



Science and
Technology
Facilities Council

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



MISP
Threat Sharing

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »

| Filters: Tags: tlp:white x | | My Events | Org Events | | tlp:white | Tag | Filter | | | | |
|----------------------------|--------------|-----------|--|--|-----------|--------|------------|---------------------|---------------------|---|--------------|
| <input type="checkbox"/> | Creator org | ID | Clusters | Tags | #Attr. | #Corr. | Date | Last modified at ↑ | Published at | Info | Distribution |
| <input type="checkbox"/> | urlabuse.com | 24090 | Attack Pattern Q Phishing - T1566 Q ≡ | Phishing tlp:white | 1288 | 89 | 2024-10-30 | 2024-11-01 07:59:37 | 2024-11-01 14:22:03 | Daily Phishing list urlabuse.com - 2024-10-30 | All ↔ |
| <input type="checkbox"/> | urlabuse.com | 24142 | Attack Pattern Q Phishing - T1566 Q ≡ | Phishing tlp:white | 1314 | 95 | 2024-10-29 | 2024-10-31 20:28:18 | 2024-11-01 14:27:30 | Daily Phishing list urlabuse.com - 2024-10-29 | All ↔ |
| <input type="checkbox"/> | Crimeware | 13122 | Ransomware Q Locky Q ≡ | tlp:white malware_classification:malware-category="Ransomware" intelmq:done circl:topic="ict" osint:source-type="block-or-filter-list" | 1599 | 27 | 2016-08-31 | 2024-10-31 08:41:21 | 2024-11-01 14:37:09 | Locky 2016-08-31 : Affid=3, DGA=1313 - "Image" - "IMG_31082016_12345.zip" | All ↔ |
| <input type="checkbox"/> | Crimeware | 13130 | Ransomware Q Locky Q ≡ | tlp:white malware_classification:malware-category="Ransomware" intelmq:done osint:source-type="block-or-filter-list" | 4806 | 60 | 2016-08-31 | 2024-10-31 08:40:18 | 2024-11-01 14:37:15 | Locky 2016-08-31 : Affid=1, DGA=1313 - "bank transactions" - "12345678abc.zip" | All ↔ |
| <input type="checkbox"/> | CIRCL_65 | 24067 | | tlp:white tlp:clear circl:incident-classification="phishing" | 2 | | 2024-10-30 | 2024-10-30 15:31:19 | 2024-11-01 14:16:31 | Malicious domain abused to send phishing/malspam | All ↔ |
| <input type="checkbox"/> | Evonik CDT | 10262 | | tlp:white PAP:WHITE veris:confidence="High" estimative-language:confidence-in-analytic-judgment="high" misp:confidence-level="completely-confident" threatmatch-incident-types:incident_type="Malware Infection" circl:incident-classification="malware" | 88 | | 2024-07-28 | 2024-10-30 15:08:49 | 2024-10-30 15:08:49 | Infrastructure to distribute malicious mobile apps | All ↔ |
| <input type="checkbox"/> | CERN_1114 | 24196 | | tlp:white | 14 | | 2021-12-17 | 2024-10-30 13:39:06 | 2024-11-01 14:37:07 | Blocked IPs in the CERN firewall (e.g. IPs engaging in DDoS attacks against CERN) | Organisation |
| <input type="checkbox"/> | CIRCL_65 | 24091 | | circl:incident-classification="scam" tlp:white tlp:clear | 4 | | 2024-10-30 | 2024-10-30 08:47:55 | 2024-11-01 14:22:03 | Fake Luxembourg Police Scam | All ↔ |
| <input type="checkbox"/> | urlabuse.com | 24174 | Attack Pattern Q Phishing - T1566 Q ≡ | Phishing tlp:white splunk:OK | 1539 | 113 | 2024-10-28 | 2024-10-30 04:50:54 | 2024-11-01 14:34:11 | Daily Phishing list urlabuse.com - 2024-10-28 | All ↔ |
| <input type="checkbox"/> | threatfox | 24088 | | type:OSINT tlp:white URLHaus | 7668 | | 2024-10-29 | 2024-10-30 00:03:12 | 2024-11-01 14:21:16 | URLhaus IOCs for 2024-10-29 | Organisation |
| <input type="checkbox"/> | threatfox | 24083 | | type:OSINT tlp:white ThreatFox | 184 | | 2024-10-29 | 2024-10-30 00:03:07 | 2024-11-01 14:16:51 | ThreatFox IOCs for 2024-10-29 | Organisation |
| <input type="checkbox"/> | threatfox | 24130 | | type:OSINT tlp:white MALWARE | 4547 | 134 | 2024-10-29 | 2024-10-30 00:03:01 | 2024-11-01 14:24:11 | MalwareBazaar malware samples for 2024-10-29 | All ↔ |

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 tip: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](#)

X 24090: Daily Phishi...

