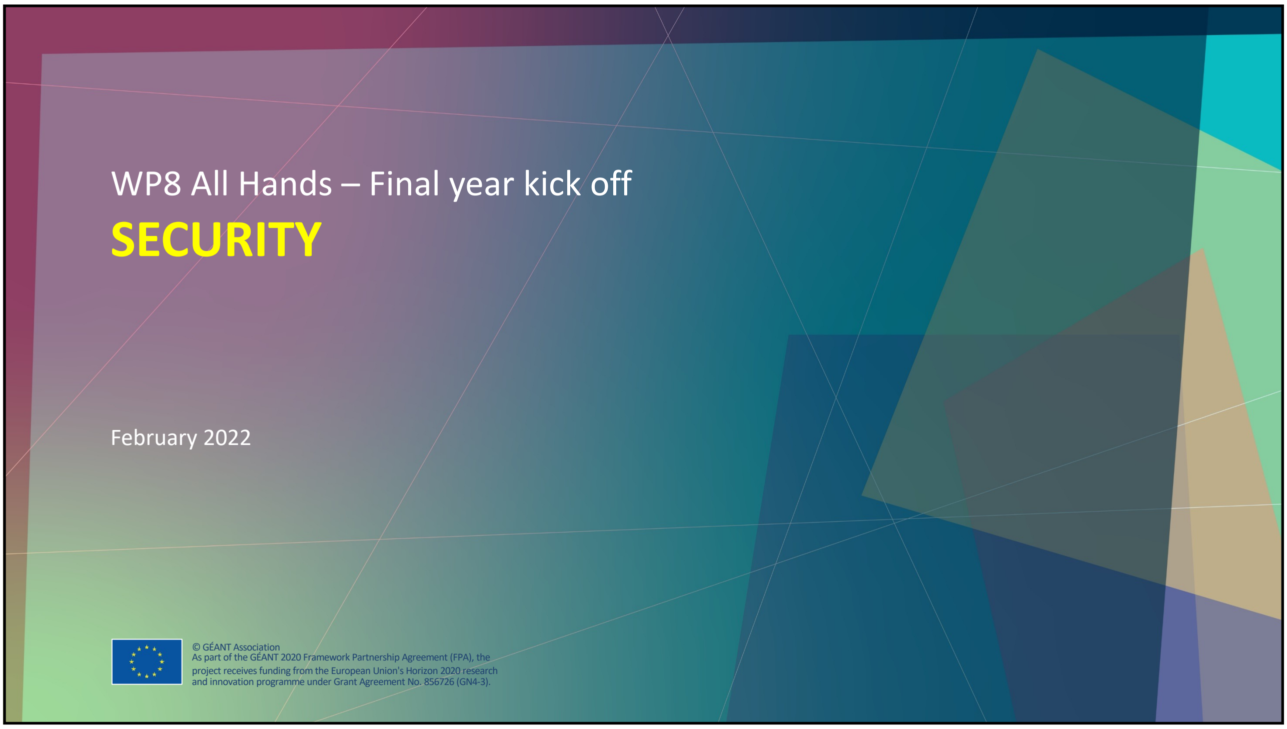


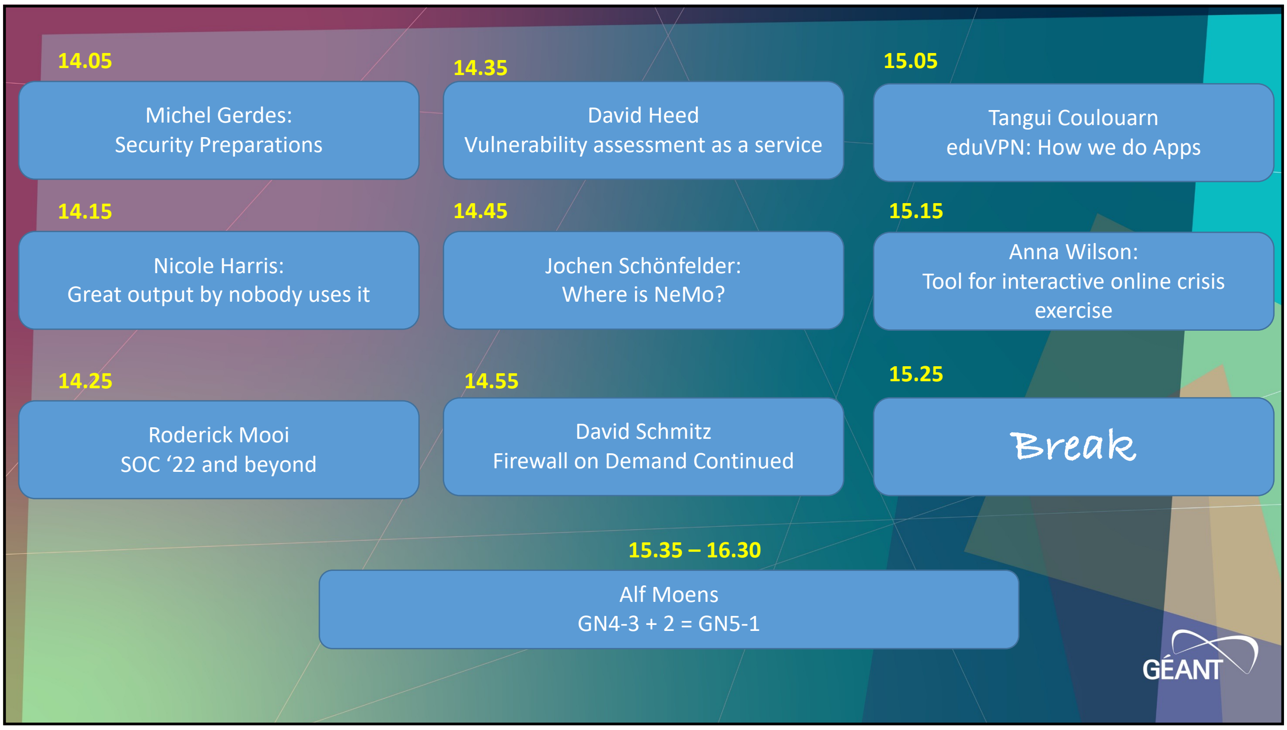
WP8 All Hands – Final year kick off

SECURITY

February 2022

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).

1



14.05
Michel Gerdes:
Security Preparations

14.15
Nicole Harris:
Great output by nobody uses it

14.25
Roderick Mooi
