GÉANT

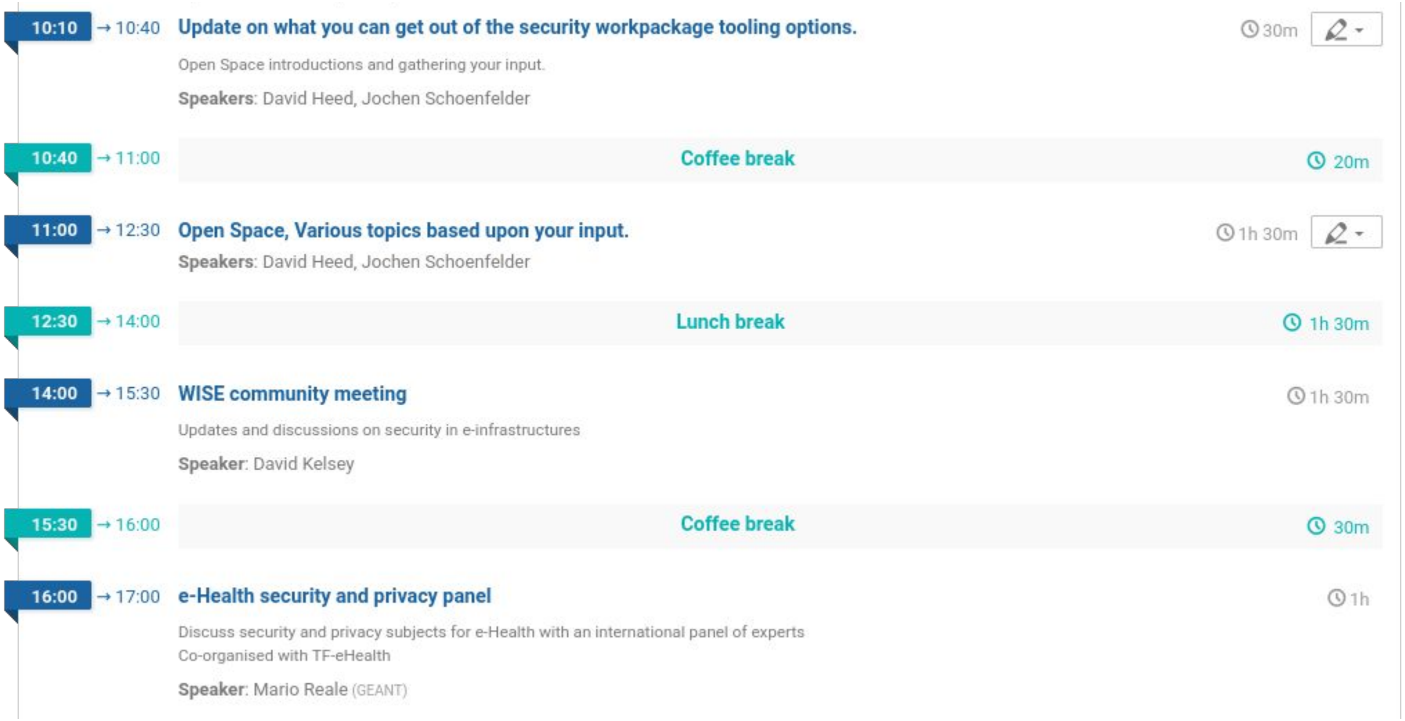
Security Day @TNC22

17 June 2022

tnc22
NAVIGATING THE UNEXPLORED

Trieste, Italy | **13-17 June 2022**

Agenda



10:10 → 10:40 **Update on what you can get out of the security workpackage tooling options.** 30m

Open Space introductions and gathering your input.

Speakers: David Heed, Jochen Schoenfelder

10:40 → 11:00 **Coffee break** 20m

11:00 → 12:30 **Open Space, Various topics based upon your input.** 1h 30m

Speakers: David Heed, Jochen Schoenfelder

12:30 → 14:00 **Lunch break** 1h 30m

14:00 → 15:30 **WISE community meeting** 1h 30m

Updates and discussions on security in e-infrastructures

Speaker: David Kelsey

15:30 → 16:00 **Coffee break** 30m

16:00 → 17:00 **e-Health security and privacy panel** 1h

Discuss security and privacy subjects for e-Health with an international panel of experts
Co-organised with TF-eHealth