Galaxies

Attack Pattern

Phishing - T1566

« 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](#)

[Date ↑](#)
[Context](#)
[Category](#)
[Type](#)
[Value](#)
[Tags](#)
[Galaxies](#)
[Comment](#)
[Correlate](#)
[Related Events](#)
[Feed hits](#)
[IDS](#)
[Distribution](#)
[Sightings](#)
[Activity](#)
[Actions](#)

Related Events

Order by date

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

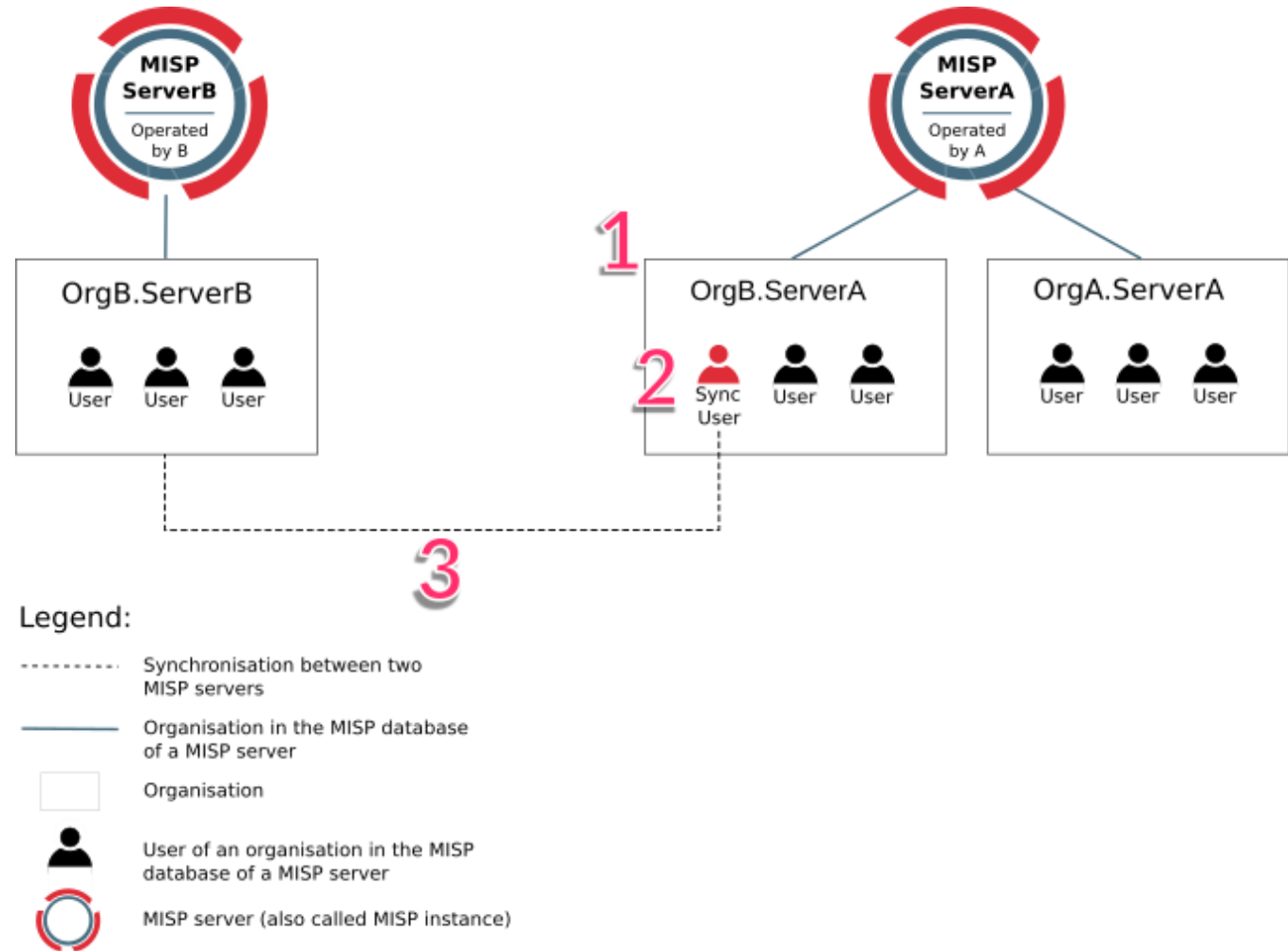
Show (79 more)

