

# SOC Tools & Security “Intelligence Sharing”

**Roderick Mooi**  
*GÉANT Information Security Officer*

EaPConnect Cybersecurity Workshop II

08 February 2022

Public

[www.geant.org](http://www.geant.org)

## So what exactly is CTI?

TTPs / MITRE ATT&CK



- “The **analysis** of an **adversary's intent, opportunity, and capability** to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is **actionable information** that addresses an organization's key **knowledge gaps, pain points, or requirements.** “

- <https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/>

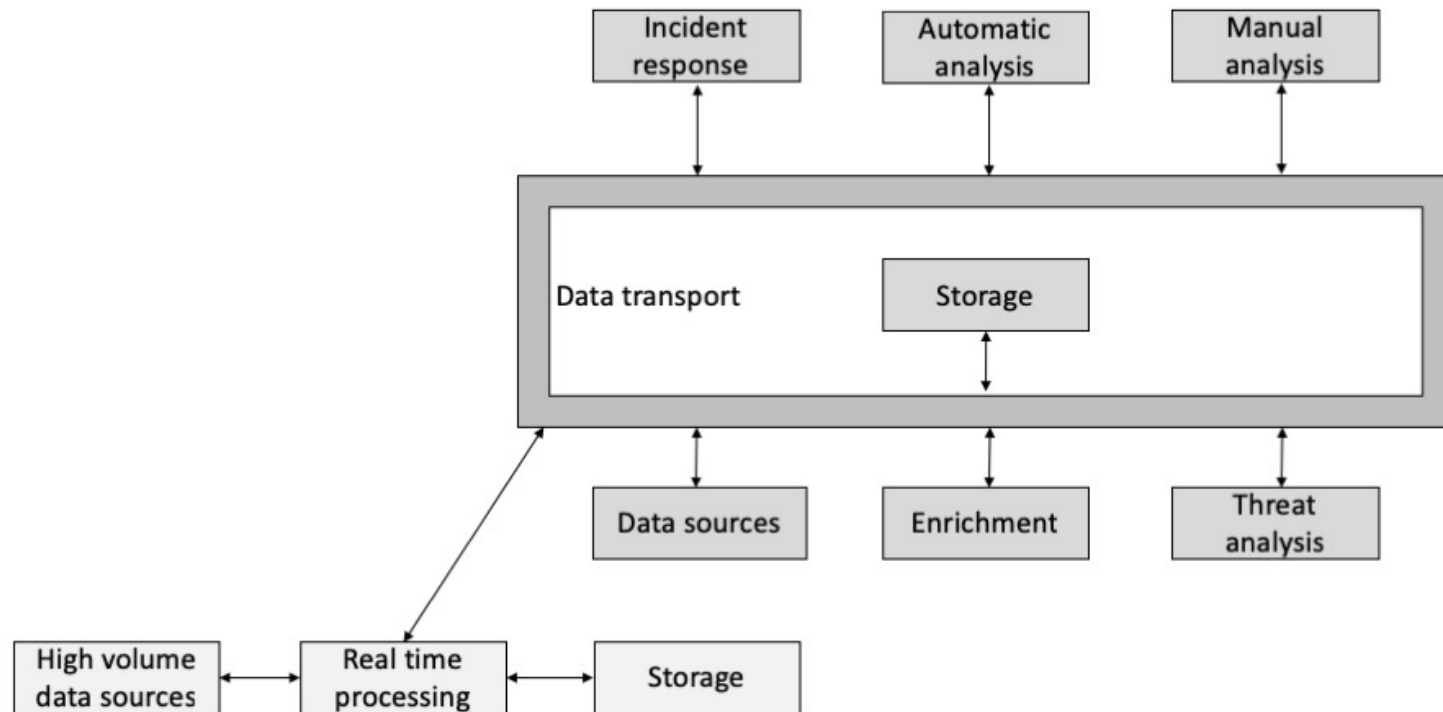
- “Cyber Threat Intelligence is **systematic collection, analysis and dissemination** of information pertaining to a company's operation in cyberspace and to an extent physical space. It is designed to inform all levels of **decision makers**. The analysis is designed to help keep **situational awareness** about current and arising **threats.**”

