GÉANT
Networks • Services • People

SOC '22 and Beyond

GN4-3 WP8 Task 3.1 → GN5

Roderick Mooi
GÉANT Information Security Officer
Task 3.1. team lead (coordinator)

WP8 All Hands, 1 February 2022

Public

www.geant.org

Current team:

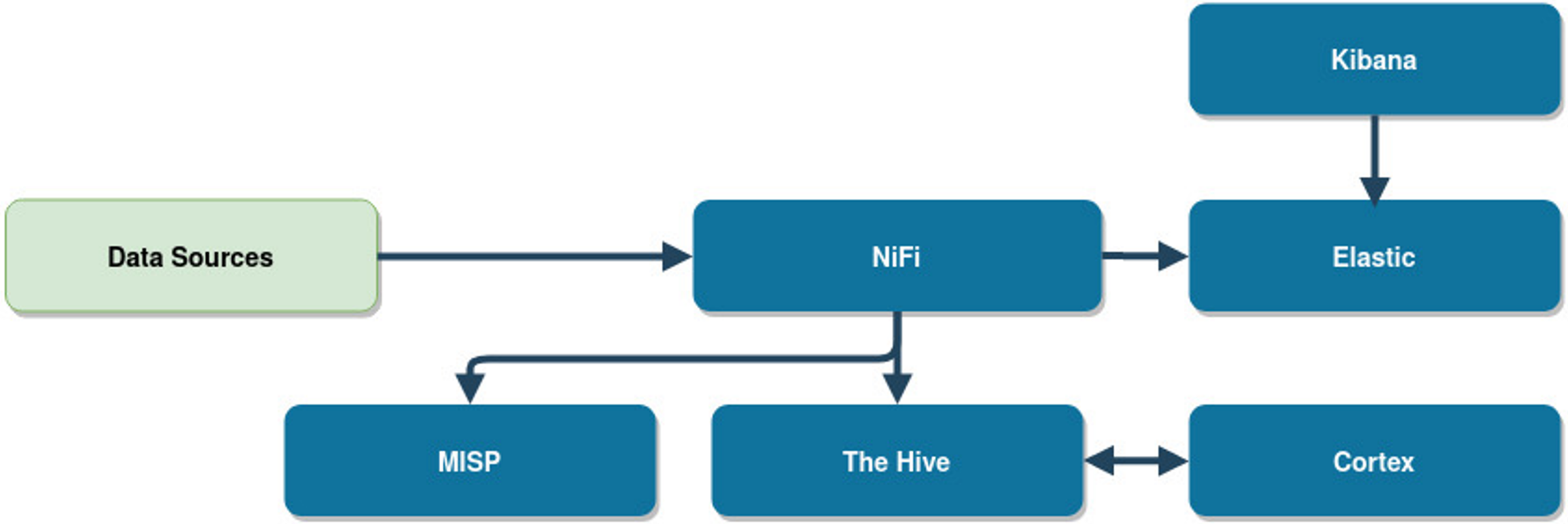
- Temur Maisuradze – GRENA
- Kiril Kjiroski – MARnet
- Fredrik Pettai – SUNET
- Vaclav Bartos – CESNET
- Roderick Mooi – GÉANT (coordination)

- Supported by:
  - David Heed – SUNET
  - Jochen Schoenfelder – DFN-CERT

- https://wiki.geant.org/display/gn43wp8/3.1+SOC

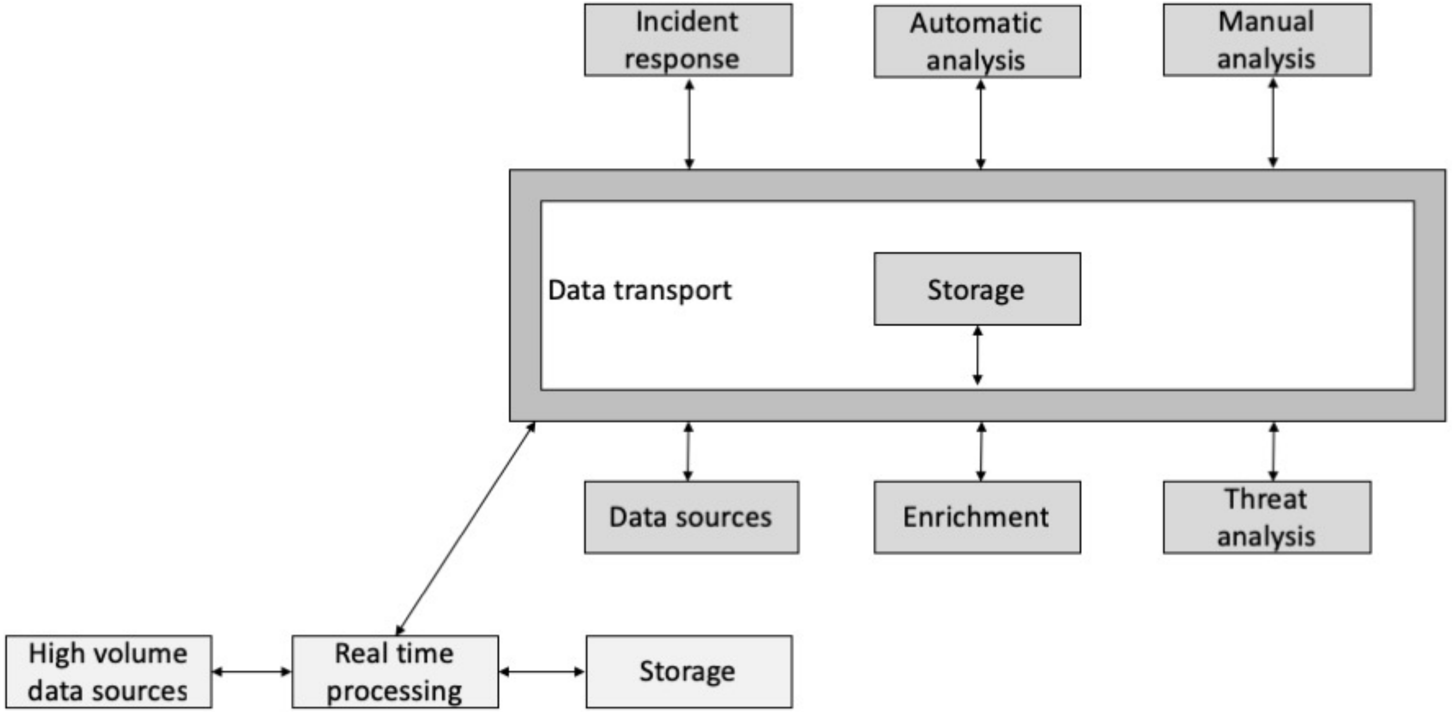
SOCTools, aka tools for "SOC-in-a-box"