SOC ‘22 and beyond

14.35
David Heed
Vulnerability assessment as a service

14.45
Jochen Schönfelder:
Where is NeMo?

14.55
David Schmitz
Firewall on Demand Continued

15.05
Tangui Coulouarn
eduVPN: How we do Apps

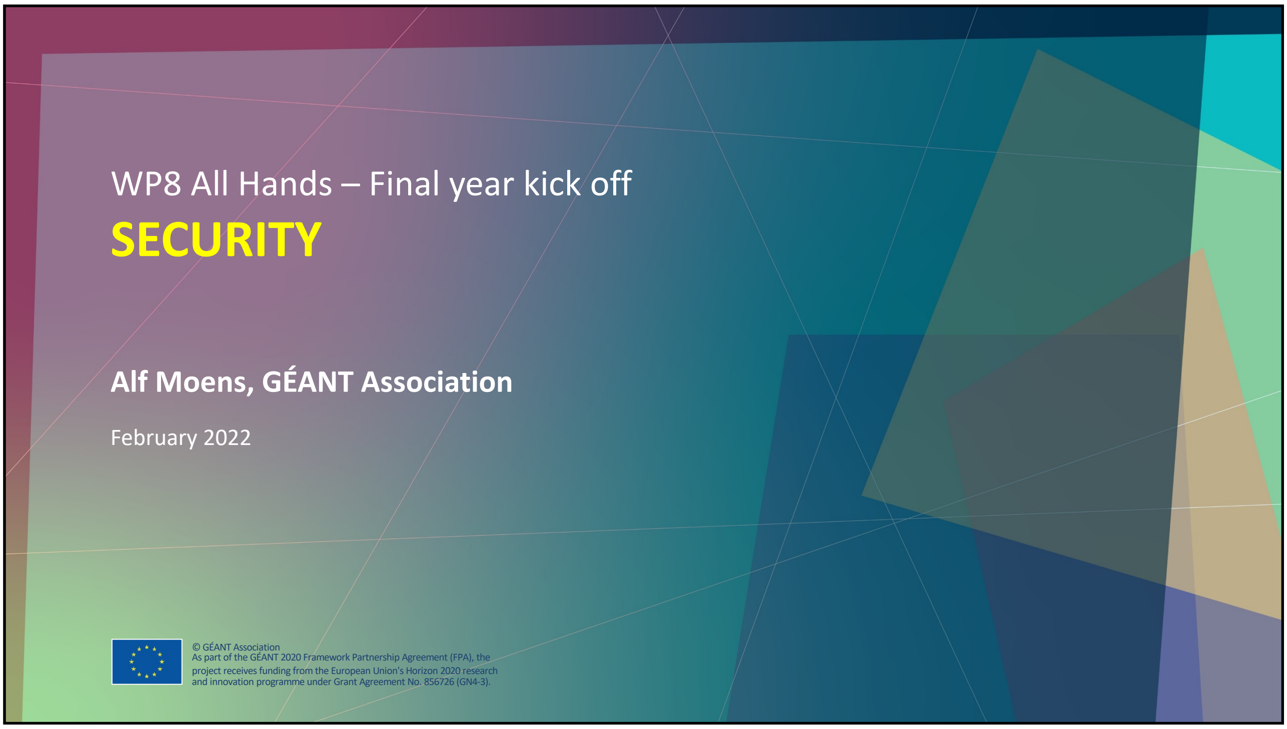
15.15
Anna Wilson:
Tool for interactive online crisis exercise