- <https://www.first.org/global/sigs/cti/curriculum/cti-introduction#A-working-definition-for-Cyber-Threat-Intelligence>

- “Cyber threat intelligence represents a **force multiplier** for organizations looking to update their response and detection programs to deal with increasingly sophisticated **advanced persistent threats**. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent **human threats** with empowered and trained **human defenders**.”
  - <https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/>

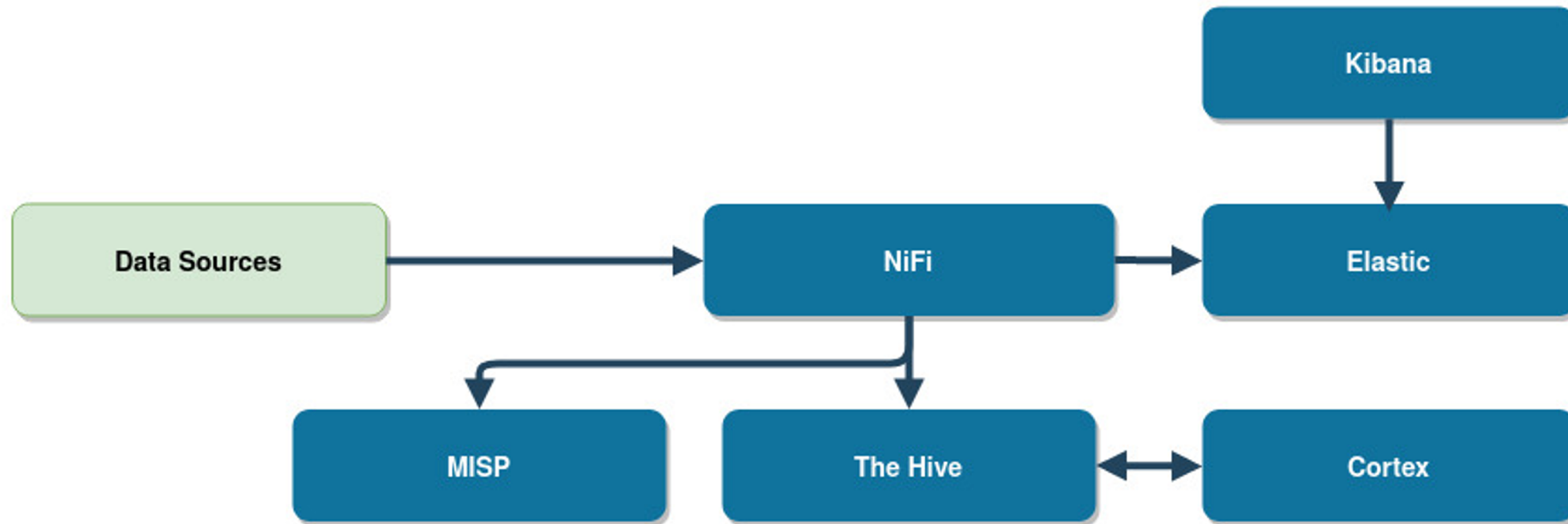
## SOCTools (1)

- SOCTools is a set of tools that can be used by a SOC for collecting and analysing security data, incident handling and threat intelligence



## SOCTools (2)

- data > normalisation > enrichment = actionable information!
- Incident report (ticketing) > threat intel. > analysis





## SOCTools (3)

- Installation and basic use

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

Close

Reset

Create Case

>

TheHive

My tasks 0

Waiting tasks 0

Alerts 0

Dashboards

Search

Case # 1 - demo

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

Details

Tasks 0

Observables 1

TTPs

Export

Filters

Add a filter

List of observables (1 of 1)

☐ Flags

Type

Value/Filename

ip

10[.]10[.]10[.]10

None

No reports available



[Home](#) [Event Actions](#) [Dashboard](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Logs](#) [API](#)

[List Events](#)  
[Add Event](#)

Last change2021-06-10 09:30:29



Modification map

Sightings0 (0) - restricted to own organisation only.