- SOCTools is a set of tools that can be used by a SOC for collecting and analysing security data, incident handling and threat intelligence
- https://gitlab.geant.org/gn4-3-wp8-t3.1-soc/soctools



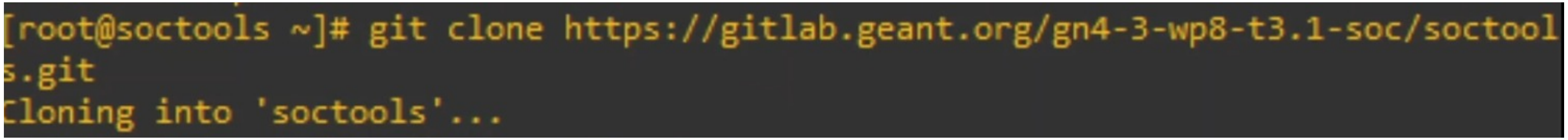
Demo @ TNC21

- Logs > normalisation > enrichment
- Incident report (ticketing) > threat intel. > analysis

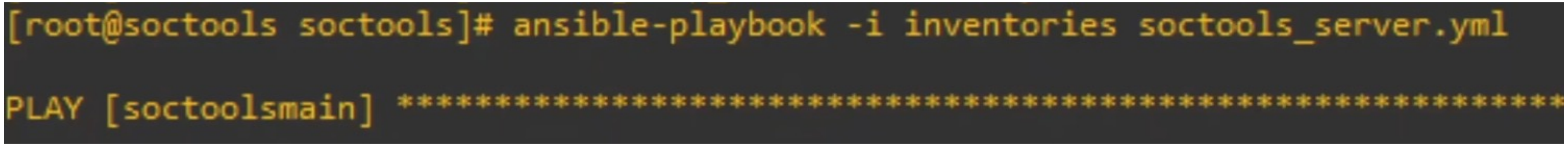


Demo @ TNC21

- Installation and basic use

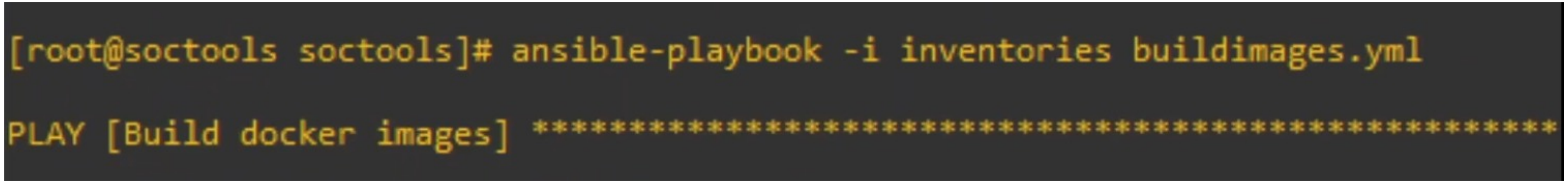


```
[root@soctools ~]# git clone https://gitlab.geant.org/gn4-3-wp8-t3.1-soc/soctool
s.git
Cloning into 'soctools'...
```



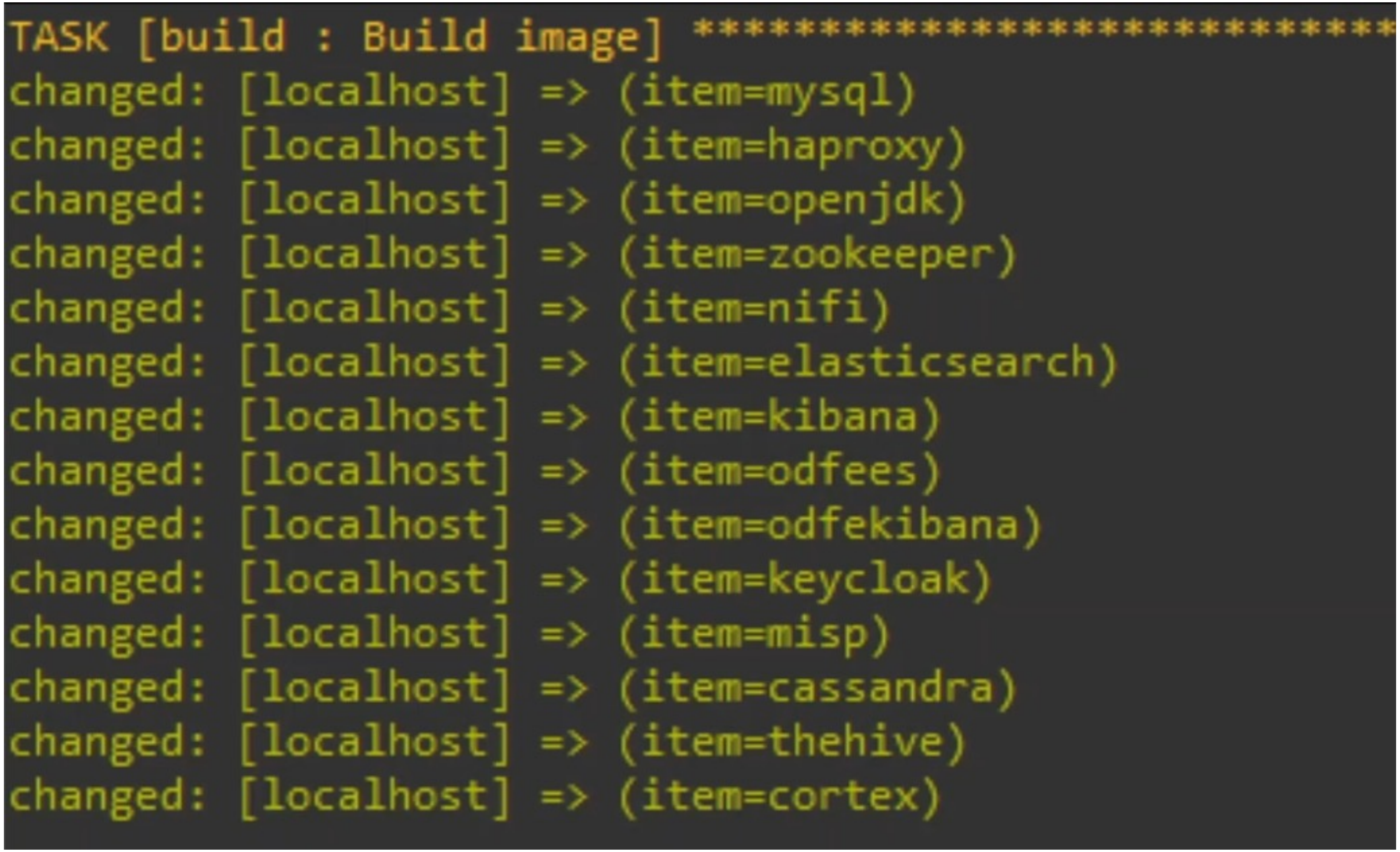
```
[root@soctools soctools]# ansible-playbook -i inventories soctools_server.yml

PLAY [soctoolsmain] ************************************************************
```



