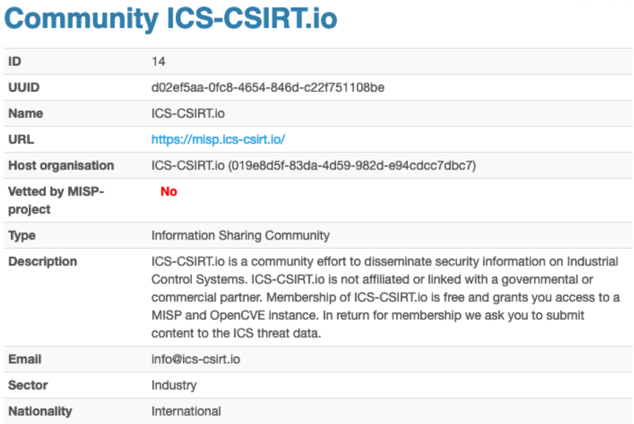
ICS-CSIRT.io

https://www.ics-csirt.io/

- **ICS-CSIRT.io**
  - Community to disseminate security information on industrial control systems
    - Not affiliated or linked with a governmental or commercial partner
  - Membership is free
    - In return, submit content (website/MISP)

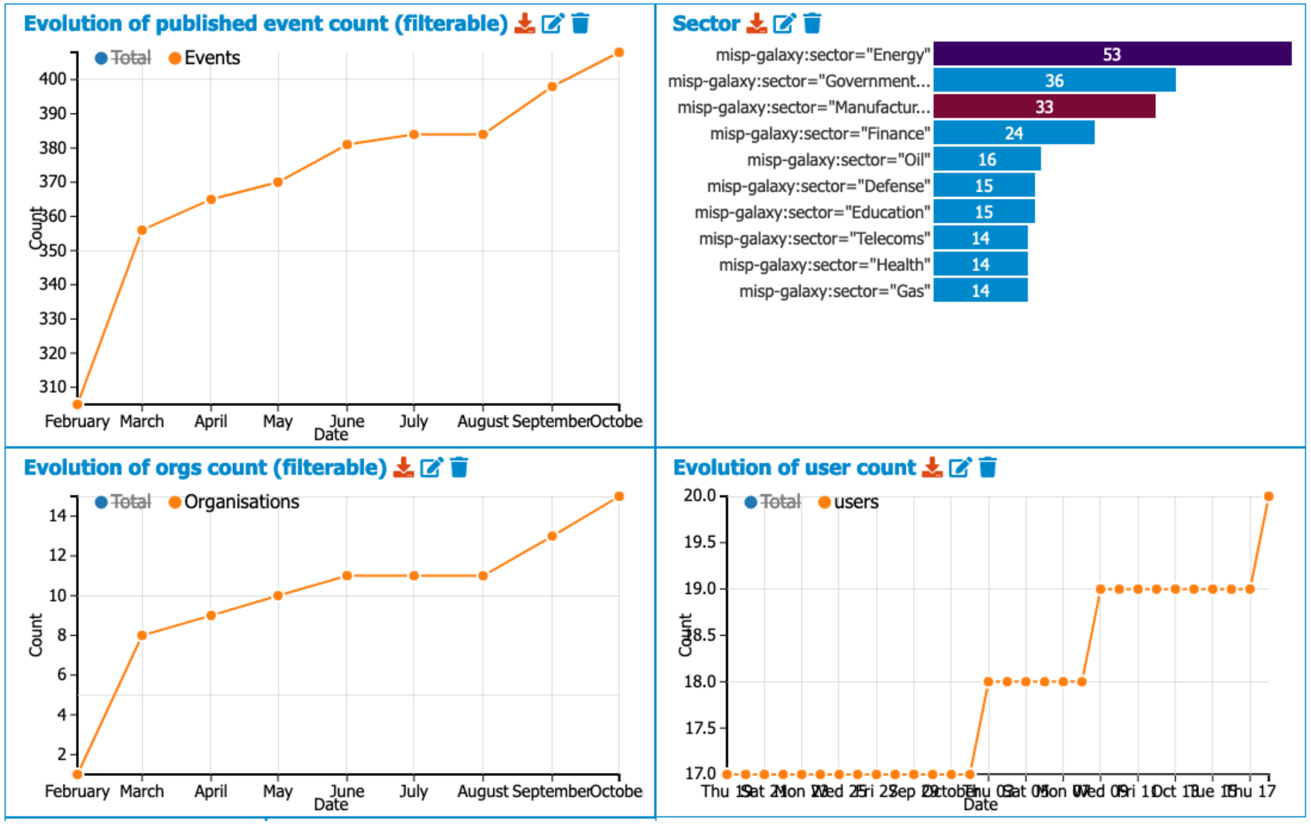
- **OpenCVE** ("advisories" > NVD)
  - https://cve.ics-csirt.io/
    - Replace with 'Vulnerability Lookup'?
      - https://github.com/cve-search/vulnerability-lookup