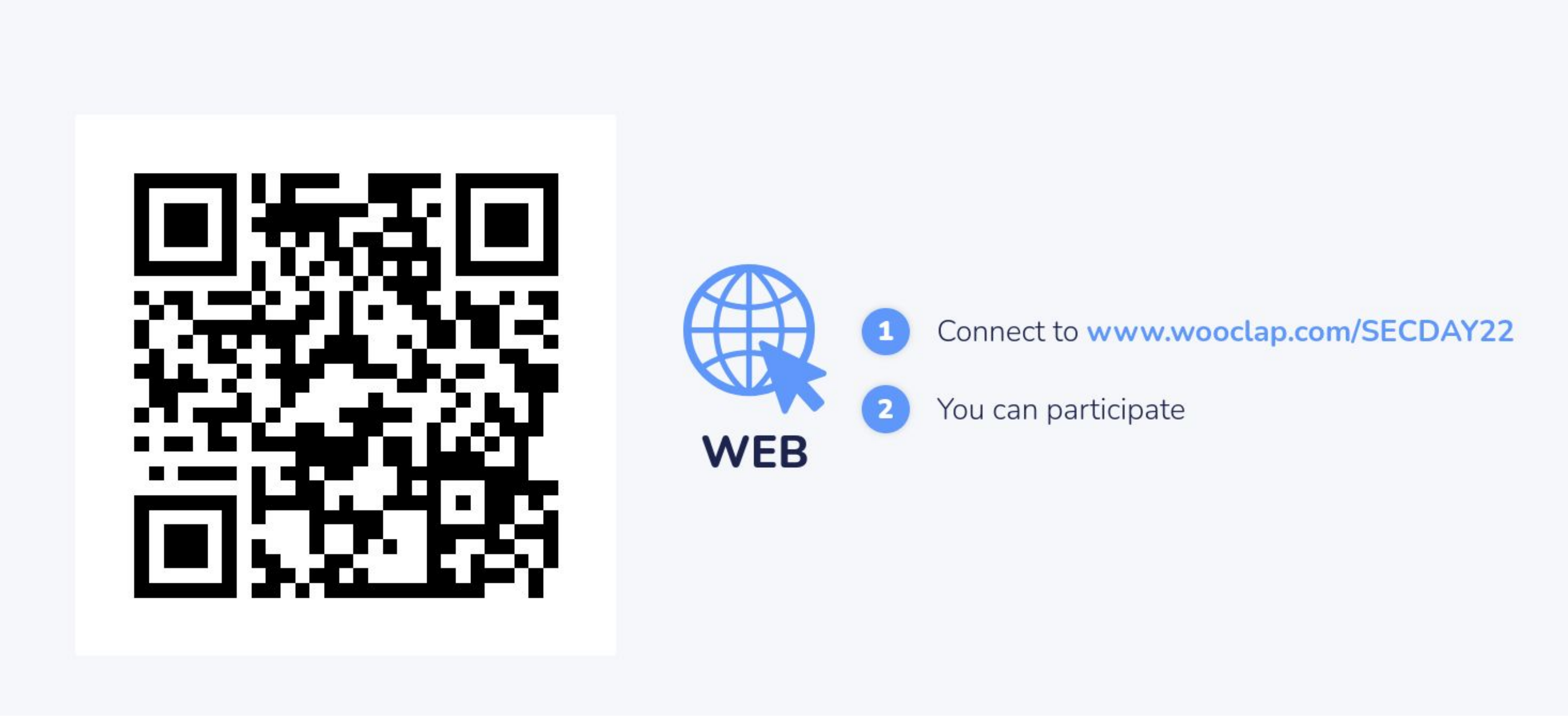
Speaker: Mario Reale (GEANT)

Agenda

Overview of products and services and other activities from the security work package.

What can you get now and collaborate on.

A reminder… please suggest topics for the Open Space



1. Connect to www.wooclap.com/SECDAY22
2. You can participate

Baseline & BCM report

Security baseline offers 3 maturity levels to aim to

- 1 is for starters, 2 advanced, 3 is where we all want to be
- get points within the assessment sheet, and see how you stand

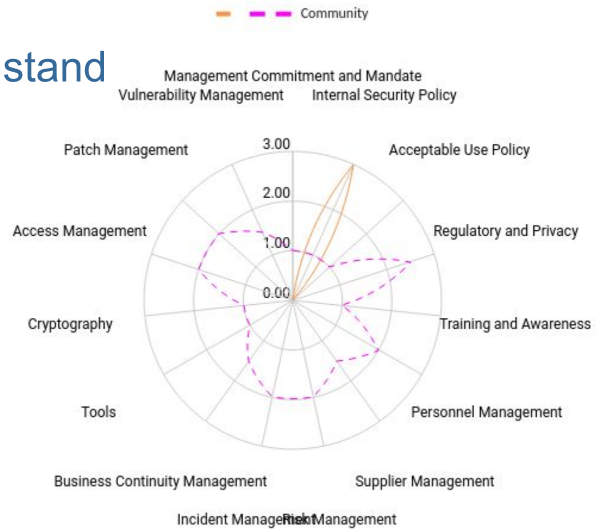
Assessment sheet is available:

- https://security.geant.org/baseline/

Additional resources upon request

Contact if you want to know more:

- michael.schmidt@lrz.de



Claw

What is this about?

- Learning how to deal with and prepare for crises!

Who is this for?

- All the people in an NREN that might have to deal with a crisis one day.
- So: NOC, Communications, CSIRT, Management, Service Owners..
- it's not for you if you will never ever have any crisis whatsoever!

Where can I book a CLAWS training?

- Via Indico: https://events.geant.org/event/1193/
- everyone from a member organisation can book ths

What does it cost?

- There is no fee to attend, your organisation just needs to approve your time and travel

Who shall I contact if I want to know more?

