GÉANT
Networks • Services • People

Safe and Secure
Research and Education Networking

Roderick Mooi
Senior Information Security Officer @ GÉANT

15 September 2022

RoEduNet Conference

www.geant.org

Agenda

Who Am I?

About GÉANT

National and International collaborations in Security

GN4-3 > 5-1 Work Package 8: Security

Security Awareness, Training and Crisis management

GÉANT: DDoS Cleansing and Alerting Future

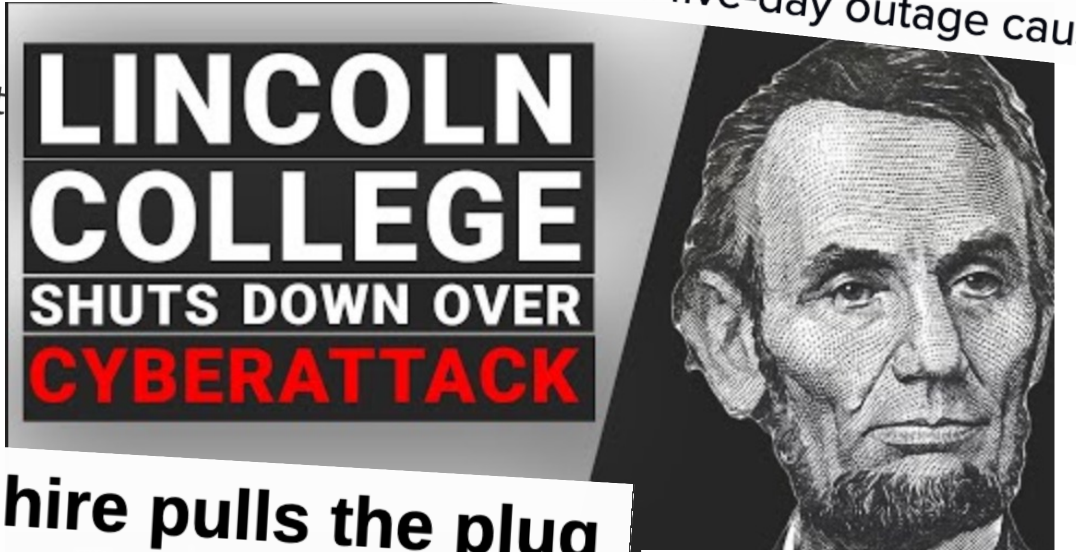
But first, why is security important?

2021 Attacks

Howard University cancels classes after ransomware attack

Brown University hit by cyberatt
some systems still offline

Data Breach at University of Kentucky



University of Hertfordshire pulls the plug on, well, everything after cyber attack

Educational institution ROC Mondriaan in The Hague victim of major cyber attack

AUAS and UvA target of cyber attack

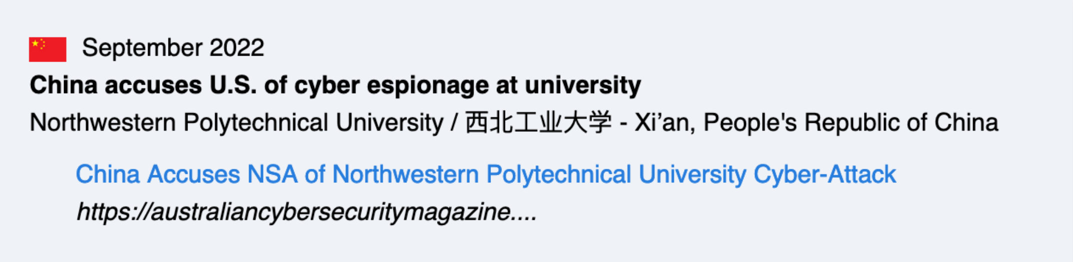
University still recovering from major cyberattack that disrupted IT systems

The University of Sunderland brings some IT systems back online after a five-day outage caused by a cyberattack.

Swinburne University confirms
5,000 individuals affected in d

University of California data breach: Sensitive information of staff, students leaked

Cyber attack disrupts services at University of the Highlands and Islands



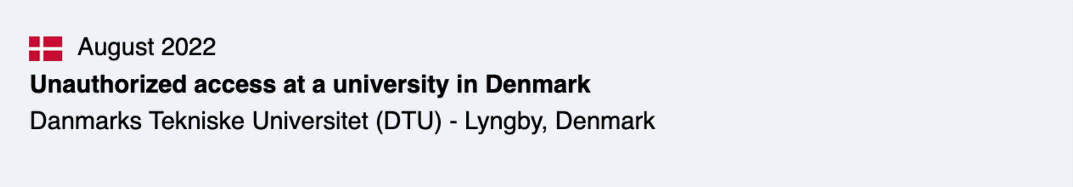
September 2022

China accuses U.S. of cyber espionage at university

Northwestern Polytechnical University / 西北工业大学 - Xi’an, People's Republic of China

China Accuses NSA of Northwestern Polytechnical University Cyber-Attack

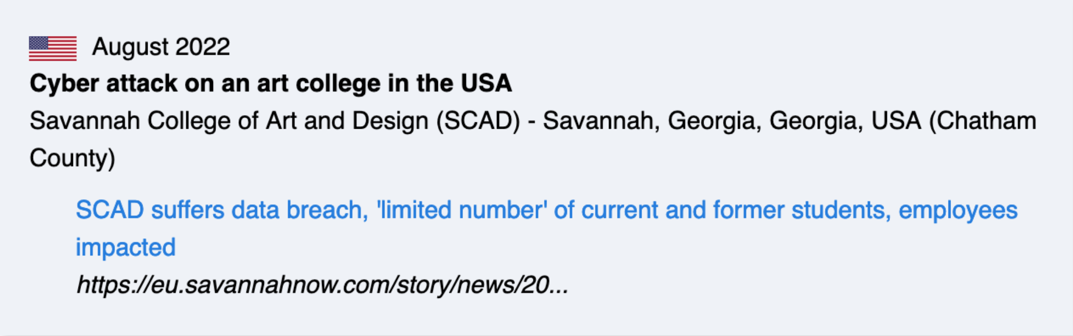
https://australiancybersecuritymagazine....



August 2022

Unauthorized access at a university in Denmark

Danmarks Tekniske Universitet (DTU) - Lyngby, Denmark



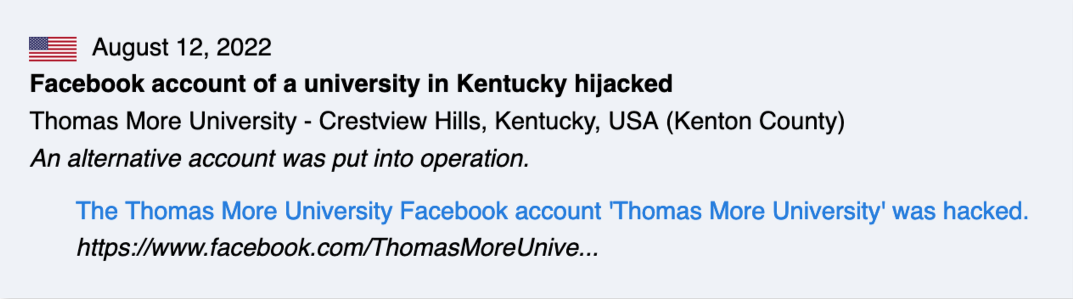
August 2022

Cyber attack on an art college in the USA

Savannah College of Art and Design (SCAD) - Savannah, Georgia, Georgia, USA (Chatham County)

SCAD suffers data breach, 'limited number' of current and former students, employees impacted

https://eu.savannahnow.com/story/news/20...



August 12, 2022

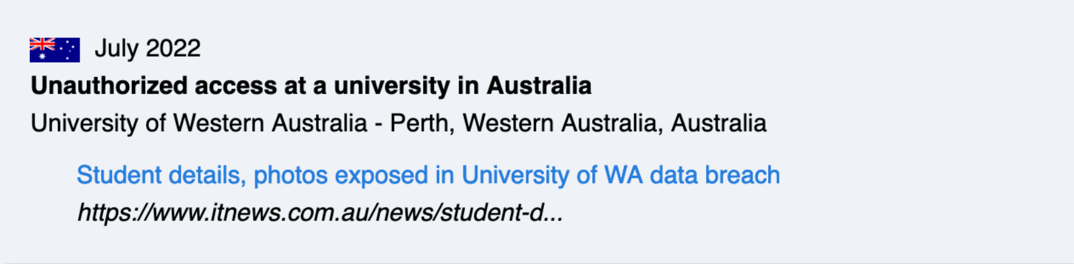
Facebook account of a university in Kentucky hijacked

Thomas More University - Crestview Hills, Kentucky, USA (Kenton County)

An alternative account was put into operation.

The Thomas More University Facebook account 'Thomas More University' was hacked.

https://www.facebook.com/ThomasMoreUnive...



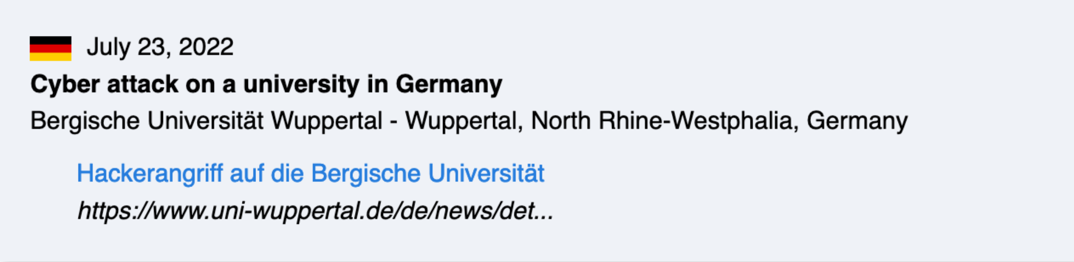
July 2022

Unauthorized access at a university in Australia

University of Western Australia - Perth, Western Australia, Australia

Student details, photos exposed in University of WA data breach

https://www.itnews.com.au/news/student-d...



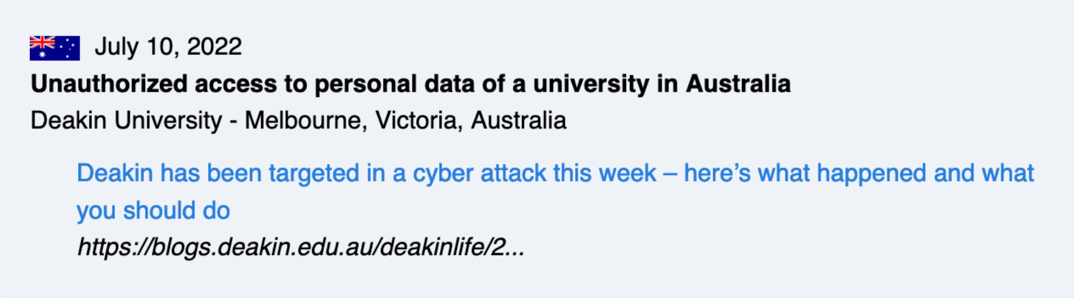
July 23, 2022

Cyber attack on a university in Germany

Bergische Universität Wuppertal - Wuppertal, North Rhine-Westphalia, Germany

Hackerangriff auf die Bergische Universität

https://www.uni-wuppertal.de/de/news/det...



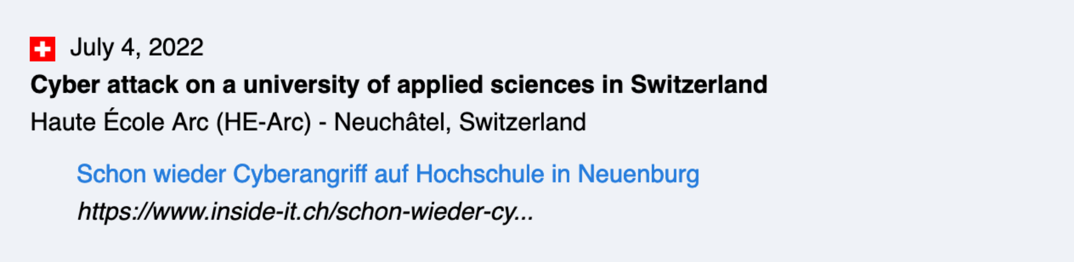
July 10, 2022

Unauthorized access to personal data of a university in Australia

Deakin University - Melbourne, Victoria, Australia

Deakin has been targeted in a cyber attack this week – here’s what happened and what you should do

https://blogs.deakin.edu.au/deakinlife/2...