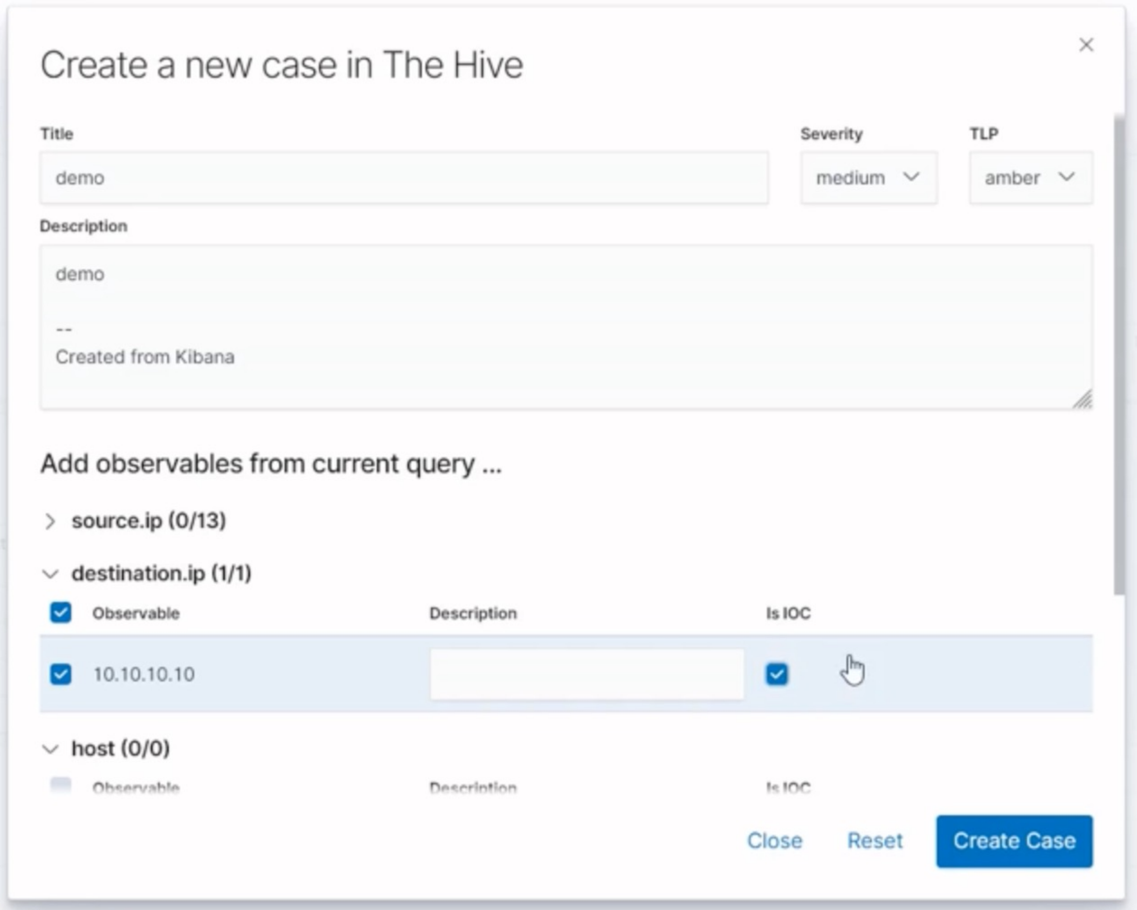
```
[root@soctools soctools]# ansible-playbook -i inventories buildimages.yml

PLAY [Build docker images] *****************************************************
```



```
TASK [build : Build image] ******************************
changed: [localhost] => (item=mysql)
changed: [localhost] => (item=haproxy)
changed: [localhost] => (item=openjdk)
changed: [localhost] => (item=zookeeper)
changed: [localhost] => (item=nifi)
changed: [localhost] => (item=elasticsearch)
changed: [localhost] => (item=kibana)
changed: [localhost] => (item=odfees)
changed: [localhost] => (item=odfekibana)
changed: [localhost] => (item=keycloak)
changed: [localhost] => (item=misp)
changed: [localhost] => (item=cassandra)
changed: [localhost] => (item=thehive)
changed: [localhost] => (item=cortex)
```

