<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:10</td>
<td>Update on what you can get out of the security workpackage tooling options.</td>
<td>30m</td>
</tr>
<tr>
<td>10:40</td>
<td>Coffee break</td>
<td>20m</td>
</tr>
<tr>
<td>11:00</td>
<td>Open Space, Various topics based upon your input.</td>
<td>1h 30m</td>
</tr>
<tr>
<td>11:30</td>
<td>Lunch break</td>
<td>1h 30m</td>
</tr>
<tr>
<td>14:00</td>
<td>WISE community meeting</td>
<td>1h 30m</td>
</tr>
<tr>
<td>15:30</td>
<td>Coffee break</td>
<td>30m</td>
</tr>
<tr>
<td>16:00</td>
<td>e-Health security and privacy panel</td>
<td>1h</td>
</tr>
</tbody>
</table>

**Speakers:**
- David Heed, Jochen Schoenfelder
- David Kelsey
- Mario Reale (GEAHT)
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

- 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
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
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
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
DDoS

- GÉANT installation in progress
- see your traffic!

- 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 interconnected 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
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 …
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/
- 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

Task 1: Best Practices, Security Baseline
- Sarunas Grigaliunas, Litnet

Task 2: Security Training and Awareness
- Cybersecurity Month, Regular awareness updates
- Security training: Expert, basic and all-round
- Incident Response and crisis management
- Career development/mentoring: identify talents, stimulate and support cross training
- Charlie van Genuchten, SURF

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
- Cyber threat Analysis and Cyber Threat Intelligence
- Jochen Schönfelder, DFN-CERT
- David Heed, SUNet

Task 4: Research
- Securing High Speed networks

Task 5: Security and privacy coordination across workpackages

TNC22: TOWARDS THE UNEXPLORED
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.
Thank you

Any Questions?
if you haven’t voted yet:

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

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