- Charlie van Genuchten , charlie.vangenuchten@surf.nl

Training materials

A lot of trainings have been done

- IT Forensics for System administrators I+II, Vulnerability Management, DDoS protection, Client Privacy & Security, Operational Network Security
- more details & video recordings: https://security.geant.org/training/

More trainings to come

- see GN5-1

Material for a CTF-like Self Online Practical Training is available on te wiki

- contact if you need direction or access

Contact point

- Sarunas Grigaliunas sarunas@litnet.it

Products and services from the work package

❑ Firewall on demand

❑ eduVPN

❑ Vulnerability assessment

❑ NeMo DDoS

❑ SOC-tools

Firewall on demand

There is a GÉANT FoD installation:

- Self-service for injecting BGP FlowSpec rules on the GEANT routers
- no need to contact the GEANT NOC admins for the particular mitigations
- access to per 5 min statistics (dropped packets/bytes)

how do I get access?

- ask partner-relations@geant.net for GÉANT FoD access

For local installations:

- router hw needed with BGP FlowSpec + FlowSpec-specific NETCONF YANG model
- server / VM for FoD: e.g. with 8GB RAM, 1 CPU, 10GB disk space

Contact points:

- gn4-3-wp8-fod@lists.geant.org / fod@lists.geant.org

eduVPN

Who can deploy it?

- institutions / universities for remote VPN access
- NRENs for secure Internet access

How to join:

- https://www.eduvpn.org/join/

eduVPN 3.0 was released some weeks ago:

- lot’s of improvements for stability, redundancy and code simplification
- WireGuard now is supported alongside OpenVPN

eduVPN

Adaption:

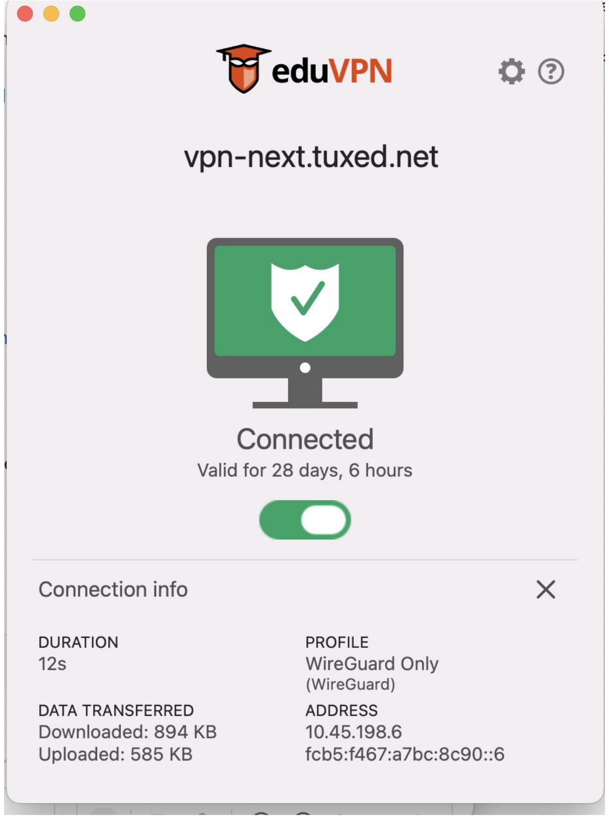
- over 110 universities / institutions
- 17 country servers

Future plans:

- pre-provisioning: start the VPN ahead of the user session

More information:

- eduvpn-support@lists.geant.org
- Tangui Coulouarn: tacou@dtu.dk



vpn-next.tuxed.net

Connected

Valid for 28 days, 6 hours

Connection info

DURATION
12s

PROFILE
WireGuard Only
(WireGuard)

DATA TRANSFERRED
Downloaded: 894 KB
Uploaded: 585 KB

ADDRESS
10.45.198.6
fcb5:f467:a7bc:8c90::6

Vulnerability assessment

Open Source version / Pilot system

Online plattform based on OpenVAS

External scanner (hosted at SUNET)

Published as a service provider with GÉANT

Additional feed from Holm security will be automatically updated for service

Source code of contribution/fork:
https://gitlab.geant.org/vulnerabilityassessment