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

✕ 2: testevent




Galaxies









« previous

next »

view all

+   

Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool

<input type="checkbox"/>	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
<input type="checkbox"/>	2021-06-10		Network activity	domain	example.evil	 	 		<input checked="" type="checkbox"/>	
<input type="checkbox"/>	2021-06-10		Network activity	ip-dst	10.10.10.10	 	 		<input checked="" type="checkbox"/>	897

« previous

next »

view all

### Discussion

Quote Event Thread Link Code

## SOCTools – What's next for 2022?

- 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

## SOCTools – Where to start / how to get it?

- `soc-tools@lists.geant.org`
- <https://gitlab.geant.org/gn4-3-wp8-t3.1-soc/soctools>

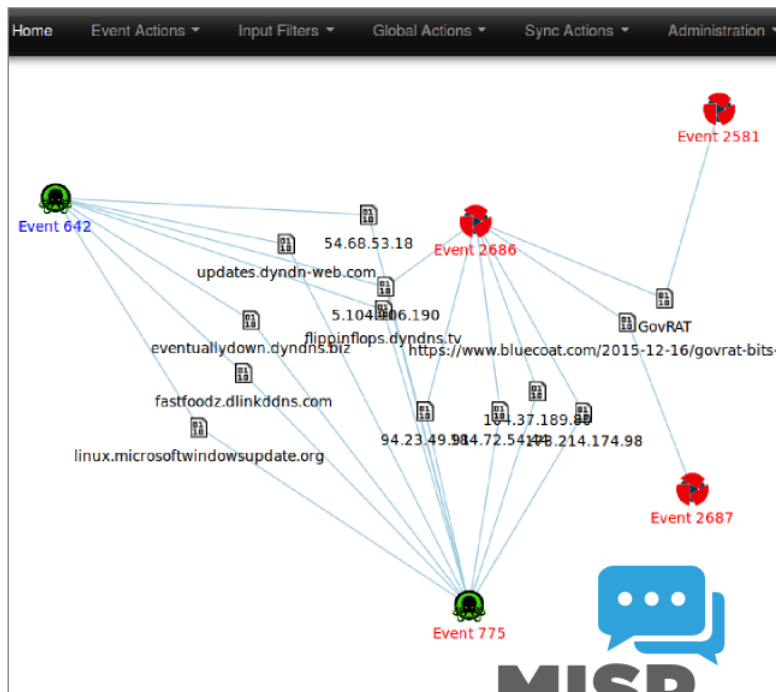
## R&E intelligence sharing and threat analysis



**MISP - Open Source Threat Intelligence Platform &  
Open Standards For Threat Information Sharing**

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





## TLP Taxonomy Library

Id	3
Namespace	tlp
Description	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
Version	1
Enabled	Yes (disable)

« previous next »

Tag	Expanded	Events	Tag	Action
<input type="checkbox"/> tlp:red	(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	
<input type="checkbox"/> tlp:amber	(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	
<input type="checkbox"/> tlp:green	(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	
<input type="checkbox"/> tlp:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	
<input type="checkbox"/> tlp:ex:chr	(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	

Id	Exportable	Name	Taxonomy	Tagged events	Actions
6	✗	APT		31	
7	✗	Actionable:NO		5	
3	✗	TLP:AMBER	tlp	131	
8	✗	TLP:EX:CHR	tlp	11	
5	✗	TLP:GREEN	tlp	550	
4	✗	TLP:RED	tlp	3	
2	✗	TLP:WHITE	tlp	531	
10	✗	TO:HIDE		2	
9	✗	TODO		9	
11	✗	TODO:VT-ENRICHMENT		8	
1	✗	Type:OSINT		832	
18	✓	admiralty-scale:information-credibility="1"	admiralty-scale	0	
19	✓	admiralty-scale:information-credibility="2"	admiralty-scale	0	
20	✓	admiralty-scale:information-credibility="3"	admiralty-scale	0	
21	✓	admiralty-scale:information-credibility="4"	admiralty-scale	0	
22	✓	admiralty-scale:information-credibility="5"	admiralty-scale	0	
23	✓	admiralty-scale:information-credibility="6"	admiralty-scale	0	