Kibana > The Hive > MISP …



Create a new case in The Hive

Title: demo

Severity: medium

TLP: amber

Description:

demo

--
Created from Kibana

Add observables from current query …

source.ip (0/13)

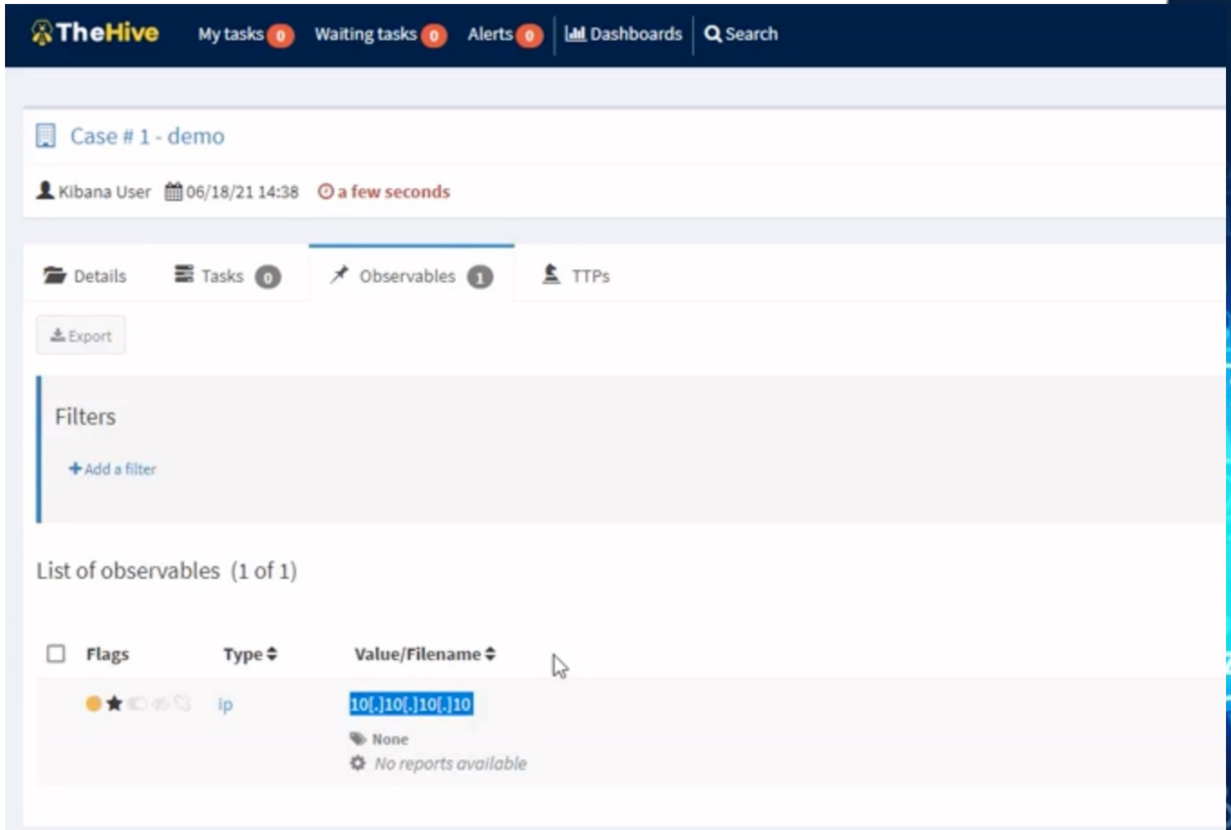
destination.ip (1/1)

☑ Observable	Description	Is IOC
☑ 10.10.10.10		☑

host (0/0)