July 4, 2022

Cyber attack on a university of applied sciences in Switzerland

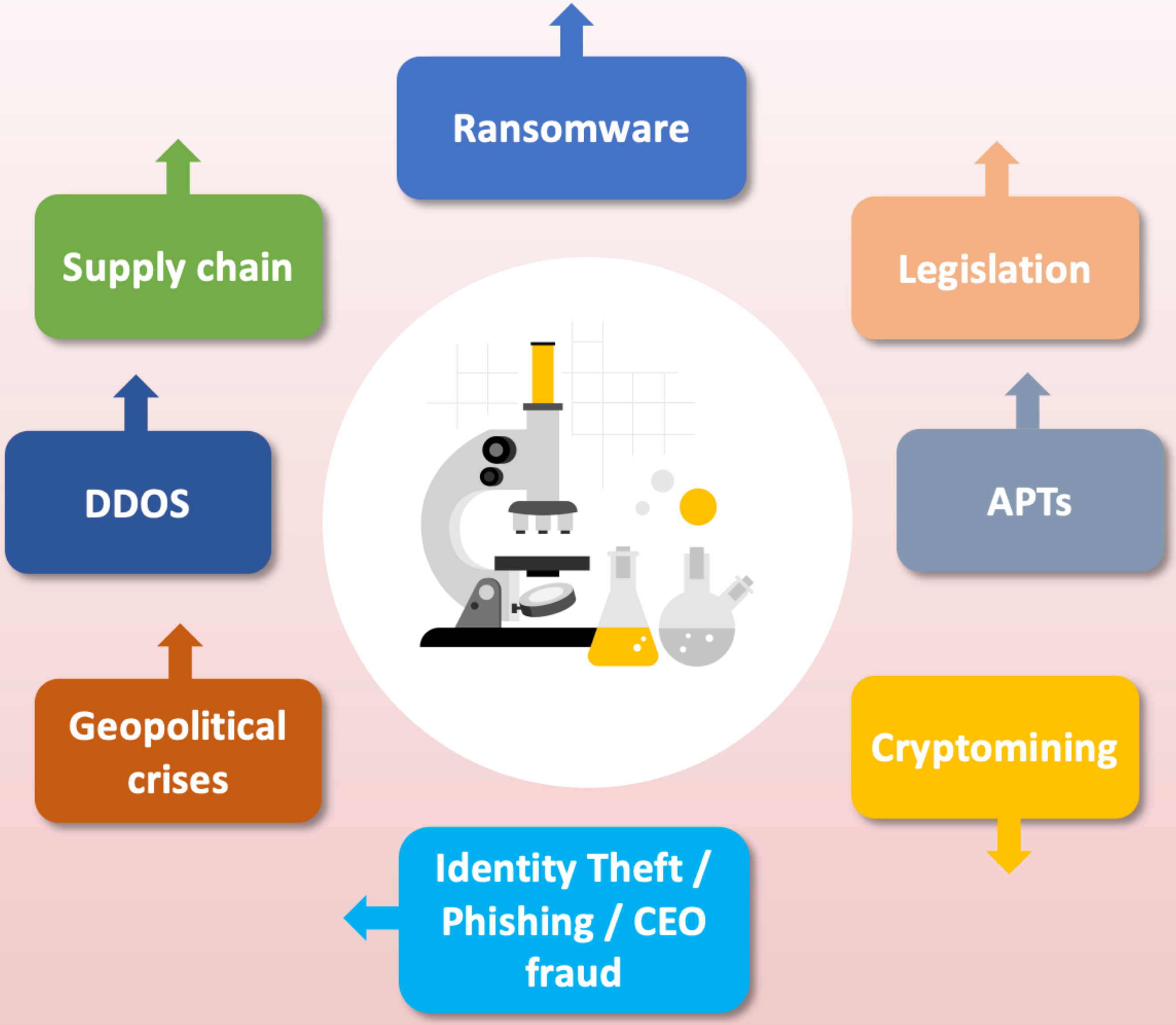
Haute École Arc (HE-Arc) - Neuchâtel, Switzerland

Schon wieder Cyberangriff auf Hochschule in Neuenburg

https://www.inside-it.ch/schon-wieder-cy...

https://konbriefing.com/en-topics/cyber-attacks-universities.html

THREATS + CHALLENGES



- Ransomware
- Legislation
- APTs
- Cryptomining
- Identity Theft / Phishing / CEO fraud
- Geopolitical crises
- DDOS
- Supply chain

- Boundaries & Borders
- Laws & Regulations
- Standards & Processes
- Resources & Skills
- Time & lack of Automation
- Different levels of Maturity

Working together to get things done

Why should you invest in building relations?

Why should you give away stuff you developed with a lot of blood, sweat and tears?

Why should you share your good ideas and insights?

Why should you share sensitive information about your own organisation?

We included some presents for you ☺

GÉANT:
Supporting collaboration and development amongst researchers, the dissemination of information & knowledge, and providing access to a portfolio of services and infrastructure resources:

Runs a membership association for Europe’s National Research & Education Networks (NRENs)
GÉANT Association

Coordinates and participates in EC-funded projects
Under Horizon 2020, the Horizon Europe programme, and other EC funding programmes, aimed at securing Europe’s global competitiveness.

Operates a pan-European e-infrastructure
GÉANT network

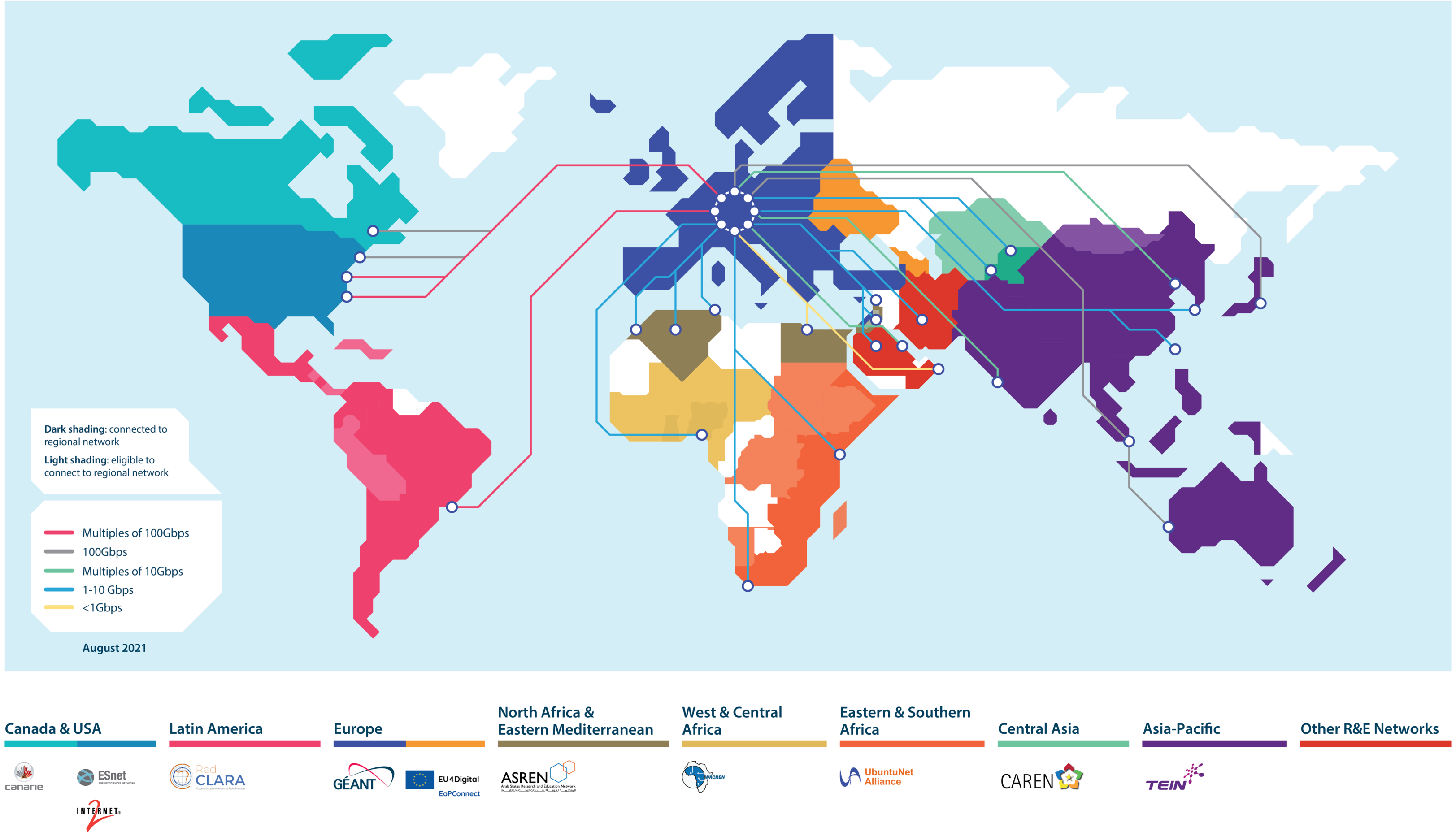
Manages a portfolio of services for research & education
eduX

Organises and runs community events & working groups
TNC, task forces & special interest groups

Network

The GÉANT network interconnects research, education and innovation communities worldwide, with secure, high-capacity networks.

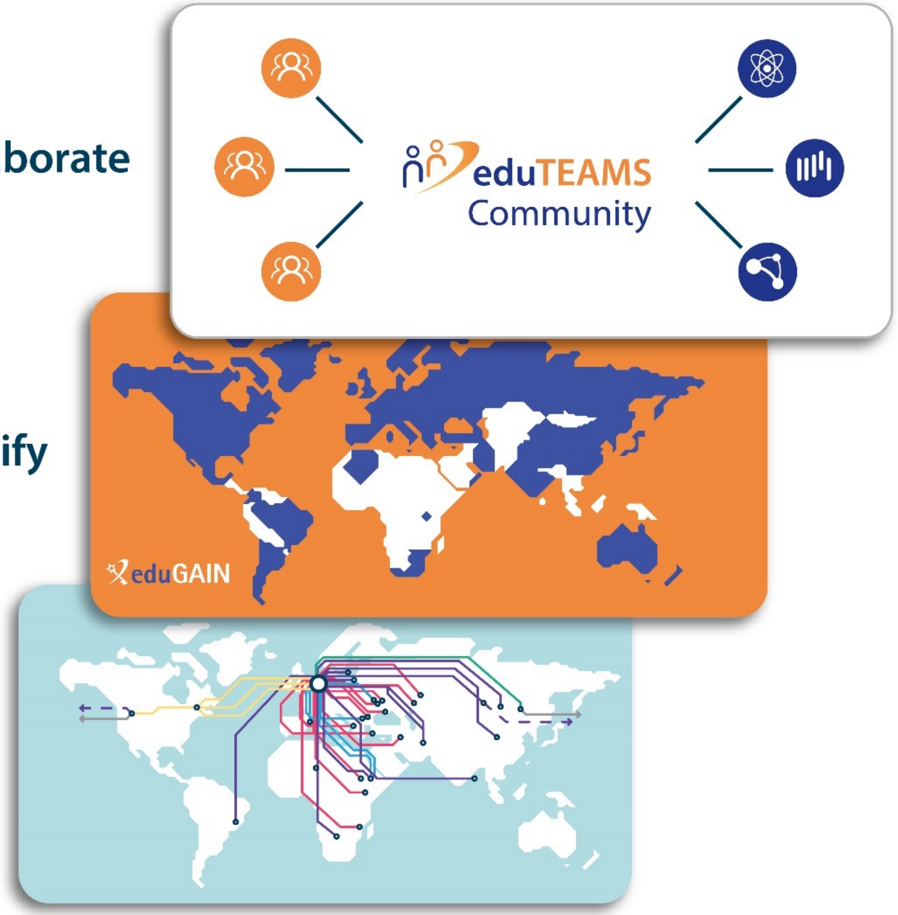
We design, plan, build and operate the large-scale, high-performance GÉANT network that connects European NRENs to each other and the rest of the world for sharing, accessing and processing the high data volumes generated by research and education communities and for testing innovative technologies and concepts.