Warning: Potential false positives (show)

Top 1000 website from Alexa

Sharing in MISP

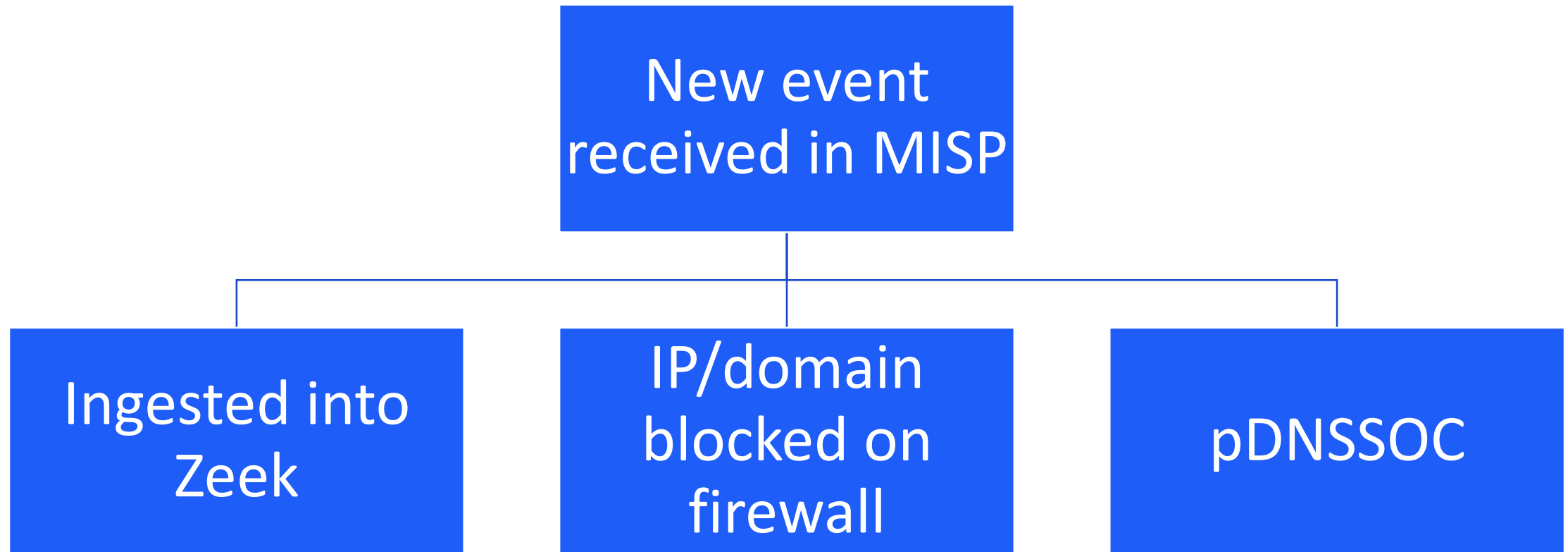
- Publicly available threat feeds
 - A good start but limited in relevance
- Syncs with other MISP servers
 - More relevant intel if from the community
- Distribution settings (set by publisher)
 - Your organisation only
 - This community only
 - Connected communities
 - All communities
 - Sharing group



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



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



JiscCTI / misp-docker



Science and
Technology
Facilities Council

Thank you

Facebook: Science and
Technology Facilities Council

Twitter: @STFC_matters

YouTube: Science and
Technology Facilities Council