Observable	Description	Is IOC

>



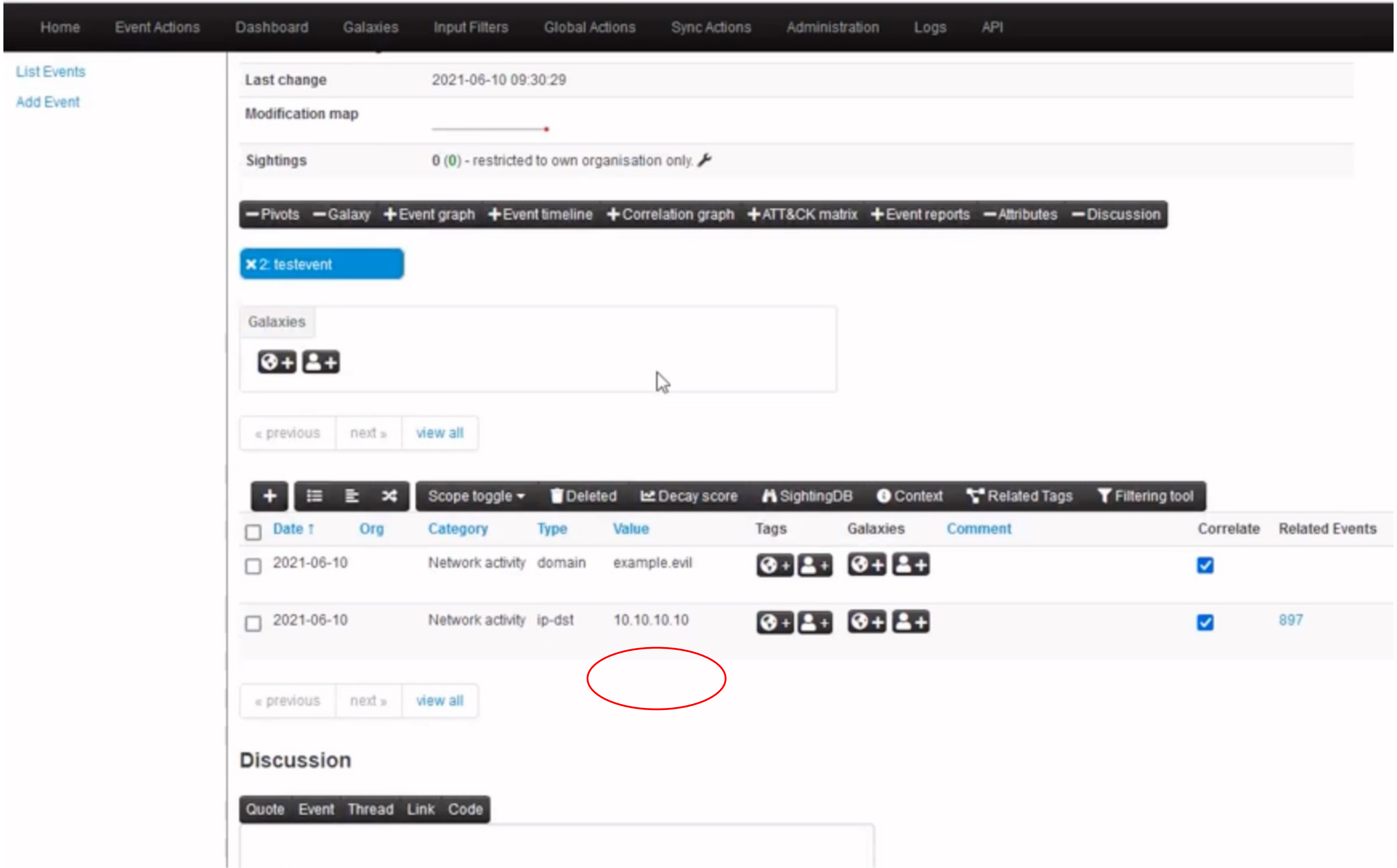
Case # 1 - demo

Kibana User 06/18/21 14:38 a few seconds

Filters

List of observables (1 of 1)

Flags	Type	Value/Filename
● ★	ip	10[.]10[.]10[.]10 None No reports available



Last change	2021-06-10 09:30:29
Sightings	0 (0) - restricted to own organisation only.

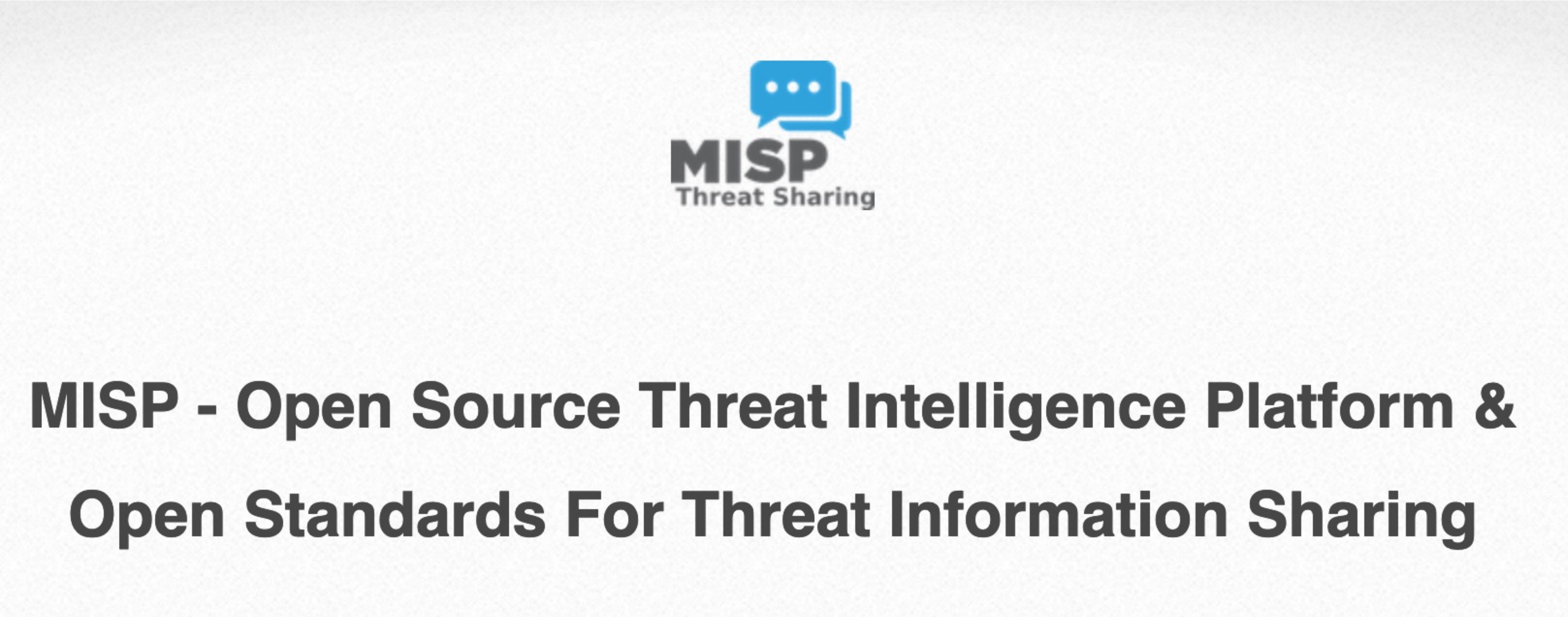
☐	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
☐	2021-06-10		Network activity	domain	example.evil				☑	
☐	2021-06-10		Network activity	ip-dst	10.10.10.10				☑	897

Discussion

What’s next?