# 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).*

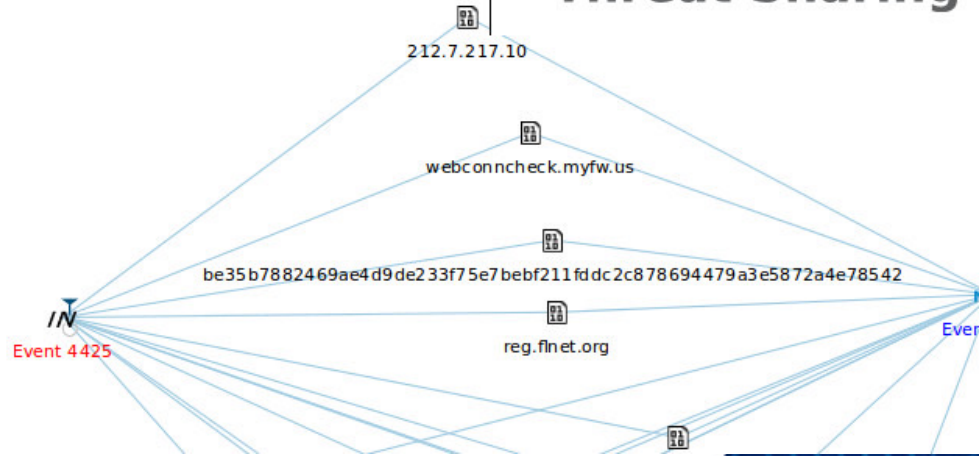
# OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Juid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner 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
Info	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 improbable - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

## Related Events

- 2016-05-27 (3883)
- 2016-05-23 (3844)
- 2016-05-06 (3828)
- Org: CIRCL
- Date: 2016-05-23
- Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware





## Getting started with MISP

- Install Guides: <https://misp.github.io/MISP/>
- MISP book: <https://www.circl.lu/doc/misp/quick-start/>
- <https://github.com/MISP/misp-training#misp-training-videos>

## (initial) Gotchas

- Use a separate partition for the DB
- How many instances
  - Synced with others?
  - integrated with IDS?
- Before subscribing to feeds, know what you're doing
  - Watch out for correlations...
  - Choose a taxonomy/framework – e.g. ENISA, VERIS, etc.
- <https://github.com/MISP/MISP/issues>
- <https://gitter.im/MISP/Support>

Remember

# Sharing is caring

- For you and for others

## Starting your own SOC

1. You need a team, incl. some analysts 😊
2. Decide on services
3. Choose tools to support those
  - Note: configuration, workflows, etc. is the bulk of the work!
4. Start using the tools – subscribe to feeds, create events/tickets, launch!



## What about a SIEM?

- OSS, Commercial, Cloud?
- Elastic SIEM
- AlienVault OSSIM
- Splunk
- ...

## Data sources

- Logs
- Honeypots
- IDS/Firewall
- pcap
- Flow data
- Host-based: AV, IDS
- DNS

# Special Mention – Wazuh!

[Product](#)[Documentation](#)[Cloud](#)[Services](#)[Company▼](#)[Blog](#)[Log in](#)

## The Open Source Security Platform

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.

[Install Wazuh](#)[Free Cloud Trial](#)

### Get started with Wazuh

Wazuh provides host-based security visibility using lightweight multi-platform agents.



### Wazuh is open source

Flexible, scalable, no vendor lock-in and no license cost. Trusted by thousands of users.



### How can we help you?

Wazuh provides professional support, training and consulting services.