You may have heard of.....

eduroam

eduVPN

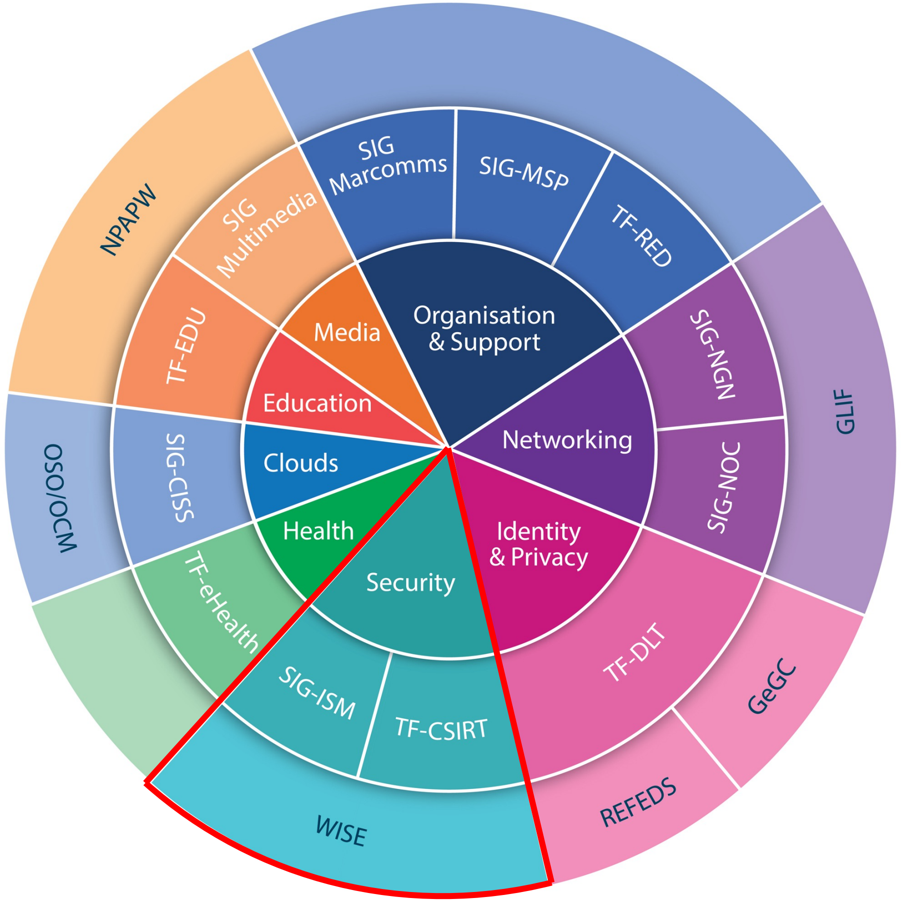


Collaborate

Identify

Connect

Special Interest Groups & Task Forces



> community.geant.org

Trusted Introducer for Incident response teams

- Sharing good practices
- Sharing security intelligence
- Training (TRANSITS)
- Trust

- https://www.trusted-introducer.org

TF-CSIRT
Trusted Introducer

SIG-ISM:
Special Interest Group on Information Security Management

- Community for security officers
- Whitepapers on security management and risk management
- Top 5 security risks and trends for R&E
- Get in contact with your peers
- Share day-to-day challenges and solutions

- https://community.geant.org/sig-ism/

Other communities

- WISE
  - Information Security for Collaborating e-Infrastructures
  - Security Specialists of e-infrastructures
  - Focused on devloping policies, risk analysis, etc.
  - a collaborative activity of information security officers from several large-scale infrastructures, including EGI, PRACE, EUDAT, WLCG, XSEDE, HBP and others.
  - **“A Trust Framework for Security Collaboration among Infrastructures”**
  - https://wise-community.org/sci/
- FIRST Academic Security SIG
  - https://www.first.org/global/sigs/academicsec/
- WLCG SOC working group
  - https://wlcg-soc-wg.web.cern.ch/

The GÉANT Association is driven by Eight Strategic Goals

Network
We are the trusted partner for pan-European and global advanced R&E networking.

Security
We provide a safe and secure information ecosystem for researchers, educators, and students.

Innovation
We continually evolve key infrastructures, innovate, and develop new services in order to fulfil the needs of the R&E community in a sustainable way.

Community
We are acknowledged worldwide as a leader for developing and supporting R&E networking communities, and global REN development.

European Union
We are seen by the EU as an indispensable partner for their vision.

Stakeholders
We forge relationships with other e-infrastructure providers, research infrastructures (RIs), and other stakeholders, to benefit the R&E community.

Governance
We have a governance structure that is agile and benefits from the diversity of our membership.

Funding
We will ensure financial sustainability to benefit our members.

GÉANT2020 Framework Partnership Agreement (FPA)

The GÉANT2020 FPA is a seven-year programme, split into three phases:

~~GN4-1~~	~~1 May 2015 to 30 Apr 2016~~
~~GN4-2~~	~~1 May 2016 to 31 Dec 2018~~
GN4-3	1 Jan 2019 to 31 Dec 2022
GN4-3N	

Action A	Drive the Evolution of the Network
Action B	Support the Knowledge Community
Action C	Provide Security, Trust and Identity
Action D	Deliver GÉANT's Collaborative Ecosystem
Action E	Develop the Human Capital of the GÉANT Partnership
Action F	Ensuring the Long-Term Future of the GÉANT Infrastructure

GN5 - Framework Partnership Agreement (FPA) Horizon Europe

The GN5 - FPA is a seven-year programme:

GN5-1	1 January 2023 to 31 December 2025
GN5-IC1	1 November 2022 to 31 October 2025

Action A Understand and respond to the requirements of R&E communities.

Action B Evolve the Communication Commons towards data-driven research and education.

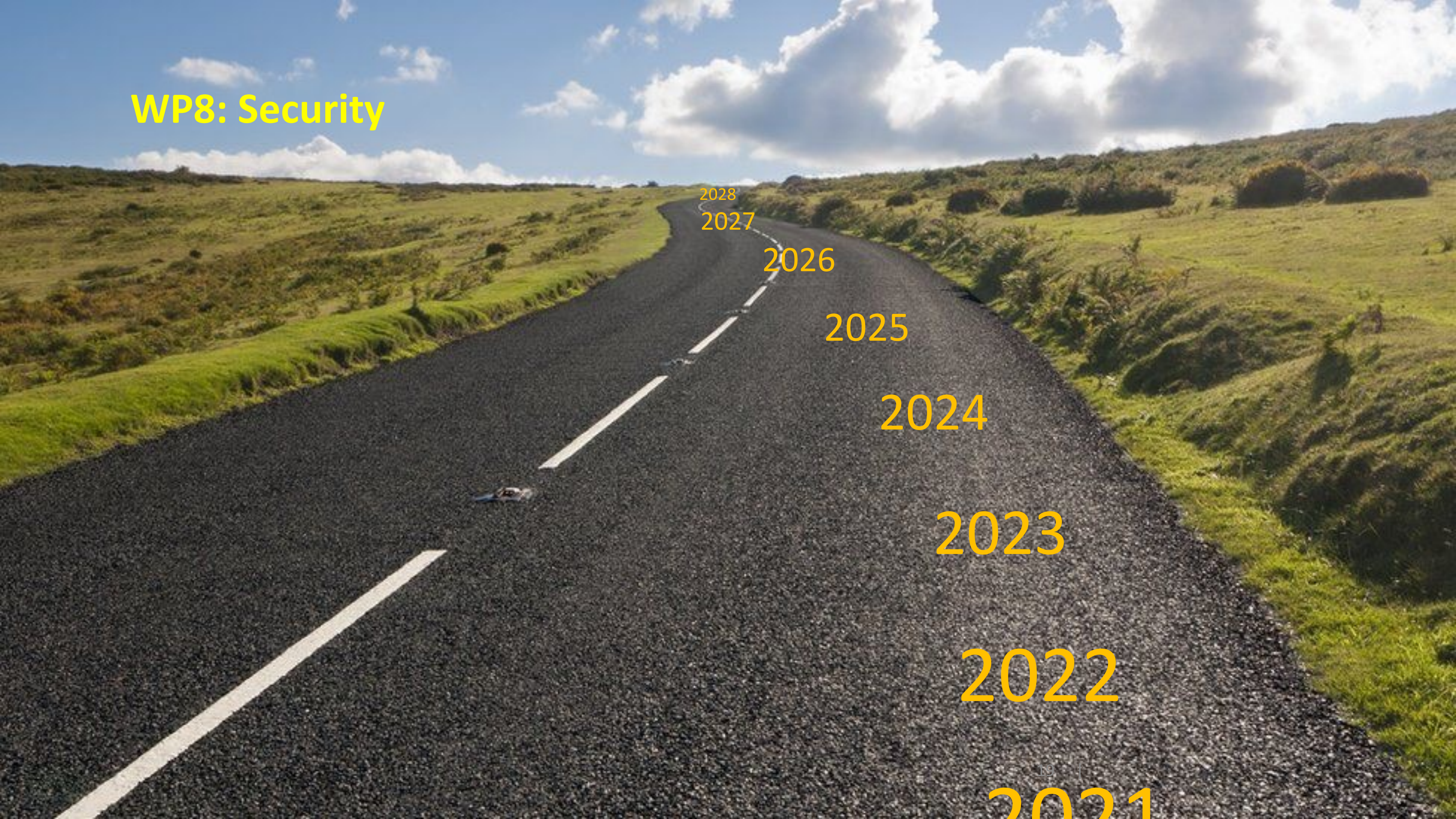
Action C Deliver state-of-the-art network connectivity and operational excellence.

Action D Deliver interoperable and distributed trust and identity infrastructure, security and above-the-net services, and procurement.

Action E Ensure innovation of key infrastructures and service development as an indispensable part of the GÉANT partnership.

Action F Strengthen the collaborative ecosystem of GÉANT and the NRENs, and develop the human capital of the GÉANT partnership.

WP8: Security



2028

2027

2026

2025

2024

2023

2022

2021

Standards and
Best Practices

Security
Operations
Support

Services
and
Tools

Incident Response and
Crisis Management

Development of
Human Capital,
Training and Awareness

Securing
High-Speed Networks

2026

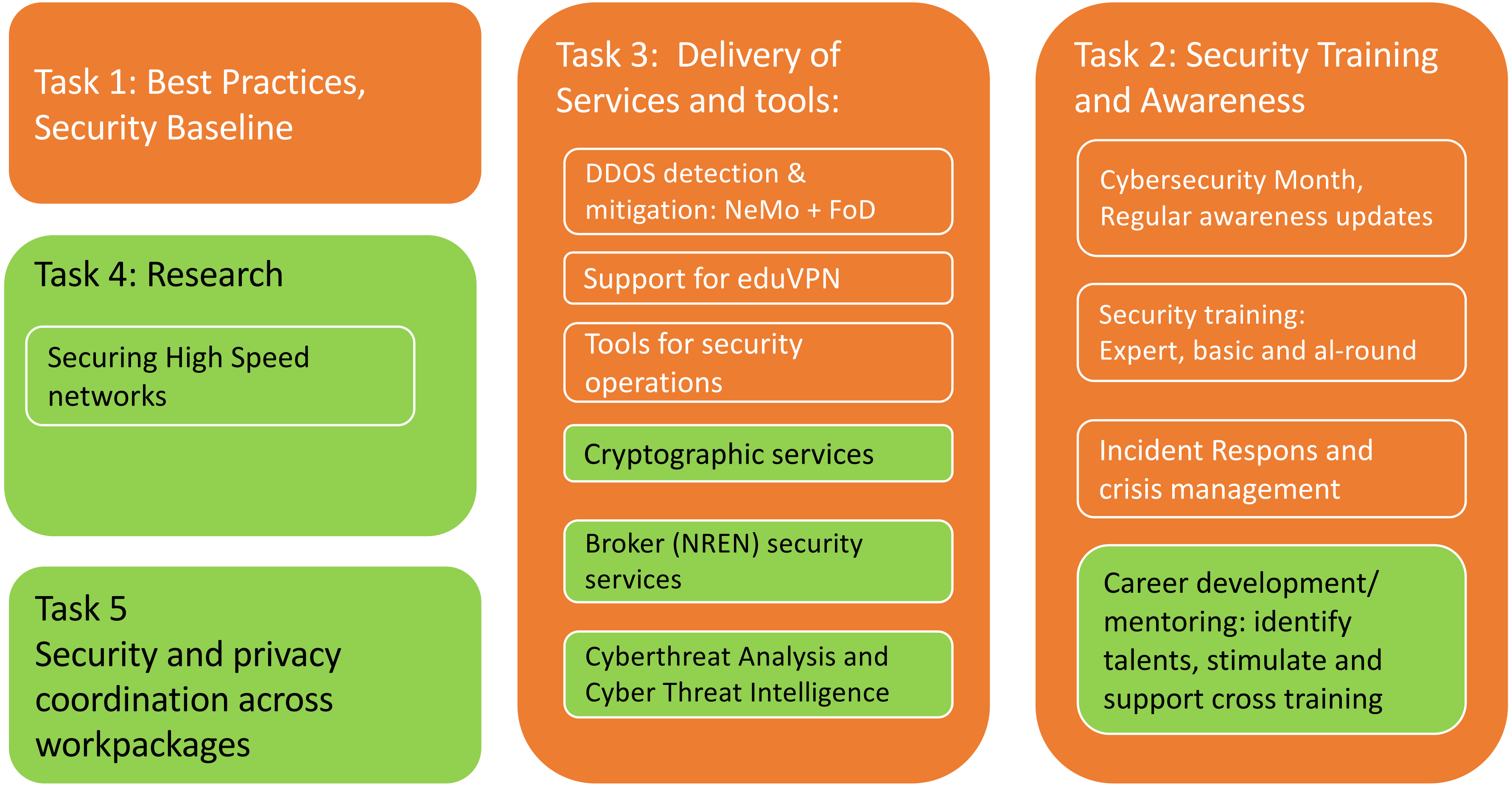
24

2023

2022

2021

WP8: Security: Proposal GN5-1 (2023 – 2025)
Overview of activity – ongoing and new