- Cluster support > scalability
- Look into further use cases / increase adoption by NRENs, etc.
- Deliverables:
  - D8.9 Best practices for security operations in research and education
  - M8.13 Review of the best practice documents on utilisation of SOC tools
  - Final release of toolkit
- Integration with other Security projects
- Threat intelligence and information sharing

R&E intelligence sharing and threat analysis

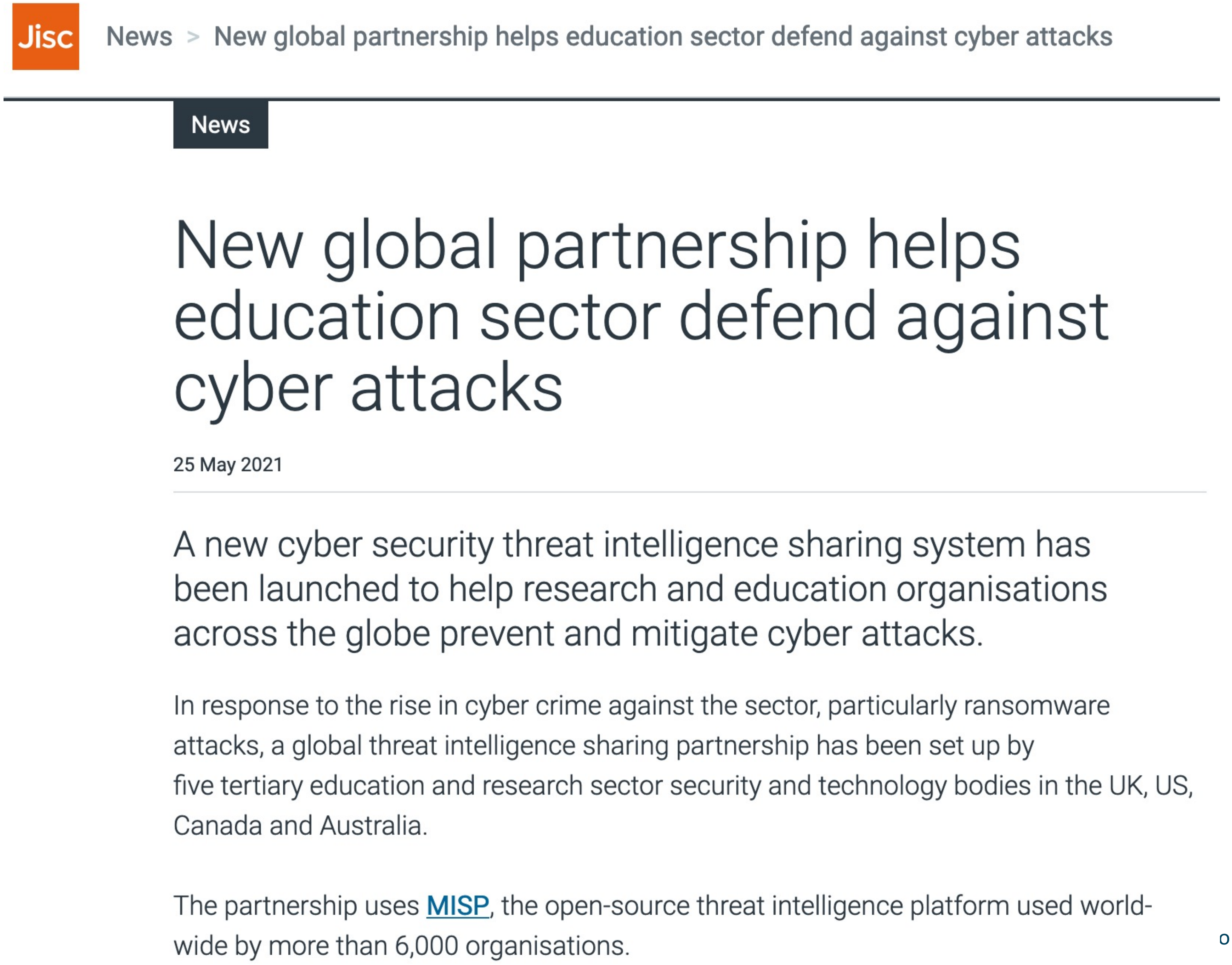


MISP
Threat Sharing

MISP - Open Source Threat Intelligence Platform &

Open Standards For Threat Information Sharing

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



Jisc
News > New global partnership helps education sector defend against cyber attacks
News

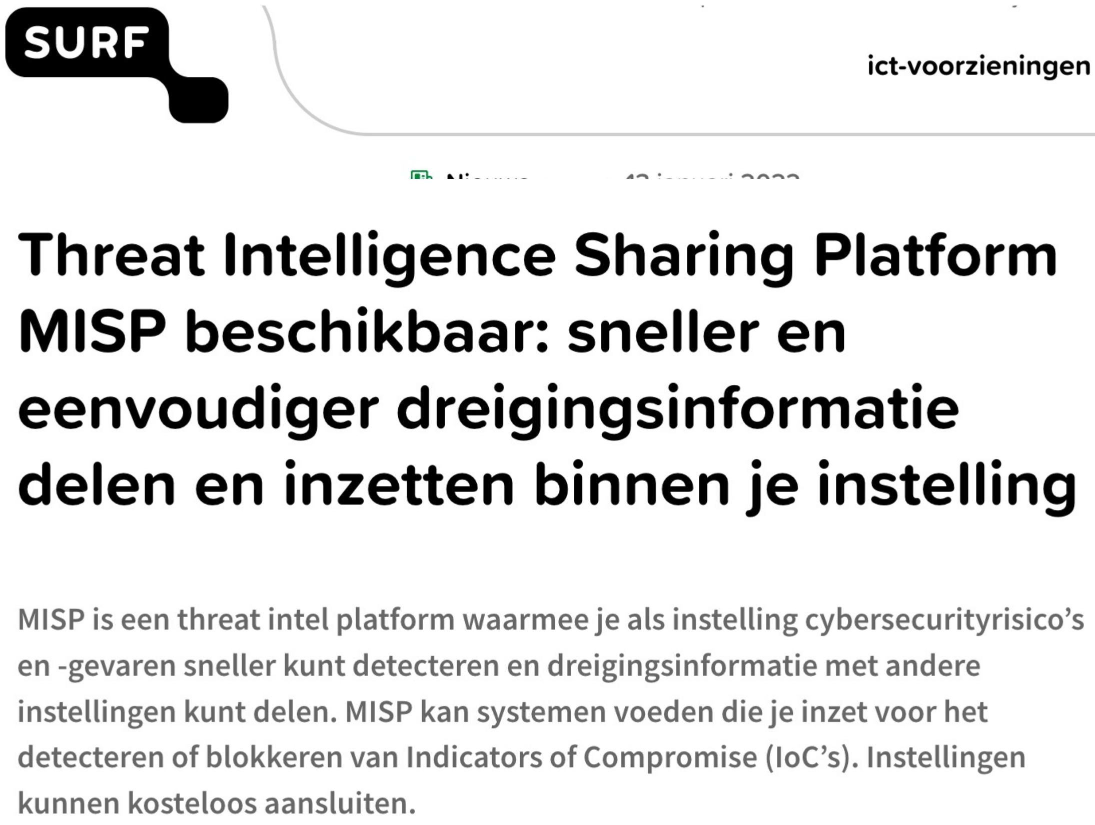
New global partnership helps education sector defend against cyber attacks