## Useful Resources

- **MITRE: Ten Strategies of a World-Class Cybersecurity Operations Center**
  - Carson Zimmerman, 2014
- **Creating security operations centres that work**
  - Steve Mansfield-Devine, *editor*, Network Security
- **SANS: Building a World-Class Security Operations Center: A Roadmap**
  - Alissa Torres, 2015



# FIRST Academic Security SIG

**Worldwide platform for collaboration of  
Research & Education security teams**

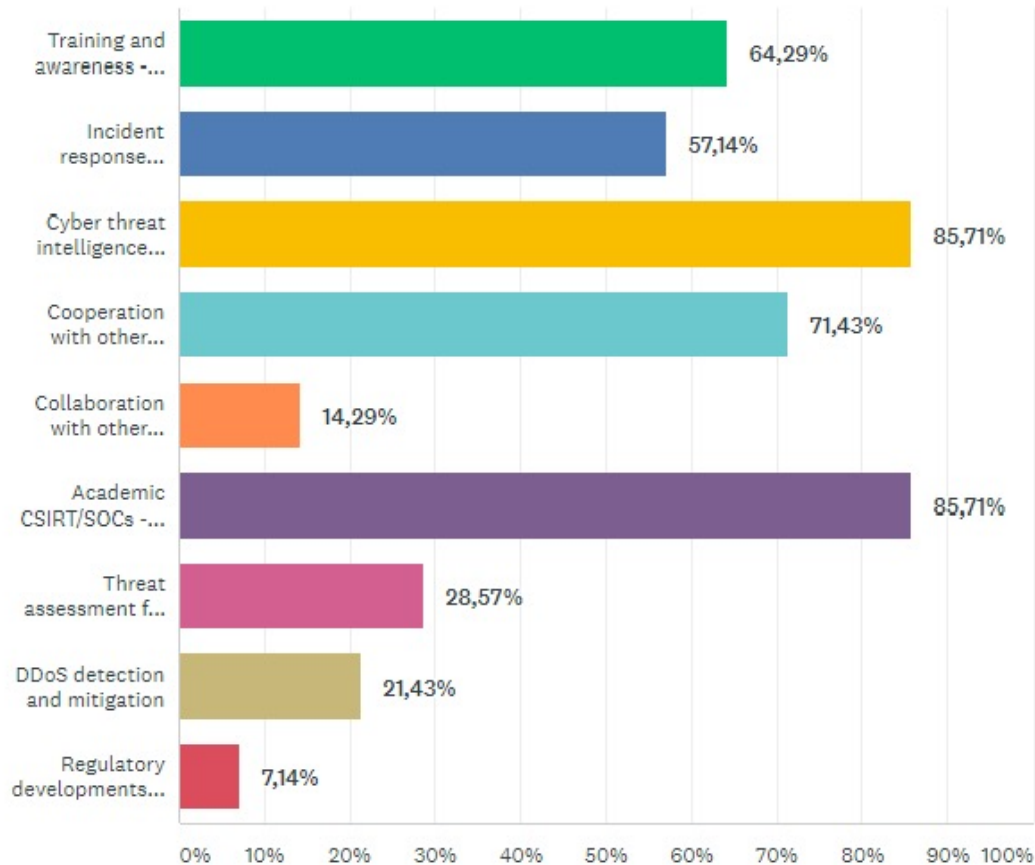
## **Primary target:**

- NREN & University security personnel
- Research & Education SOC/CSIRTs in general

## **Resources:**

- SIG mailing list
- SIG wiki @FIRST Portal (SIG members-only)
- SIG meetings (virtual + annual FIRST conference)

# 2021: New SIG Working Groups



SIG should focus on:

Cyber threat intelligence

Academic CSIRTs/SOCs

Cooperation with other similar regional and global initiatives

Training and awareness

Incident response coordination

<https://www.first.org/global/sigs/academicsec>



# What about?

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



News & Insights   Statistics   Become a Sponsor

WHO WE ARE   WHAT WE DO   WHO

Home > What We Do > Network Reporting



## 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!

Questions?

[www.geant.org](http://www.geant.org)