Task 1: Best Practices, Security Baseline

Task 4: Research

- Securing High Speed networks

Task 5
Security and privacy coordination across workpackages

Task 3: Delivery of Services and tools:

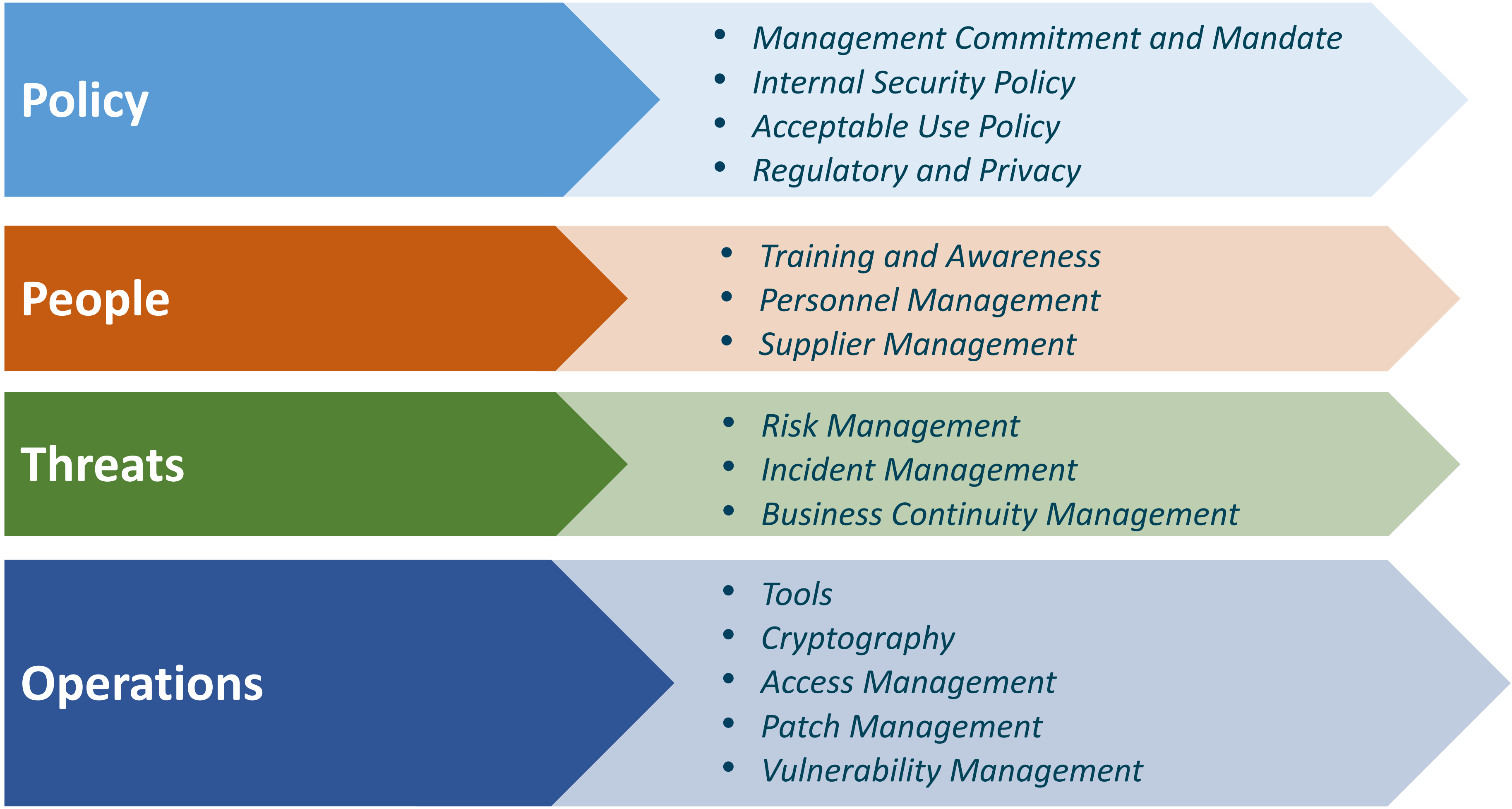
- DDOS detection & mitigation: NeMo + FoD
- Support for eduVPN
- Tools for security operations
- Cryptographic services
- Broker (NREN) security services
- Cyberthreat Analysis and Cyber Threat Intelligence

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

Jointly led by Henry Hughes (JISC) and Alf Moens (GÉANT)

Security Baselining



Policy

- *Management Commitment and Mandate*
- *Internal Security Policy*
- *Acceptable Use Policy*
- *Regulatory and Privacy*

People

- *Training and Awareness*
- *Personnel Management*
- *Supplier Management*

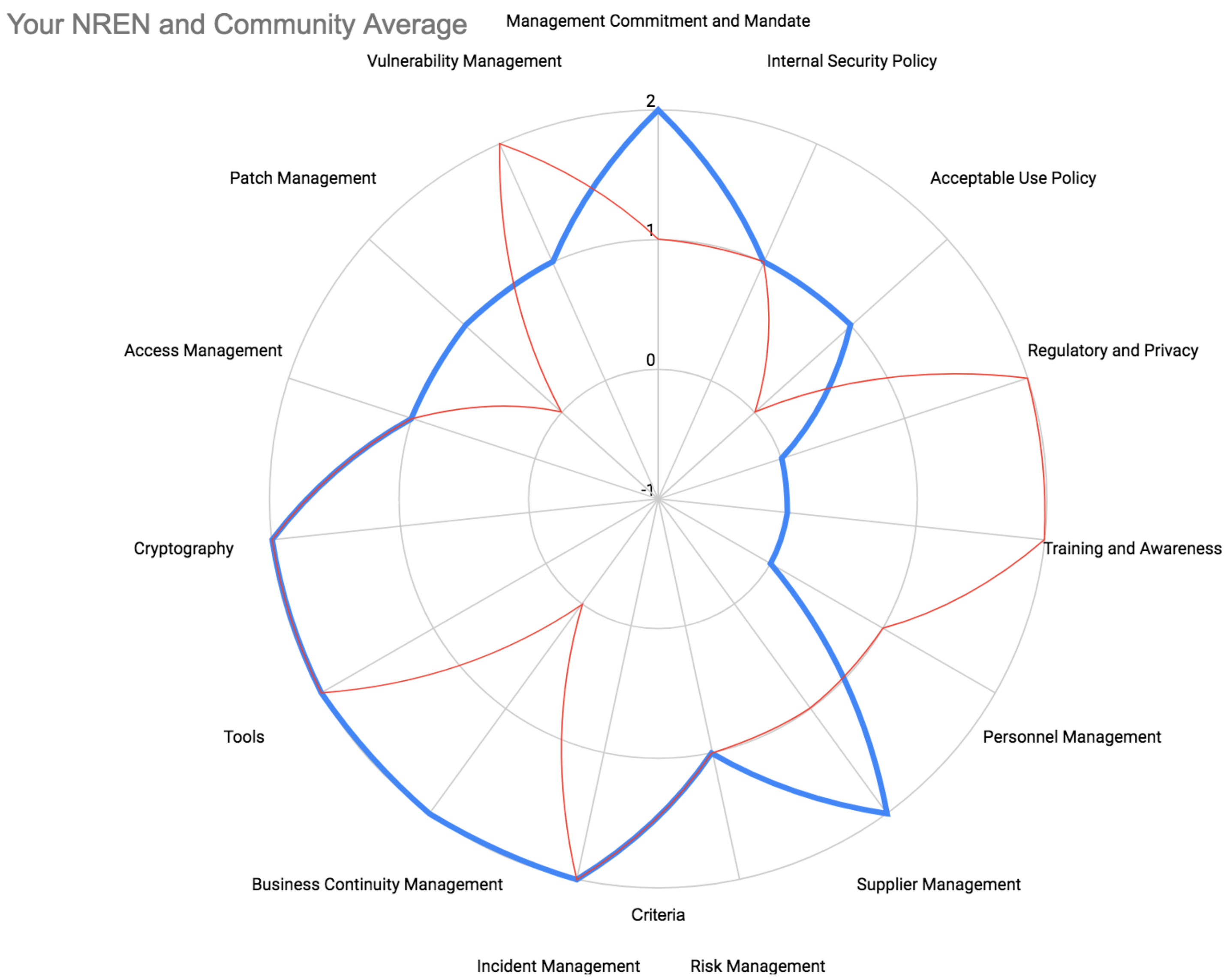
Threats

- *Risk Management*
- *Incident Management*
- *Business Continuity Management*

Operations

- *Tools*
- *Cryptography*
- *Access Management*
- *Patch Management*
- *Vulnerability Management*

Security Baselining



ACHIEVEMENTS (TASK 3)

Security Products and Services

SOC tooling

Coherent set of tools, packaged in Docker containers

Firewall on Demand

Migration to Python 3 and Django 2

Virtual network testbed API for DDOS

eduVPN

Uptake:
91 servers in 23 countries, 15 secure Internet servers
39K new Macos users observed
National usage is not registered centrally

Vulnerability Management

Agreement with Holm Security

Evaluation of Vulnerability Scanners

Distributed Denial of Service Mitigation: NeMo

Testbeds in GÉANT network

Acquisition of equipment

virtualisation with Docker

Expanded team

https://geant.org/projects/gn4-3-deliverables/

D8.6 Vulnerability Assessment as a Service Pilot Project

Published date | **16 August 2022**

This deliverable provides an introduction to common vulnerability assessment and management methodologies and tools and reports on the results of a pilot project conducted by WP8 T3.2 to evaluate different vulnerability scanning tools in production or test environments in various NRENs and institutions.

Download PDF

D8.10 Firewall on Demand

Published date | **9 August 2022**

This document provides a summary of the enhancements and improvements to Firewall on Demand (FoD) developed and tested during GN4-3. These comprise mainly development of the core service as well as the introduction of Docker containers for installation and runtime-management support and the establishment of testing on various layers.

Download PDF

D8.9 Best Practices for Security Operations in Research and Education

Published date | **30 June 2022**

This report introduces the concepts of security operations, including its goals, benefits and best practices, and of operational intelligence, as well as Security Operations Centres (SOCs) as a means to realise their practical implementation. It presents three research and education SOC case studies, including utilisation of the SOCTools package developed by GN4-3 WP8 Task 3.1 Security Operations Centre.

Download PDF

Status August 2020:
9 countries added in apps: Norway, Uganda, Pakistan, Finland, France, Sri Lanka, Morocco, Estonia, Albania

28 institutes added in apps: Unit, EUR, PolSl, STC, Trimbos, HEAnet, Tuni, Differ, Perdana, Pionier, GÉANT, Cnous, CSC, Uminho, HS-OS, Hiof, UniOsnabrück, VAMK, DIAK, IPB, University of Nimes, ENSMA, RENU, VU, HSTrier, KENET, Saxion, TUDelft

Estimated between 35,000 and 60,000 unique App downloads
Example: Radboud University (NL) reported over June 2020: 3300 unique users, max 900 simultaneous users

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

eduVPN

Secure

- Used VPN technology audited by international community
- Strong Cryptography
- eduVPN server/apps audited

Privacy enhancing

- 'privacy by design' philosophy fully applied
- GDPR compliant by policy and technical design
- eduVPN helps avoiding data leakage on insecure WiFi