Commercial service

Procurement open for bidding at this moment

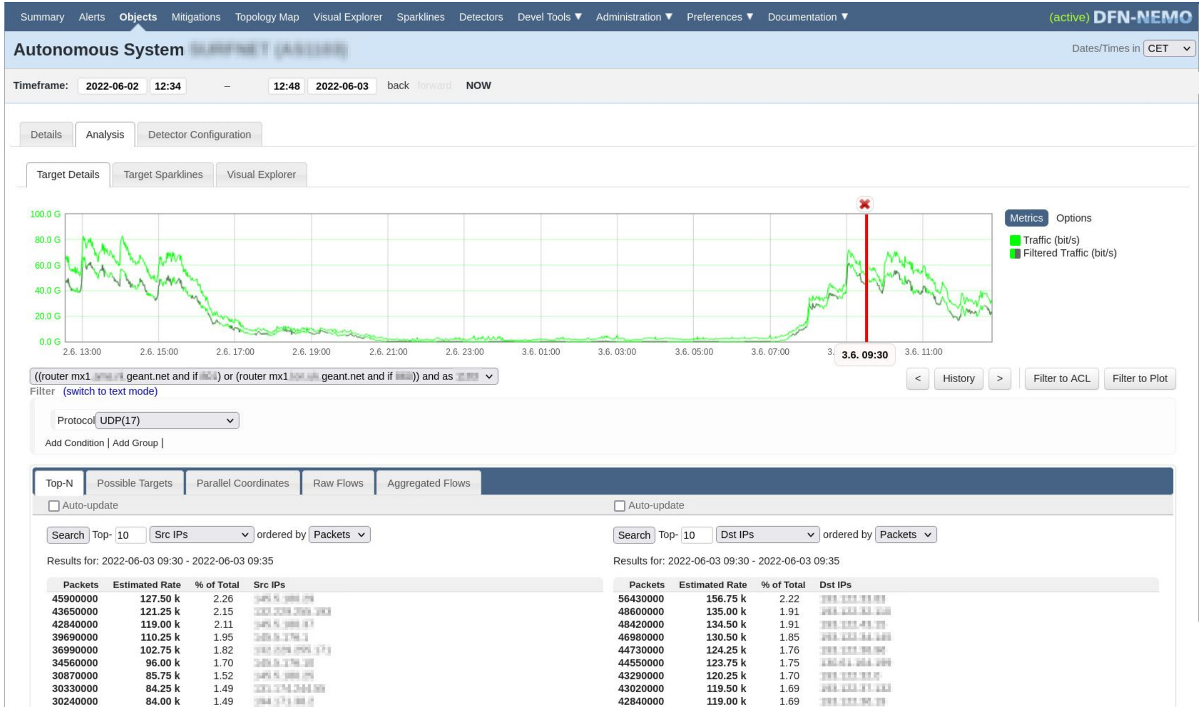
Evaluation weights:

Scanning capability excellence	15%
Scanning control excellence	10%
Feeds, quality and dashboard	10%
Community contribution	15%
Price	50%

Contact point: david@sunet.se

DDoS

- NeMo-DDoS is available for download as a full featured DDoS detection system
- container-based fast-track installation
- comes with NetFlow / IPfix-support for standard routers out there
- install in your own network
- strong flow analysis platform



Autonomous System [redacted]

Dates/Times in CET

Timeframe: 2022-06-02 12:34 – 12:48 2022-06-03 back forward NOW

Filter ((router mx1 [redacted] geant.net and if [redacted]) or (router mx1 [redacted] geant.net and if [redacted])) and as [redacted]
(switch to text mode)

Protocol UDP(17)

□ Auto-update

Top- 10 Src IPs ordered by Packets

Results for: 2022-06-03 09:30 - 2022-06-03 09:35

Packets	Estimated Rate	% of Total	Src IPs
45900000	127.50 k	2.26	[redacted]
43650000	121.25 k	2.15	[redacted]
42840000	119.00 k	2.11	[redacted]
39690000	110.25 k	1.95	[redacted]
36990000	102.75 k	1.82	[redacted]
34560000	96.00 k	1.70	[redacted]
30870000	85.75 k	1.52	[redacted]
30330000	84.25 k	1.49	[redacted]
30240000	84.00 k	1.49	[redacted]

□ Auto-update

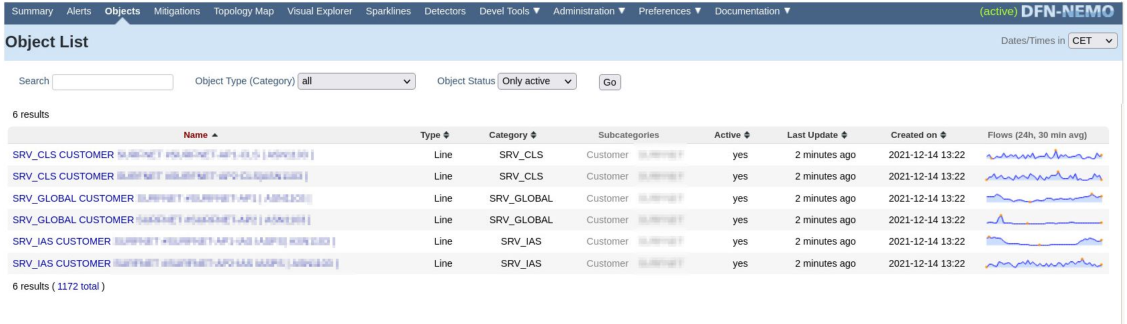
Top- 10 Dst IPs ordered by Packets

Results for: 2022-06-03 09:30 - 2022-06-03 09:35

Packets	Estimated Rate	% of Total	Dst IPs
56430000	156.75 k	2.22	[redacted]
48600000	135.00 k	1.91	[redacted]
48420000	134.50 k	1.91	[redacted]
46980000	130.50 k	1.85	[redacted]
44730000	124.25 k	1.76	[redacted]
44550000	123.75 k	1.75	[redacted]
43290000	120.25 k	1.70	[redacted]
43020000	119.50 k	1.69	[redacted]
42840000	119.00 k	1.69	[redacted]

DDoS

- GÉANT installation in progress
- see your traffic!