- **MISP** community ("threats")
  - https://misp.ics-csirt.io/



Community ICS-CSIRT.io

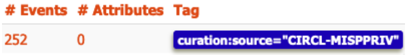
ID	14
UUID	d02ef5aa-0fc8-4654-846d-c22f751108be
Name	ICS-CSIRT.io
URL	https://misp.ics-csirt.io/
Host organisation	ICS-CSIRT.io (019e8d5f-83da-4d59-982d-e94cdcc7dbc7)
Vetted by MISP-project	No
Type	Information Sharing Community
Description	ICS-CSIRT.io is a community effort to disseminate security information on Industrial Control Systems. ICS-CSIRT.io is not affiliated or linked with a governmental or commercial partner. Membership of ICS-CSIRT.io is free and grants you access to a MISP and OpenCVE instance. In return for membership we ask you to submit content to the ICS threat data.
Email	info@ics-csirt.io
Sector	Industry
Nationality	International



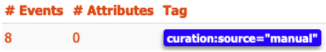
ICS-CSIRT.io

https://www.ics-csirt.io/

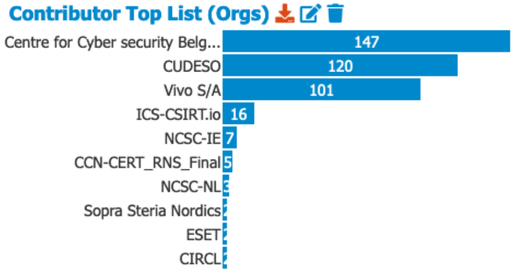
- **Bootstrapped** with shareable threat events from MISPPRIV



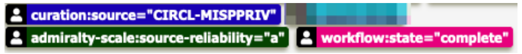
# Events	# Attributes	Tag
252	0	curation:source="CIRCL-MISPPRIV"



# Events	# Attributes	Tag
8	0	curation:source="manual"

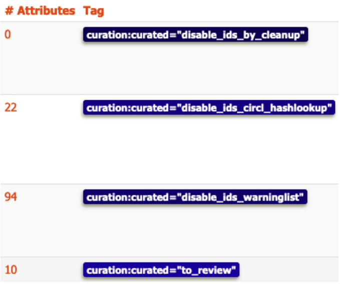


- **Curation** process



curation:source="CIRCL-MISPPRIV" [redacted]
admiralty-scale:source-reliability="a" workflow:state="complete"

  - Matches with common **warning lists** and **hashlookup** are automatically disabled
  - Manual relevance check



# Attributes	Tag
0	curation:curated="disable_ids_by_cleanup"
22	curation:curated="disable_ids_circl_hashlookup"
94	curation:curated="disable_ids_warninglist"
10	curation:curated="to_review"

- Sharing guidelines (*similar to MISPPRIV*)
  - All shared information must adhere to the **Traffic Light Protocol** (TLP) classification system
    - Users are responsible for the accuracy and integrity of the information they contribute
    - Users must respect the privacy and confidentiality of the information shared on the platform
  - Users must **comply with the dissemination restrictions** associated with each TLP level
  - If a TLP classification is not set on an event, the default classification is **TLP:AMBER**