Trust

- Software approved by GÉANT
- Governance software @ Commons Conservancy foundation
- eduVPN service policy under governance of GÉANT
- eduVPN servers operated by NRENs or institutes
- All software: client apps to server (management) fully open-source

eduVPN

91

Servers in

23

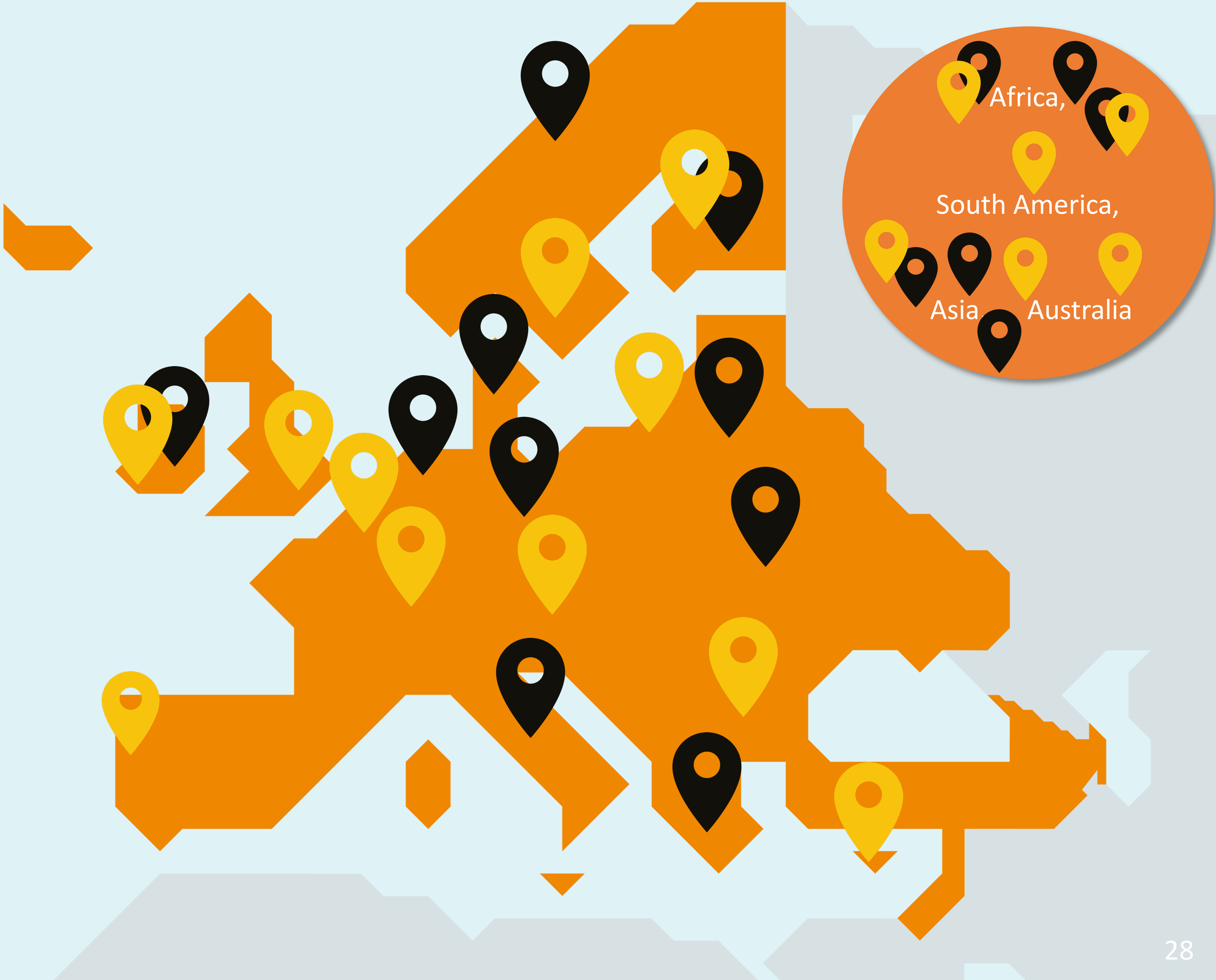
countries

16

Secure internet servers

🟨 Institute access

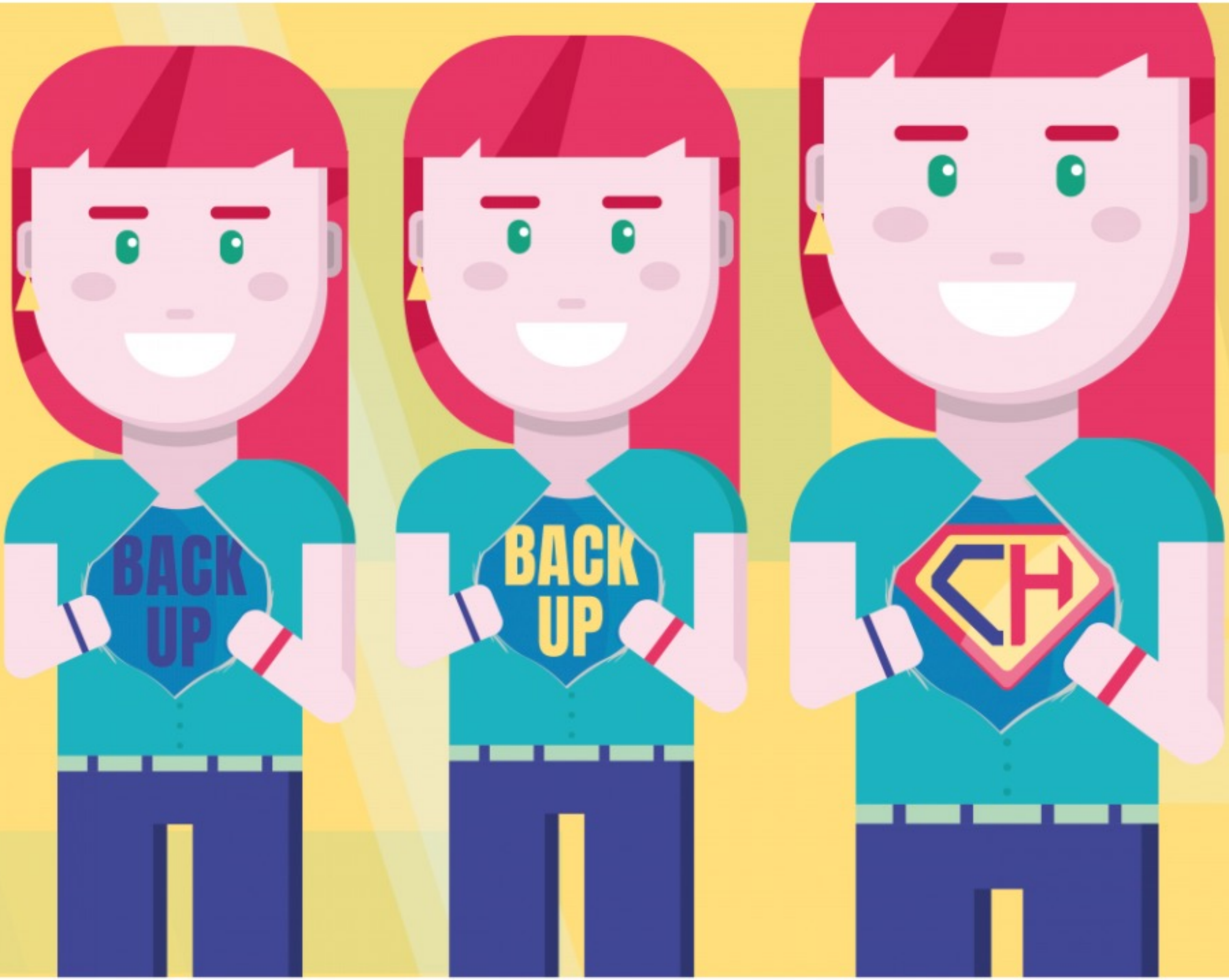
⬛ Secure internet



The First present: Security Awareness

Security Awareness Month 2020 (Anthology)

- #BecomeACyberHero
- Weekly themes:
  - Week 1: Social engineering
  - Week 2: Phishing
  - Week 3: Ransomware
  - Week 4: Password security
- Case studies:
  - Ransomware Maastricht University
  - Awareness at the Paul Scherrer Institute in Switzerland
- Interviews
- Articles
  - Passwords, phishing, Ransomware
- Tip-of-the-day
- Combination of new material and existing local material



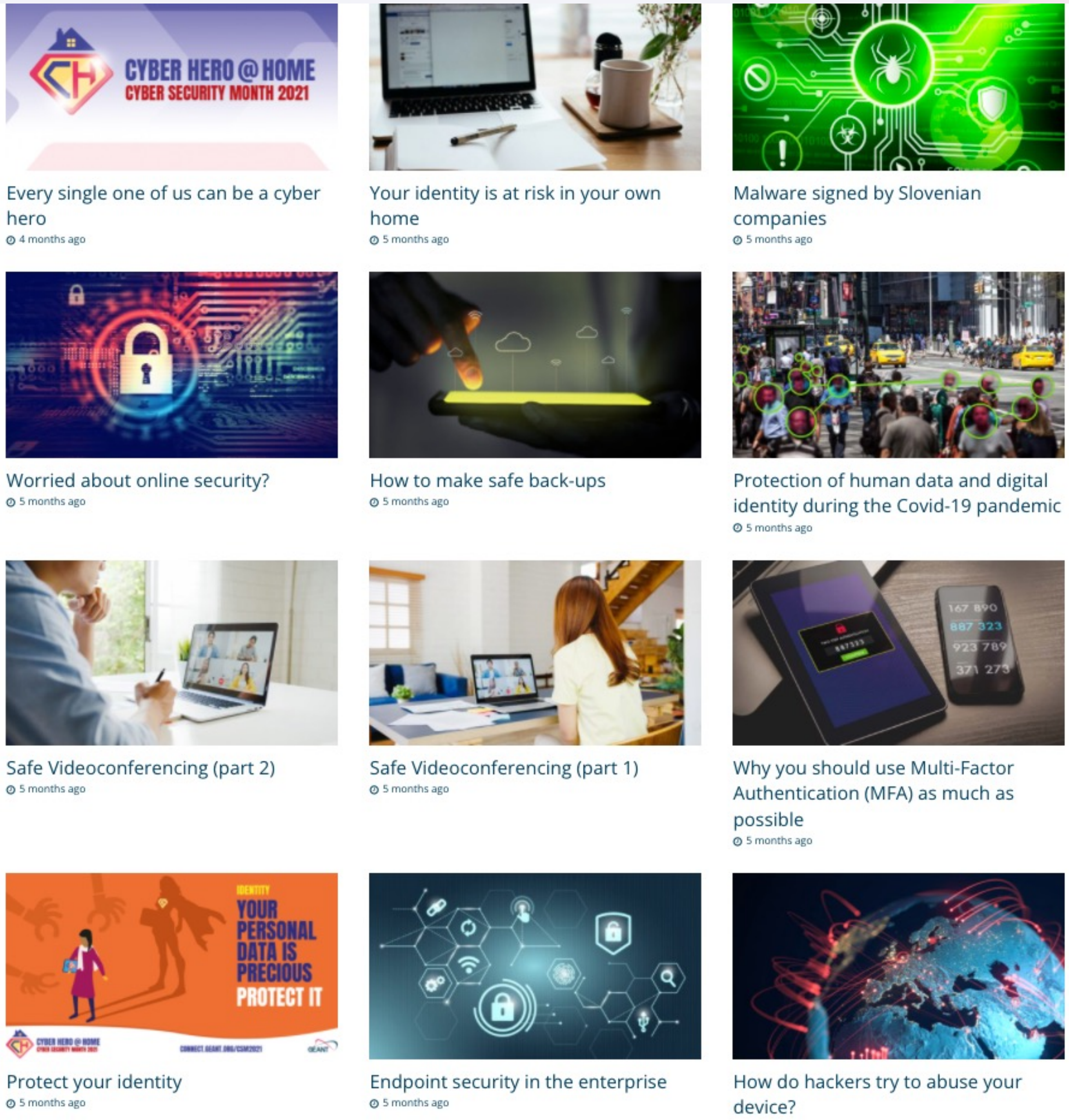
RANSOMWARE

MINIMISE IMPACT

BACK-UP YOUR DATA AND STORE IT SECURELY. ALWAYS.

Resources still available @

https://connect.geant.org/csm2021


CYBER HERO @ HOME
CYBER SECURITY MONTH 2021
IDENTITY
YOUR PERSONAL DATA IS PRECIOUS
PROTECT IT
CONNECT.GEANT.ORG/CSM2021

Every single one of us can be a cyber hero
4 months ago

Your identity is at risk in your own home
5 months ago

Malware signed by Slovenian companies
5 months ago

Worried about online security?
5 months ago

How to make safe back-ups
5 months ago

Protection of human data and digital identity during the Covid-19 pandemic
5 months ago

Safe Videoconferencing (part 2)
5 months ago

Safe Videoconferencing (part 1)
5 months ago

Why you should use Multi-Factor Authentication (MFA) as much as possible
5 months ago

Protect your identity
5 months ago

Endpoint security in the enterprise
5 months ago

How do hackers try to abuse your device?

Participate in 2022?