Object List

Dates/Times in CET

Search

Object Type (Category) all

Object Status Only active

Go

6 results

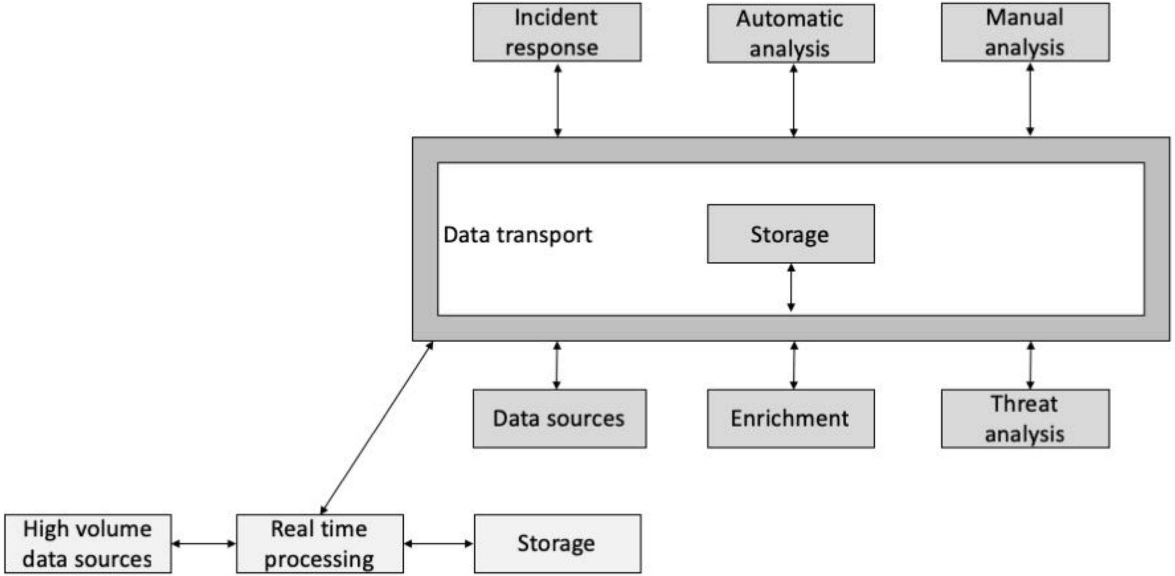
Name ▲	Type ⬍	Category ⬍	Subcategories	Active ⬍	Last Update ⬍	Created on ⬍	Flows (24h, 30 min avg)
SRV_CLS CUSTOMER [redacted]	Line	SRV_CLS	Customer [redacted]	yes	2 minutes ago	2021-12-14 13:22	
SRV_CLS CUSTOMER [redacted]	Line	SRV_CLS	Customer [redacted]	yes	2 minutes ago	2021-12-14 13:22	
SRV_GLOBAL CUSTOMER [redacted]	Line	SRV_GLOBAL	Customer [redacted]	yes	2 minutes ago	2021-12-14 13:22	
SRV_GLOBAL CUSTOMER [redacted]	Line	SRV_GLOBAL	Customer [redacted]	yes	2 minutes ago	2021-12-14 13:22	
SRV_IAS CUSTOMER [redacted]	Line	SRV_IAS	Customer [redacted]	yes	2 minutes ago	2021-12-14 13:22	
SRV_IAS CUSTOMER [redacted]	Line	SRV_IAS	Customer [redacted]	yes	2 minutes ago	2021-12-14 13:22	

6 results (1172 total)

- Software lives on GÉANT’s gitlab
- mitigation capabilities upcoming
- “satellite” setup capabilities planned
- contact points:
  - partner-relations@geant.net
  - ddos@lists.geant.org