25 May 2021

A new cyber security threat intelligence sharing system has been launched to help research and education organisations across the globe prevent and mitigate cyber attacks.

In response to the rise in cyber crime against the sector, particularly ransomware attacks, a global threat intelligence sharing partnership has been set up by five tertiary education and research sector security and technology bodies in the UK, US, Canada and Australia.

The partnership uses MISP, the open-source threat intelligence platform used world-wide by more than 6,000 organisations.

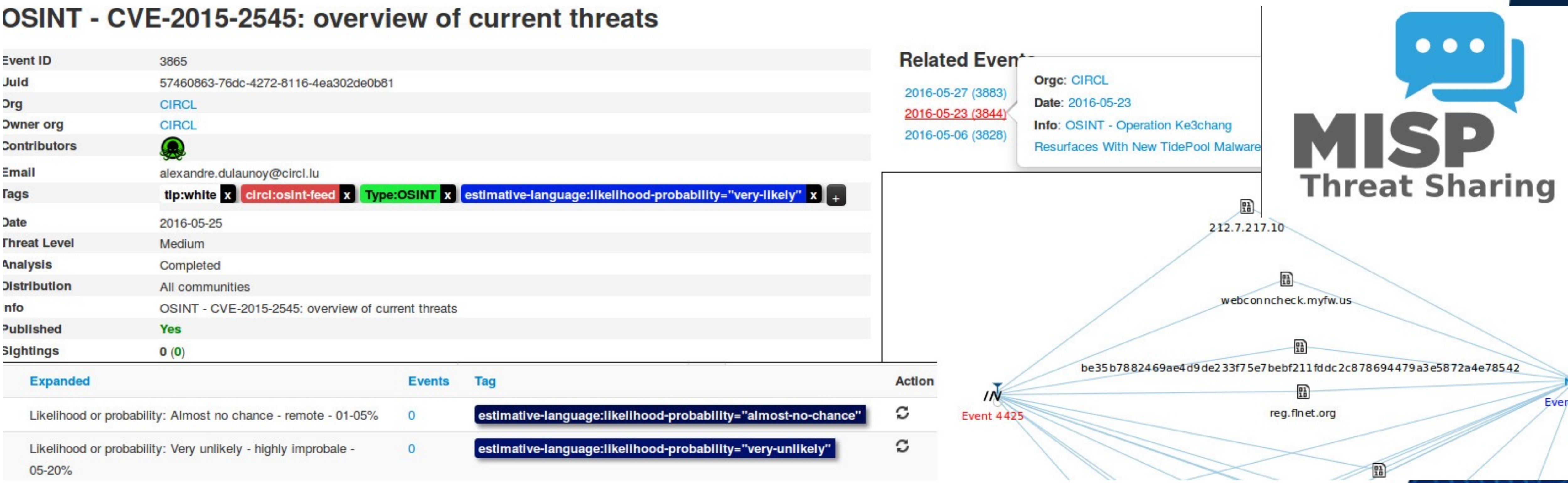


Threat Intelligence Sharing Platform MISP beschikbaar: sneller en eenvoudiger dreigingsinformatie delen en inzetten binnen je instelling

MISP is een threat intel platform waarmee je als instelling cybersecurityrisico's en -gevaren sneller kunt detecteren en dreigingsinformatie met andere instellingen kunt delen. MISP kan systemen voeden die je inzet voor het detecteren of blokkeren van Indicators of Compromise (IoC's). Instellingen kunnen kosteloos aansluiten.

… MISP available: faster and easier sharing and deploying threat intelligence across your institution

… MISP enables you as an institution to detect cybersecurity risks and threats faster and to share threat information with other institutions. MISP can feed systems that you use to detect or block Indicators of Compromise (IoCs).



OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Juid	57460863-76dc-4272-8116-4ea302de0b81
Drg	CIRCL
Dwner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
nfo	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	↻
Likelihood or probability: Very unlikely - highly improbale - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	↻