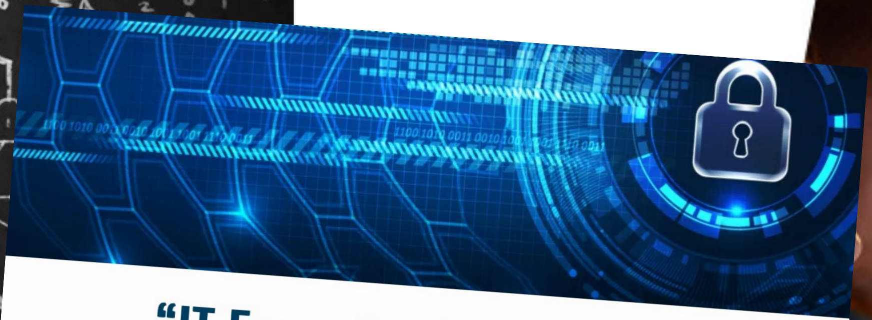
https://connect.geant.org/csm2022

The second present: Training

Client privacy and security

Distributed Denial of Service (DDoS) Protection (Operational

"Vulnerability Management"



"IT Forensics for System Administrators" – new for 2021

Operational network security – new for 2020 – virtual learning with experts

Domain Name System (DNS)

Virtual learning with experts:

Operating System Privacy and Security
Operating System Telemetry
Logging and Audit
File Integrity Monitoring (FIM) for detecting security incidents
Network 1st Hop Security
Authentication Methods

Client Privacy and Security
Browser Security and Privacy
E-Mail Security and Privacy
Instant Messaging Security and Privacy
Videoconferencing Security and Privacy
Office Security and Privacy

Domain Name System (DNS) protection
Introduction to DNS and its Security Challenges
DNS for Network Defence
DNSSEC
DNS Privacy Protocols

Distributed Denial of Service (DDoS) protection
Introduction to DDoS Attacks
Details of Selected DDoS Attacks
DDoS Detection
DDoS Mitigation

Vulnerability Management
Vulnerability Management Process and Standards
Vulnerability Information
Patch Management
Looking into the Network
Network Vulnerability Scanning
Penetration Tests
Code Audits
Vulnerability Disclosure
Breach and Attack Simulation

5 Modules
27 x 1 hour webinars

Recordings on GEANT TV (YouTube)

Slide decks available

From and with the experts of DFN-CERT

https://security.geant.org/training/

The third present: Crisis Preparation

Let’s talk about Crisis Management

- Since Covid-19 everyone knows what a crisis is
    - Working form home, massive online education. And what about research?
    - How do you keep track?
    - Where you prepared?
- Crisis management is a multi-discipline acivity
    - Not just ICT or Security
    - Strong role for communication
- These were the most important lessons from nation wide cybercrisis exercises in R&E the Netherlands

GUILDER.

GUILDERLAND ER SANN WIDUNDERLAND!

CLAW

The second Crisis Management Workshop for the GÉANT Community

How well is your organisation prepared for a network or cyber crisis?

Do you have crisis management procedures in place?

Do you know who should be involved when crisis hits?

And do you know how to reach out to – and work with – other organisations, in the eventuality of a pan-European crisis?

CRISIS CLAW

CRISIS MANAGEMENT WORKSHOP FOR THE GÉANT COMMUNITY

29-30 NOVEMBER 2022

PSNC, POZNAN, POLAND

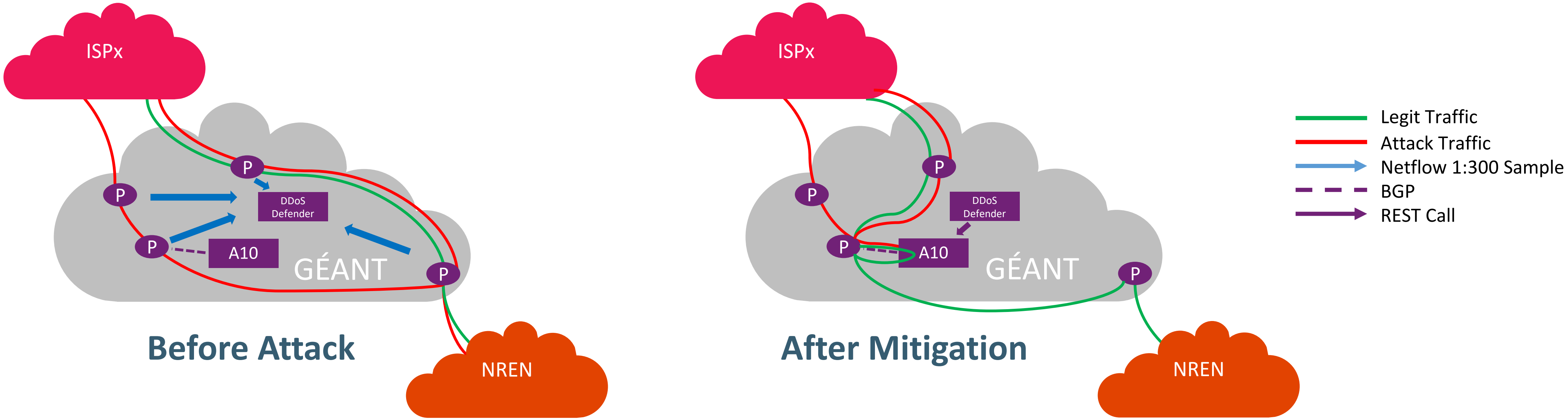
GÉANT

https://connect.geant.org/2022/07/27/save-the-date-claw-2022-29-and-30-november-psnc-poznan

https://events.geant.org/event/1193/

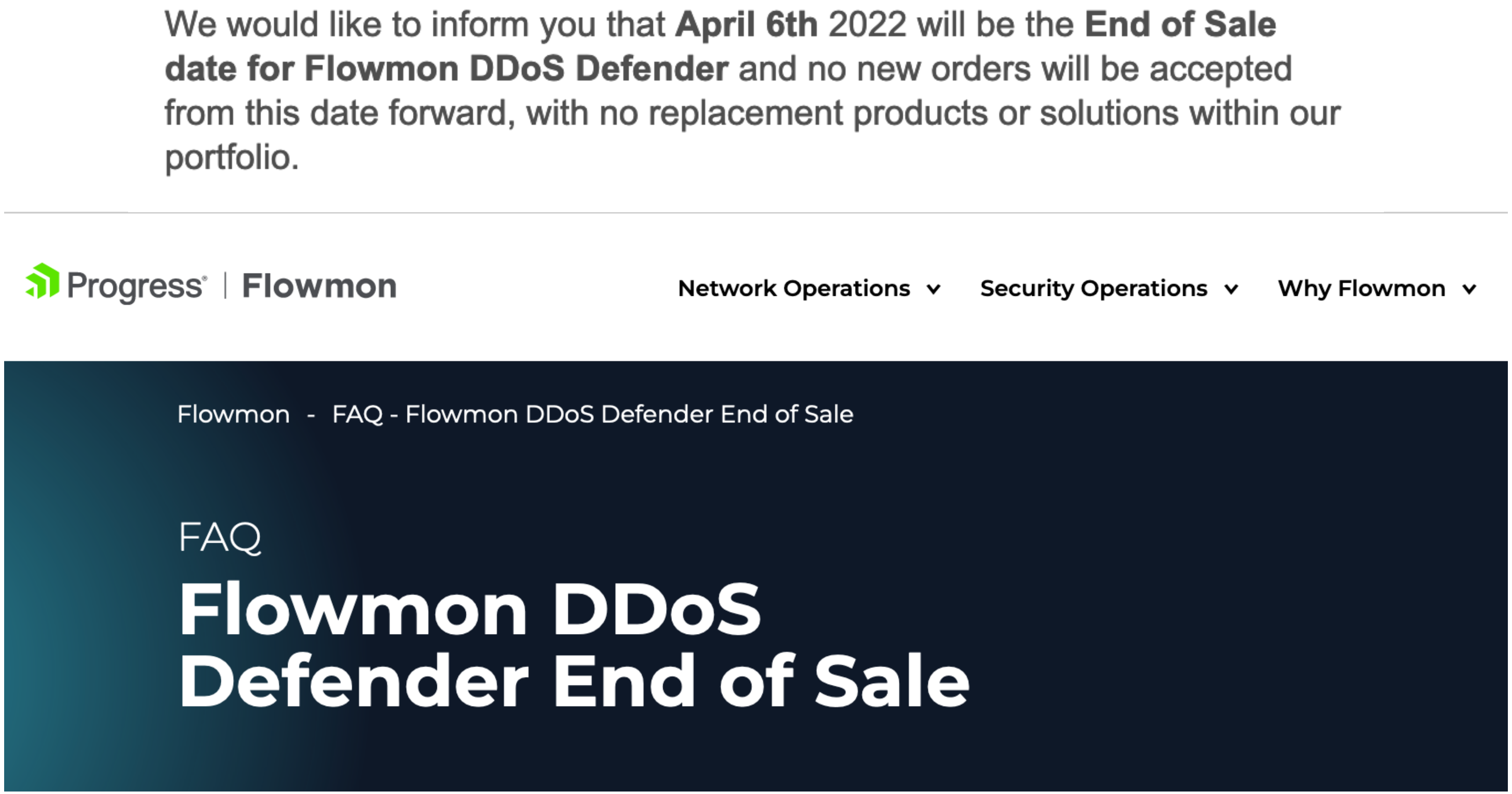
GÉANT DDoS Cleansing and Alerting

- Distributed Denial of Service (DDoS) is a large and growing problem
- GÉANT DDoS Cleansing provides a dynamic, automated detection and mitigation service



- DDoS Cleansing uses Flowmon monitoring to divert DDoS traffic to A10 TPS service.
    - Can support up to 38Gbps throughput of attack data
    - No NREN staff resource required
    - No-cost option to add service to peering users
- Firewall on Demand remains to support inter-NREN DDoS

FlowMon



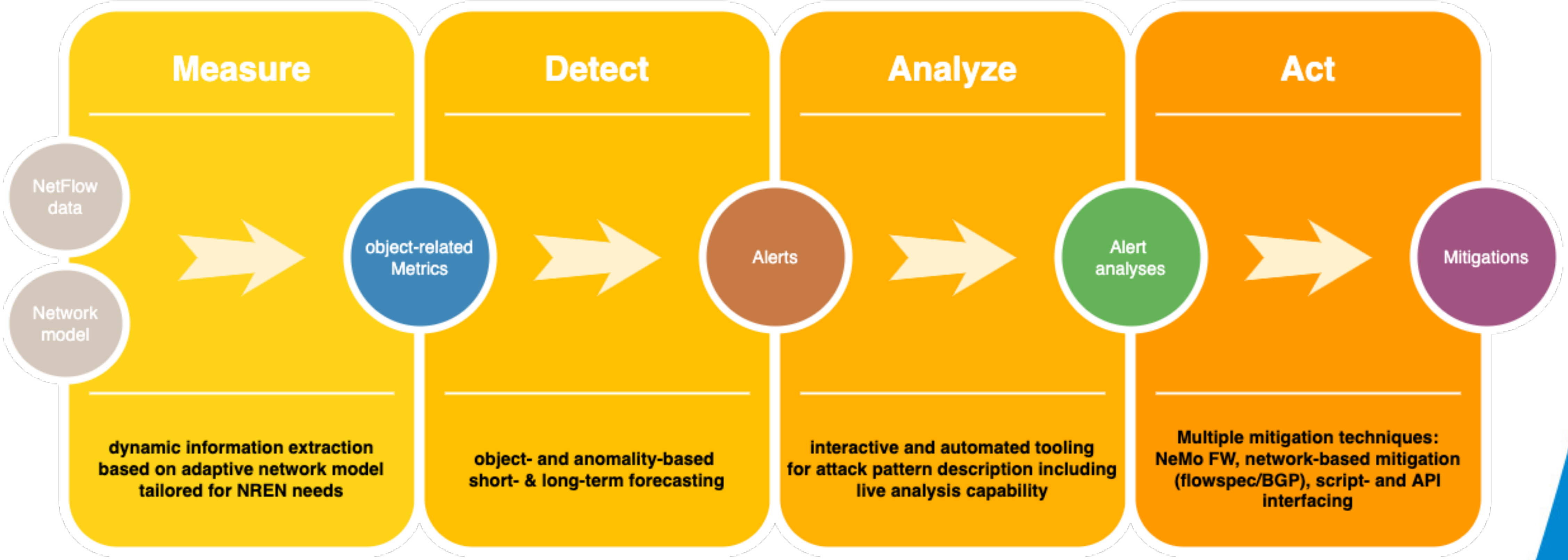
We would like to inform you that **April 6th** 2022 will be the **End of Sale date for Flowmon DDoS Defender** and no new orders will be accepted from this date forward, with no replacement products or solutions within our portfolio.