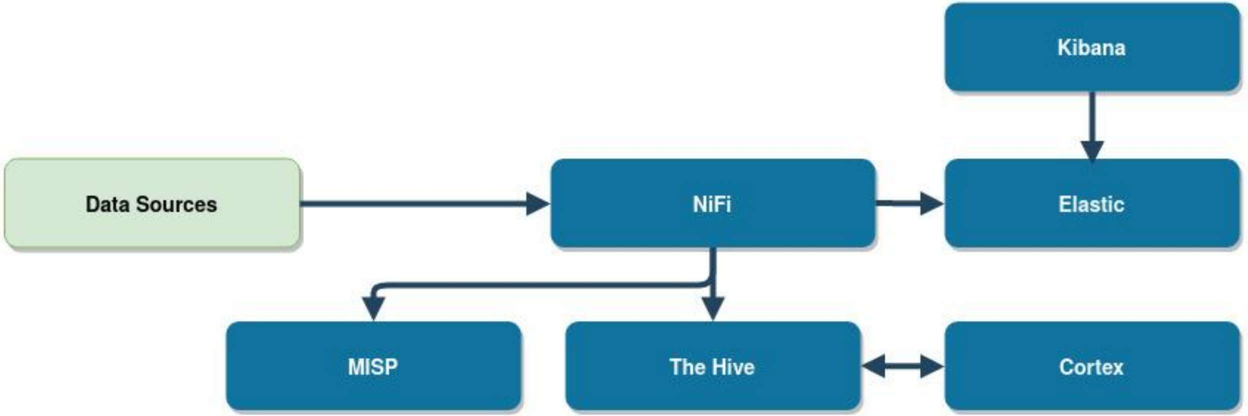
SOCTools

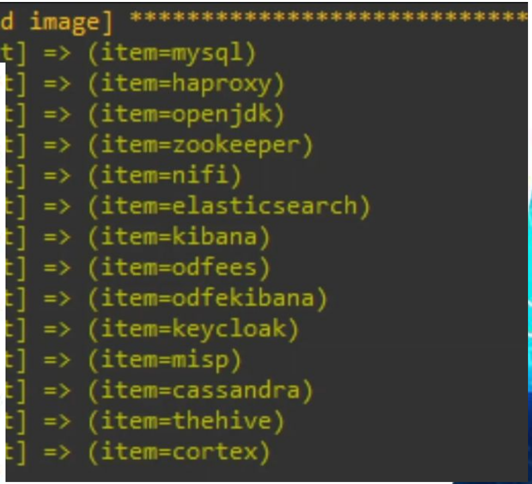
- a interconected set of tools that can be used by a SOC for collecting and analysing security data, incident handling and threat intelligence



SOCTools (2)