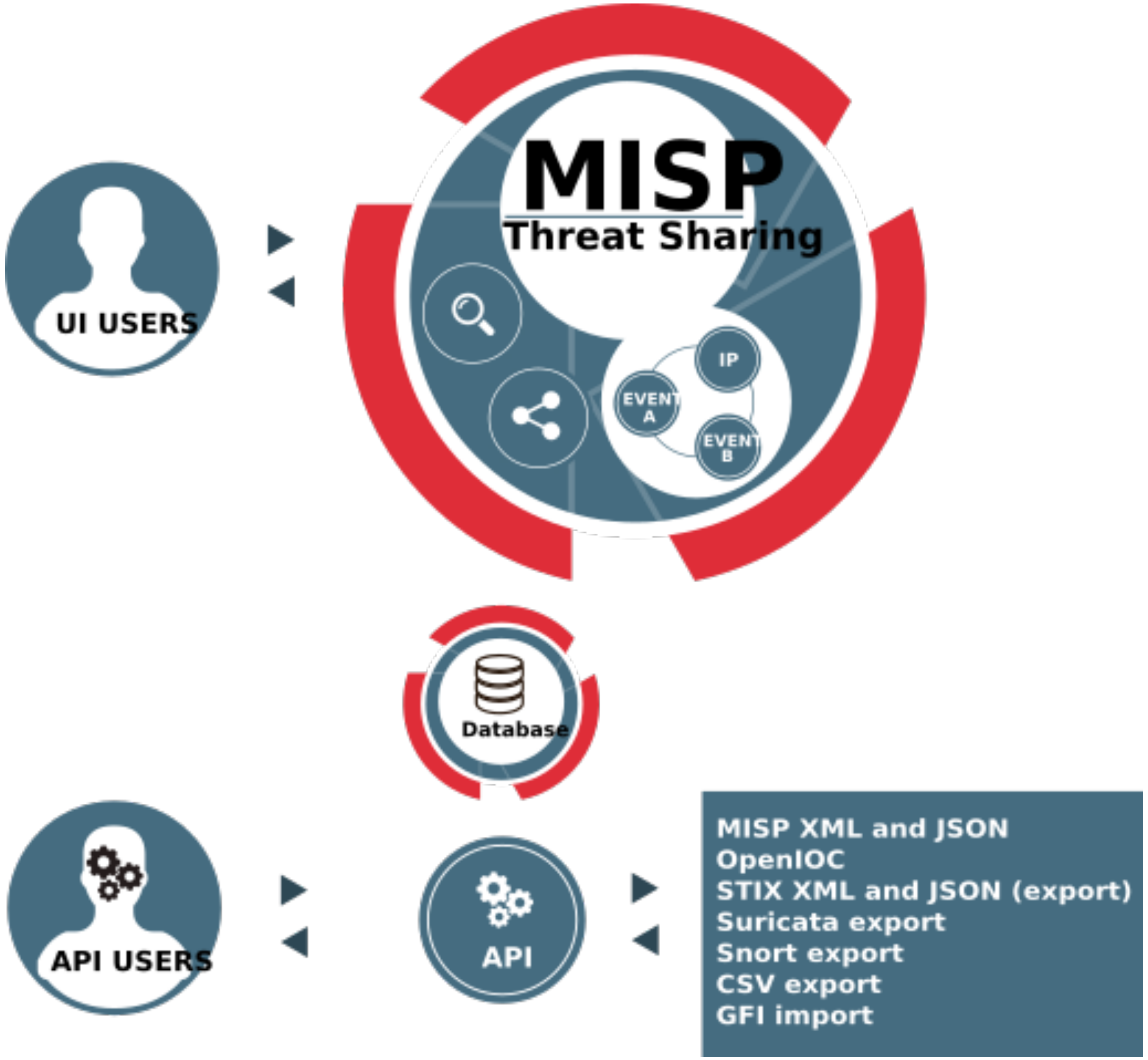
Related Even

2016-05-27 (3883)
2016-05-23 (3844)
2016-05-06 (3828)

Orgc: CIRCL
Date: 2016-05-23
Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware

212.7.217.10
webconncheck.myfw.us
be35b7882469ae4d9de233f75e7bebf211fddc2c878694479a3e5872a4e78542
reg.flnet.org
Event 4425
Ever

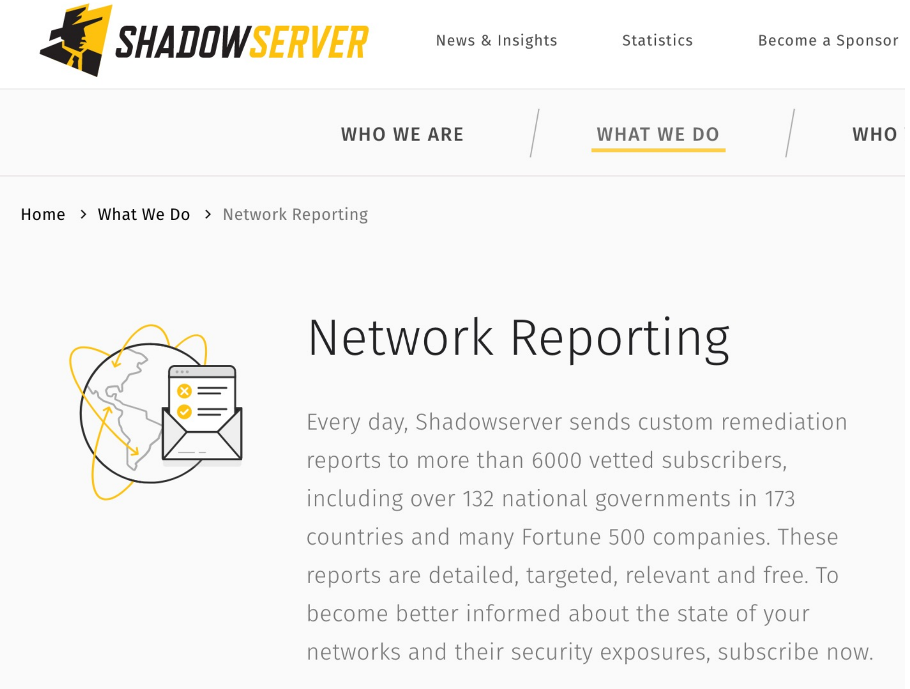
Analysts & Threat Hunters: please join us ☺



MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

What about?

- Using flow data for threat intel.
- Reports/alerts/advisories
  - Shadowserver, Team Cymru, etc.
- DNS (threat) intelligence
- Your ideas!!



Network Reporting

Every day, Shadowserver sends custom remediation reports to more than 6000 vetted subscribers, including over 132 national governments in 173 countries and many Fortune 500 companies. These reports are detailed, targeted, relevant and free. To become better informed about the state of your networks and their security exposures, subscribe now.

CSIRT Assistance Program

Helping CSIRTS worldwide protect their countries.

Thank you

gn4-3-wp8-soc@lists.geant.org

soc-tools@lists.geant.org

www.geant.org

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).