FAQ

Flowmon DDoS Defender End of Sale

🤔

Finding NeMo ☺



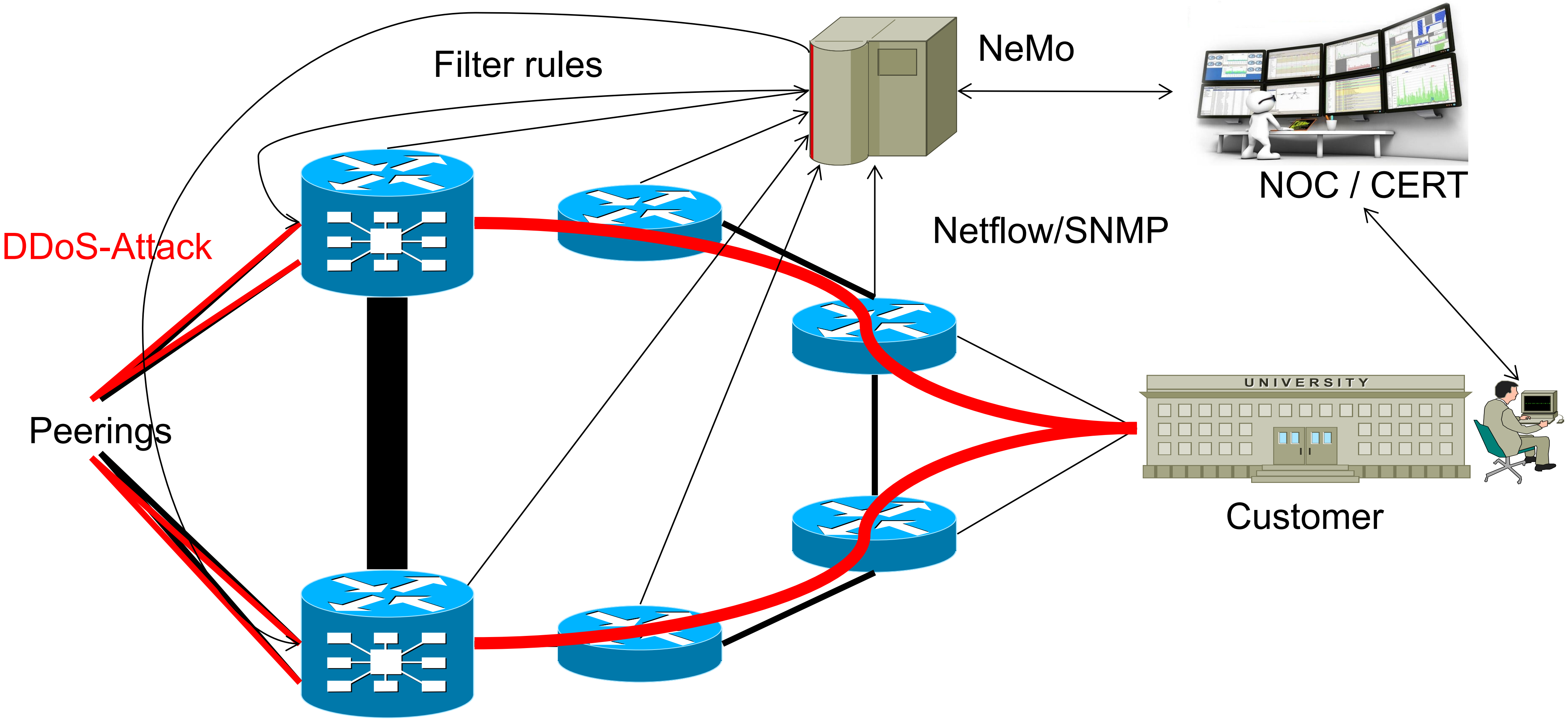
dynamic information extraction based on adaptive network model tailored for NREN needs

object- and anomality-based short- & long-term forecasting

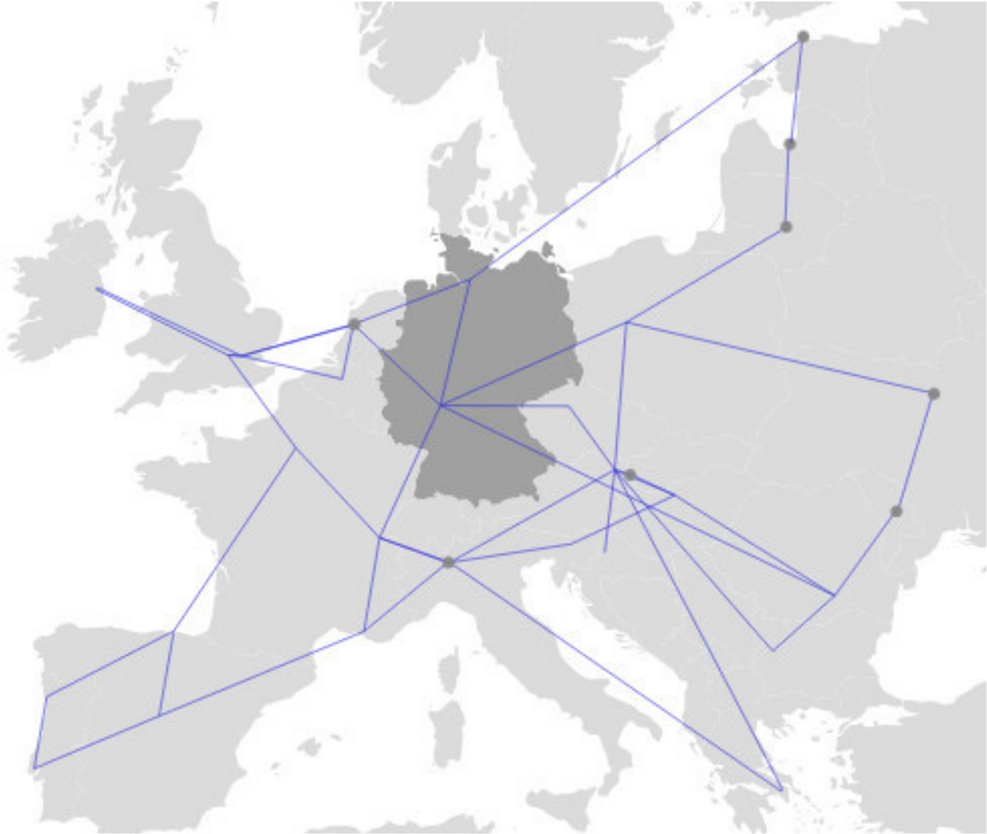
interactive and automated tooling for attack pattern description including live analysis capability

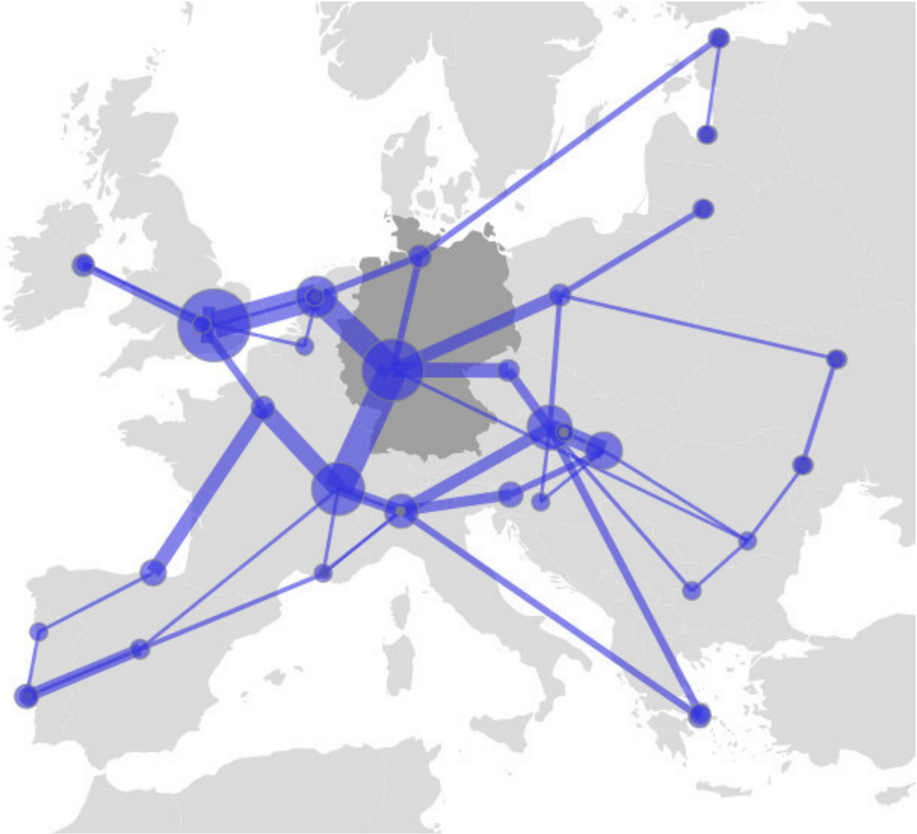
Multiple mitigation techniques: NeMo FW, network-based mitigation (flowspec/BGP), script- and API interfacing

NeMo: Topology

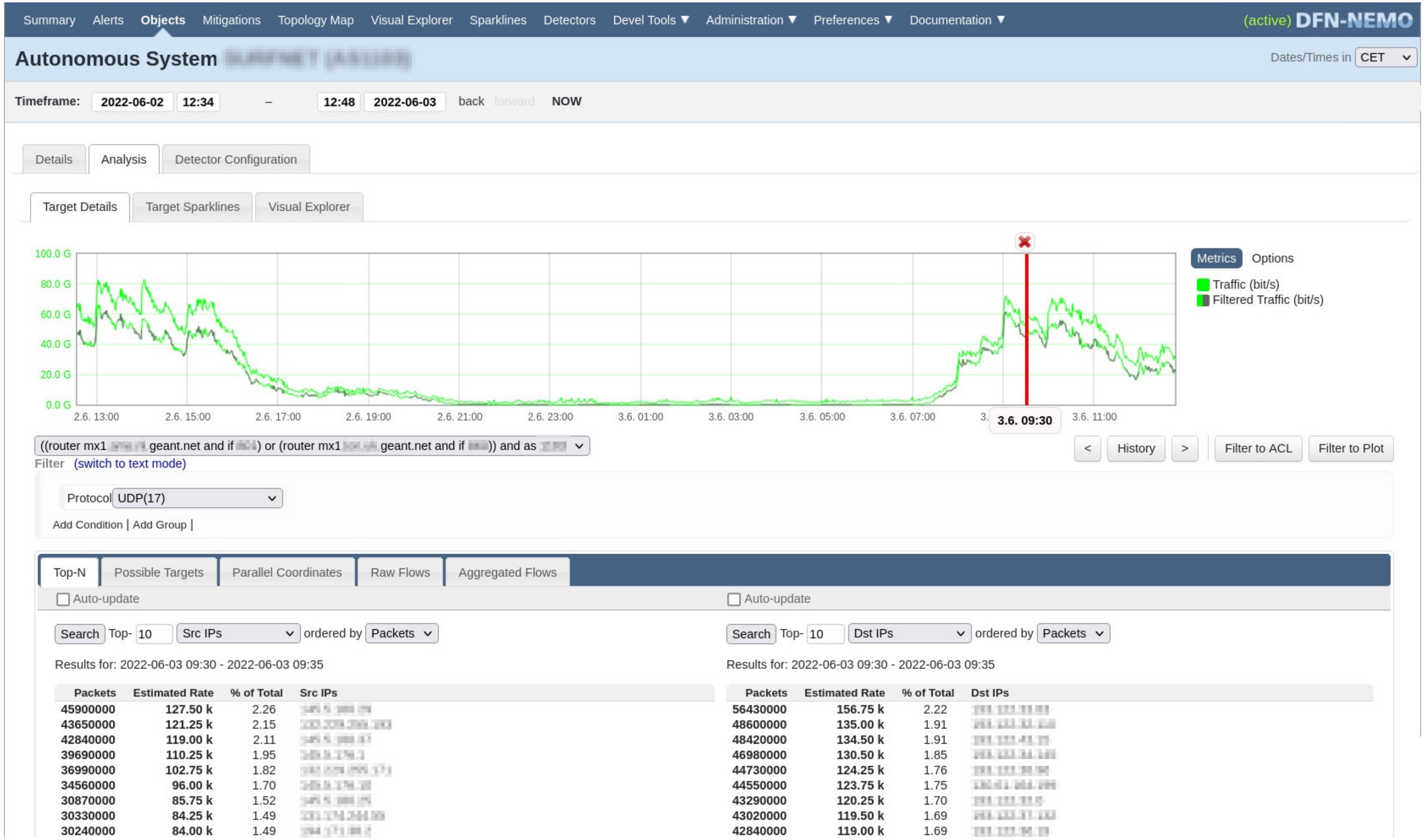


NeMo: GÉANT Network





NeMo: Object Analysis



Autonomous System [redacted]

Dates/Times in CET

Timeframe: 2022-06-02 12:34 – 12:48 2022-06-03

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)