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





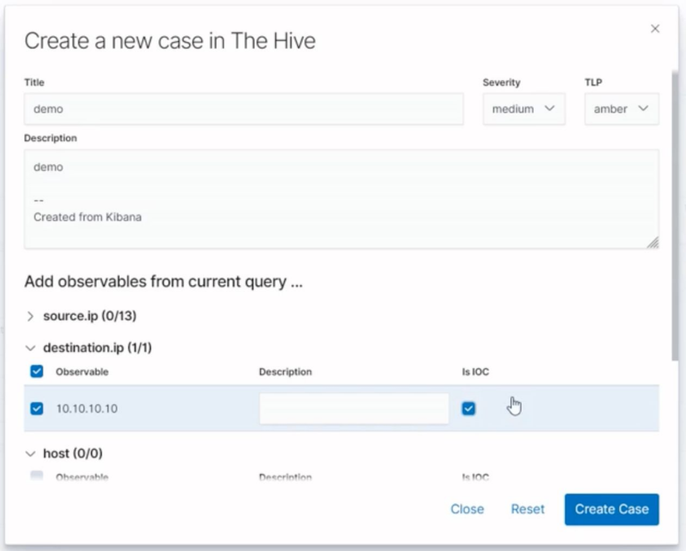
```
TASK [build : Build image] ***************************
changed: [localhost] => (item=mysql)
t] => (item=haproxy)
t] => (item=openjdk)
t] => (item=zookeeper)
t] => (item=nifi)
t] => (item=elasticsearch)
t] => (item=kibana)
t] => (item=odfees)
t] => (item=odfekibana)
t] => (item=keycloak)
t] => (item=misp)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

SOCTools – Where to start / how to get it?

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

- Upcoming report (June/July):
  - “Best practices for security operations in research and education”
  - find it on GÉANT’s deliverable page
  - also to appear on: https://security.geant.org/

Kibana > The Hive > MISP …



Create a new case in The Hive

Title	Severity	TLP
demo	medium	amber

Description

demo

--
Created from Kibana

Add observables from current query ...

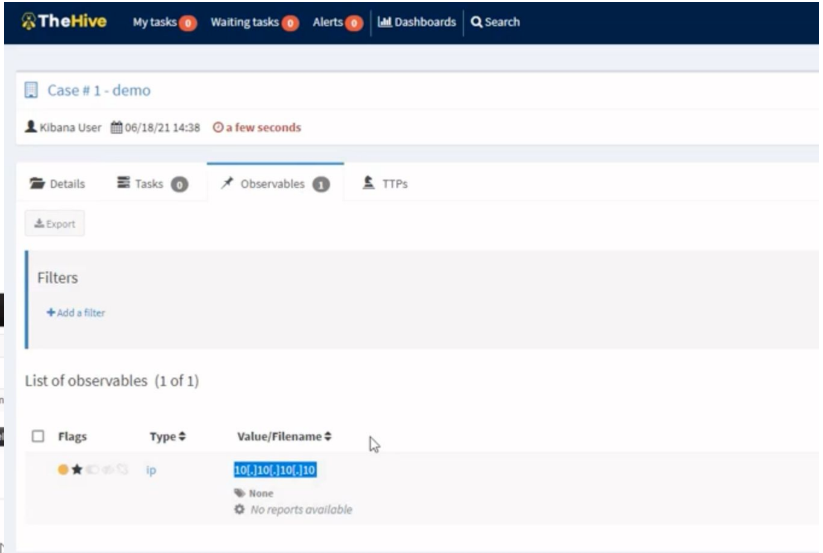
- source.ip (0/13)
- destination.ip (1/1)

☑ Observable	Description	Is IOC
☑ 10.10.10.10		☑

- host (0/0)

Observable	Description	Is IOC

>

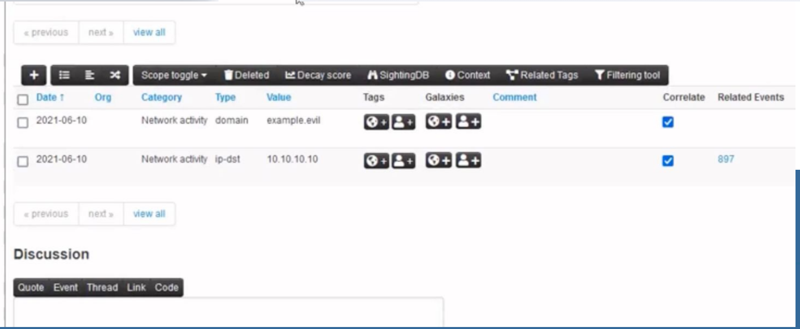


Case # 1 - demo

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

List of observables (1 of 1)

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



☐	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

tnc22 NAVIGATING THE UNEXPLORED

GÉANT

Secure Coding Training 2022: 5th-8th September, virtually

What is it?

Training on how to develop (mainly Web) secure applications

Who organizes it?

WP9T2 + GLAD Team

When?

5-8.09 (Mon-Thu)
10:00-14:00 CEST

Where?

This year at your desk again: a fully virtual training

How to know **more**?

Registration:
https://events.geant.org/event/691/registrations/561/
GÉANT Wiki:
https://wiki.geant.org/display/GSD/Secure+Code+Training
E-mail: Gerard Frankowski, PSNC: gerard@man.poznan.pl

What will be covered?

- OWASP ASVS 4.0.3 areas
- CI/CD and SDLC
- Static analysis tools
- Fuzzing tests workshop
- HackMe contest

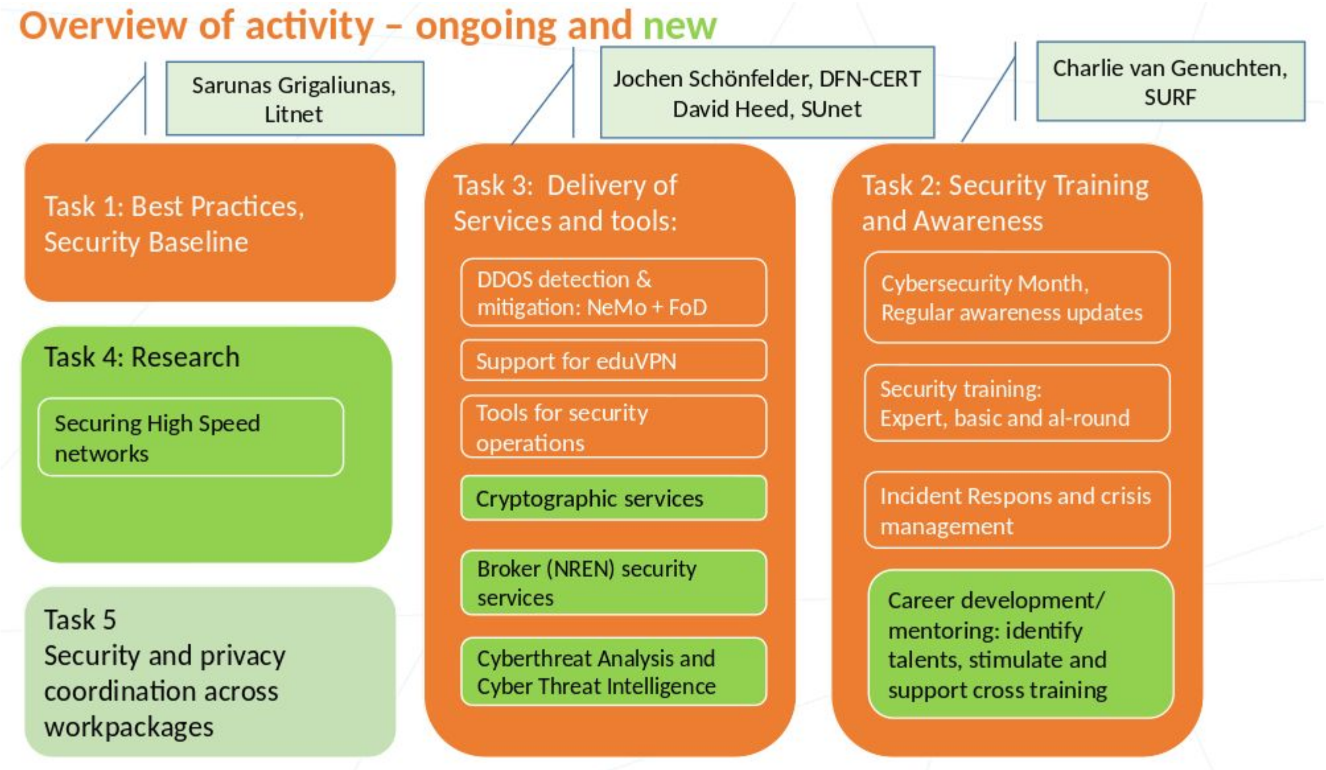
What ASVS areas?

- Validation, Sanitization and Encoding
- Data protection
- Miscellaneous

Social event?

SCT 2022 is virtual but we'll have prizes (:

Future of work package



Overview of activity – ongoing and new

Sarunas Grigaliunas, Litnet

Task 1: Best Practices, Security Baseline

Task 4: Research

- Securing High Speed networks

Task 5
Security and privacy coordination across workpackages

Jochen Schönfelder, DFN-CERT
David Heed, SUnet

Task 3: Delivery of Services and tools:

- DDOS detection & mitigation: NeMo + FoD
- Support for eduVPN
- Tools for security operations
- Cryptographic services
- Broker (NREN) security services
- Cyberthreat Analysis and Cyber Threat Intelligence

Charlie van Genuchten, SURF

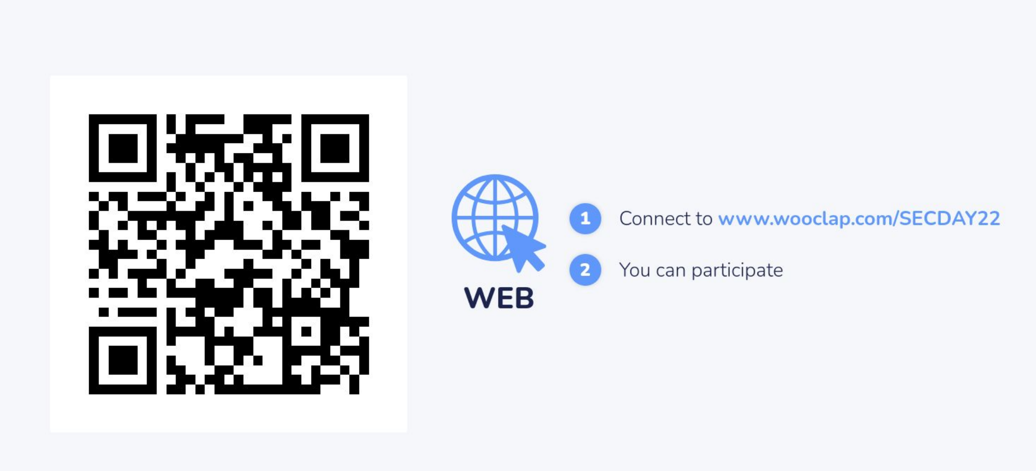
Task 2: Security Training and Awareness

- Cybersecurity Month, Regular awareness updates
- Security training: Expert, basic and al-round
- Incident Respons and crisis management
- Career development/ mentoring: identify talents, stimulate and support cross training

Open space preparations

How will Open Space work?

- Submit ideas and vote/like existing ones!
- We’ll take the top topics, discussing them in serial.
  - be prepared to moderate a topic you submitted! :)
- Time range will be from coffee break till lunch
  - we’ll close voting in a few, so that we can start then.



WEB

1 Connect to www.wooclap.com/SECDAY22

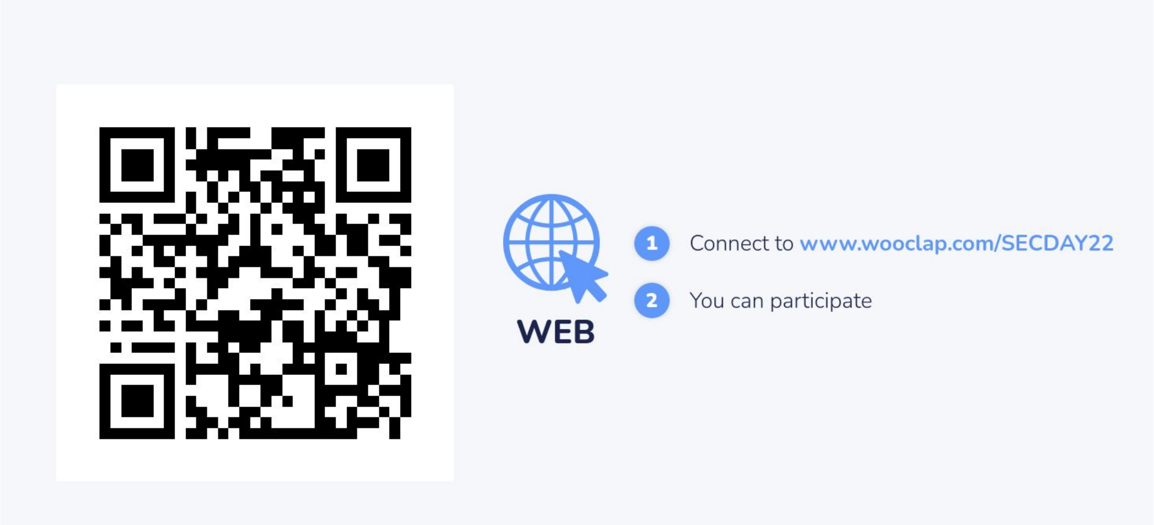
2 You can participate

Thank you

Any Questions?

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).

if you haven’t voted yet:



1 Connect to www.wooclap.com/SECDAY22

2 You can participate

also: do you want to moderate one of the topics?