Search Top- 10 Src IPs ordered by Packets

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

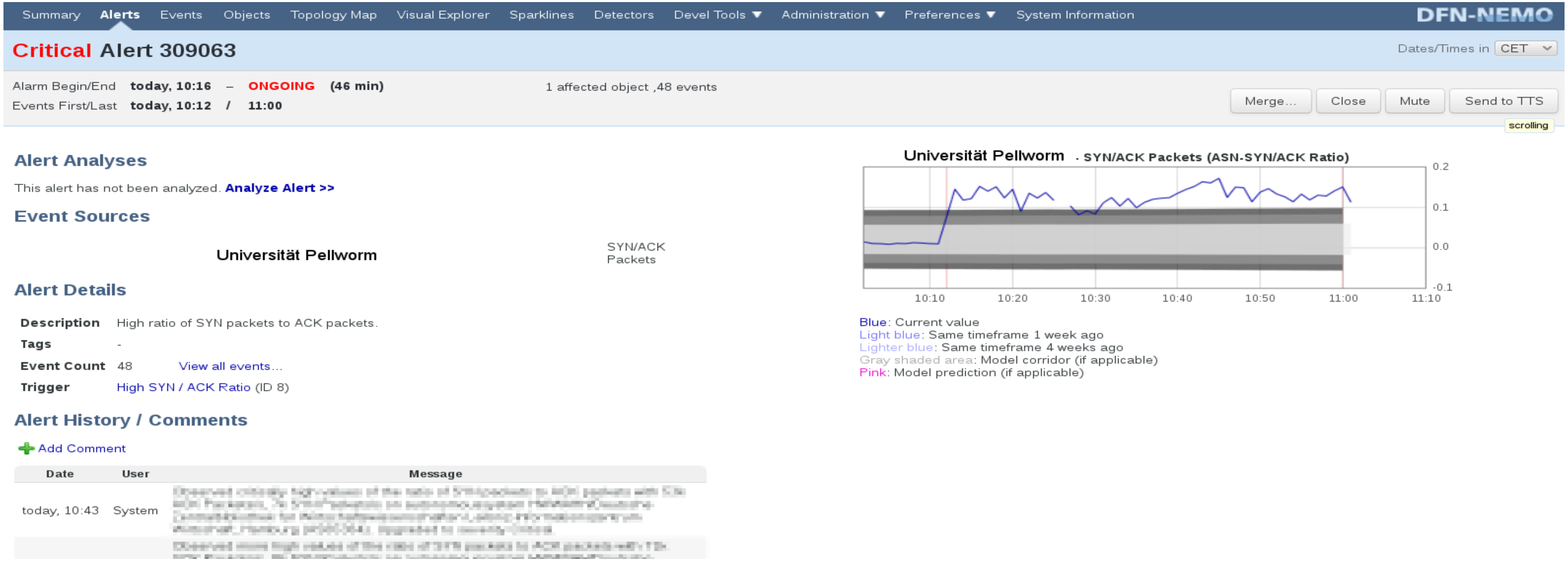
Packets	Estimated Rate	% of Total	Src IPs
45900000	127.50 k	2.26	[redacted]
43650000	121.25 k	2.15	[redacted]
42840000	119.00 k	2.11	[redacted]
39690000	110.25 k	1.95	[redacted]
36990000	102.75 k	1.82	[redacted]
34560000	96.00 k	1.70	[redacted]
30870000	85.75 k	1.52	[redacted]
30330000	84.25 k	1.49	[redacted]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

Search 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]

NeMo: Alert Details



Critical Alert 309063

Alarm Begin/End **today, 10:16 – ONGOING (46 min)**
Events First/Last **today, 10:12 / 11:00**

1 affected object ,48 events

Alert Analyses

This alert has not been analyzed. **Analyze Alert >>**

Event Sources

Universität Pellworm   SYN/ACK Packets

Alert Details

Description	High ratio of SYN packets to ACK packets.
Tags	-
Event Count	48 View all events…
Trigger	High SYN / ACK Ratio (ID 8)

Alert History / Comments

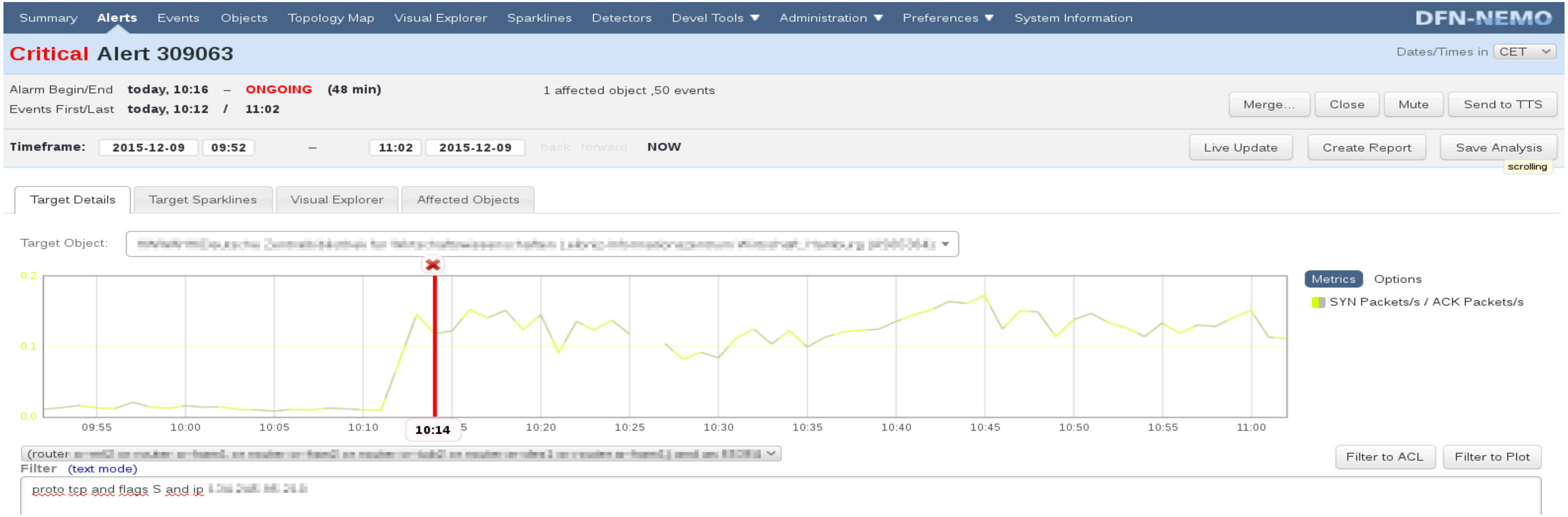
➕ Add Comment

Date	User	Message
today, 10:43	System	[redacted]
		[redacted]

Universität Pellworm . SYN/ACK Packets (ASN-SYN/ACK Ratio)

Blue: Current value
Light blue: Same timeframe 1 week ago
Lighter blue: Same timeframe 4 weeks ago
Gray shaded area: Model corridor (if applicable)
Pink: Model prediction (if applicable)

NeMo: Alert Analysis



Critical Alert 309063

Dates/Times in CET

Alarm Begin/End **today, 10:16** – **ONGOING** **(48 min)**

Events First/Last **today, 10:12** / **11:02**

1 affected object ,50 events

Timeframe: 2015-12-09 09:52 – 11:02 2015-12-09

Target Object: [redacted]

🟩 SYN Packets/s / ACK Packets/s

(router [redacted]

Filter (text mode)

proto tcp and flags S and ip [redacted]

NeMo: Mitigation

- Analyse the attack traffic
  - Basis for countermeasure development
- Routing-changes using Flowspec
  - Acting directly on the routers (similar to FoD)
- Possibility to offramp to a VM
  - Firewall-like filters
- Within GÉANT: + A10 integration*

NeMo: contact / for more info.

- GÉANT NeMo deployment:
  - help@geant.org

- Own deployment / other Qs:
  - gn4-3-wp8-ddos@lists.geant.org

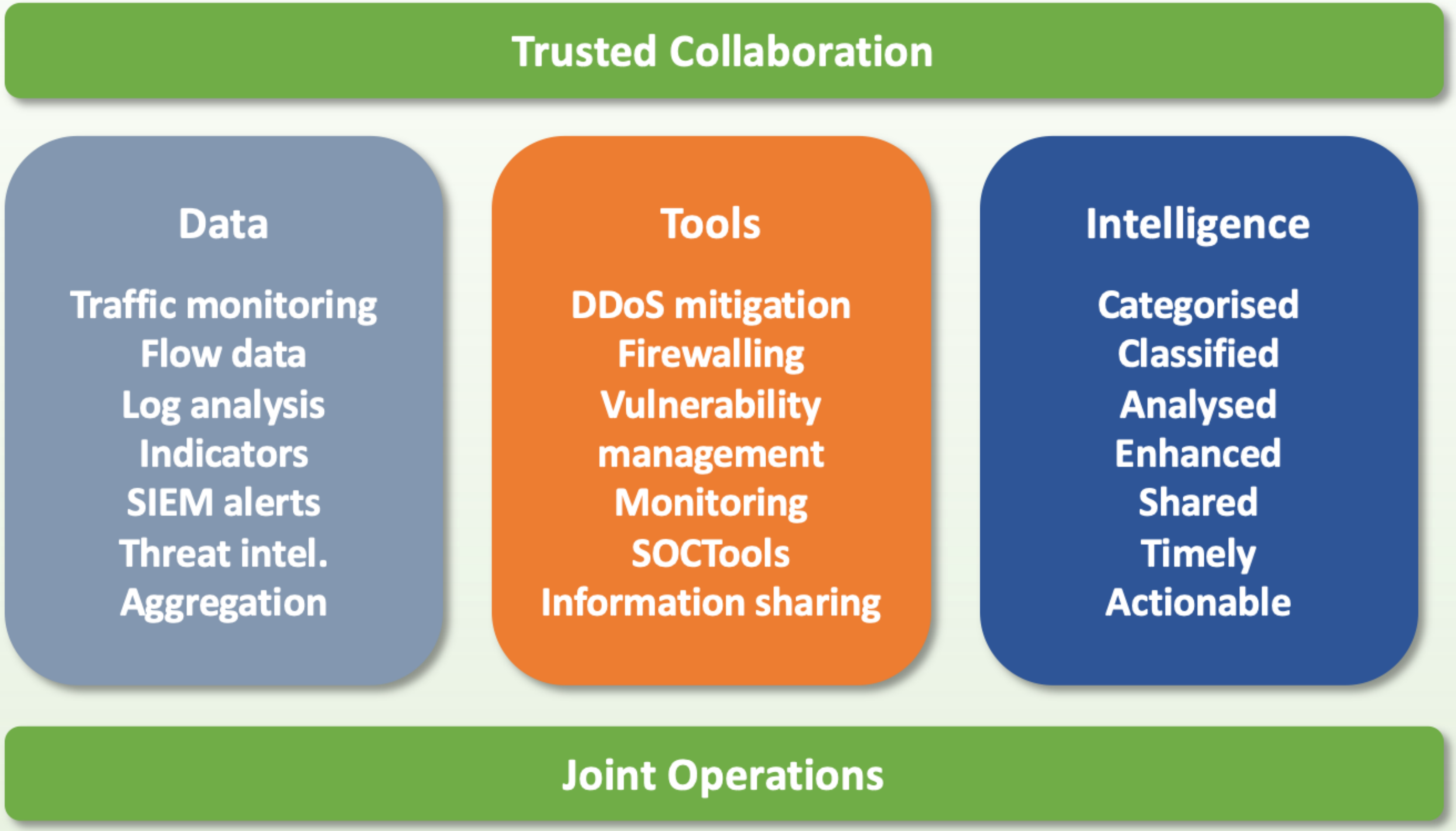
- https://security.geant.org/nemo-ddos-software/

Working together to get things done – why?

- Efficient use of limited expertise and budgets
- Not only Techies, also Management and Marketing/Communications
- Because working together with peers, sharing and caring, helps you to get more things done in better ways.
- You give and you take. The balance is good and....
- It is more fun.

Images source: Unsplash

SOLUTIONS



Trusted Collaboration

Data

Traffic monitoring
Flow data
Log analysis
Indicators
SIEM alerts
Threat intel.
Aggregation

Tools

DDoS mitigation
Firewalling
Vulnerability management
Monitoring
SOCTools
Information sharing

Intelligence

Categorised
Classified
Analysed
Enhanced
Shared
Timely
Actionable

Joint Operations

Summary

- 3 presents:
  - Security Awareness (cybersecurity month)
  - Security Training
  - Crisis Exercise-in-a-box
- What communities can do for you
- Share information, share intelligence, share experience, work together
- Work on trust
  - “A Trust Framework for Security Collaboration among Infrastructures”
  - V2.0 https://wise-community.org/sci/
- Recommended security products and services
  - NeMo DDoS detection and mitigation
  - Firewall on Demand (FoD)
  - eduVPN (https://www.eduvpn.org/)

Thank You !!

roderick.mooi@geant.org

www.geant.org

security.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)

Resources

- https://www.trusted-introducer.org
- https://community.geant.org/sig-ism/
- https://wise-community.org
- https://www.first.org/global/sigs/academicsec
- https://wlcg-soc-wg.web.cern.ch/

- https://geant.org/projects/gn4-3-deliverables/

- https://connect.geant.org/csm2022
- https://security.geant.org/training
- https://connect.geant.org/2022/07/27/save-the-date-claw-2022-29-and-30-november-psnc-poznan
- CLAW22: https://events.geant.org/event/1193

- https://security.geant.org/nemo-ddos-software/
- https://www.eduvpn.org/join/