15.25
Break

15.35 – 16.30
Alf Moens
GN4-3 + 2 = GN5-1

GÉANT

2



WP8 All Hands – Final year kick off

SECURITY

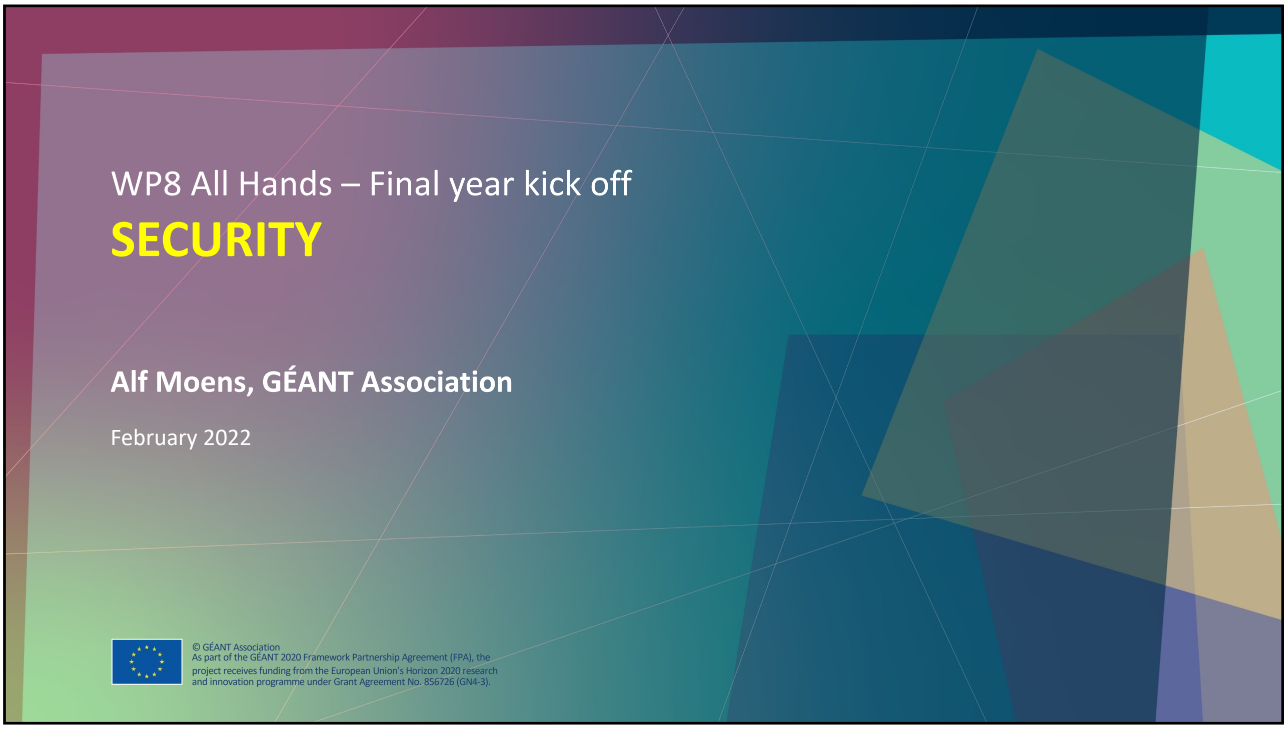
Alf Moens, GÉANT Association

February 2022

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).

3

4



WP8 All Hands – Final year kick off

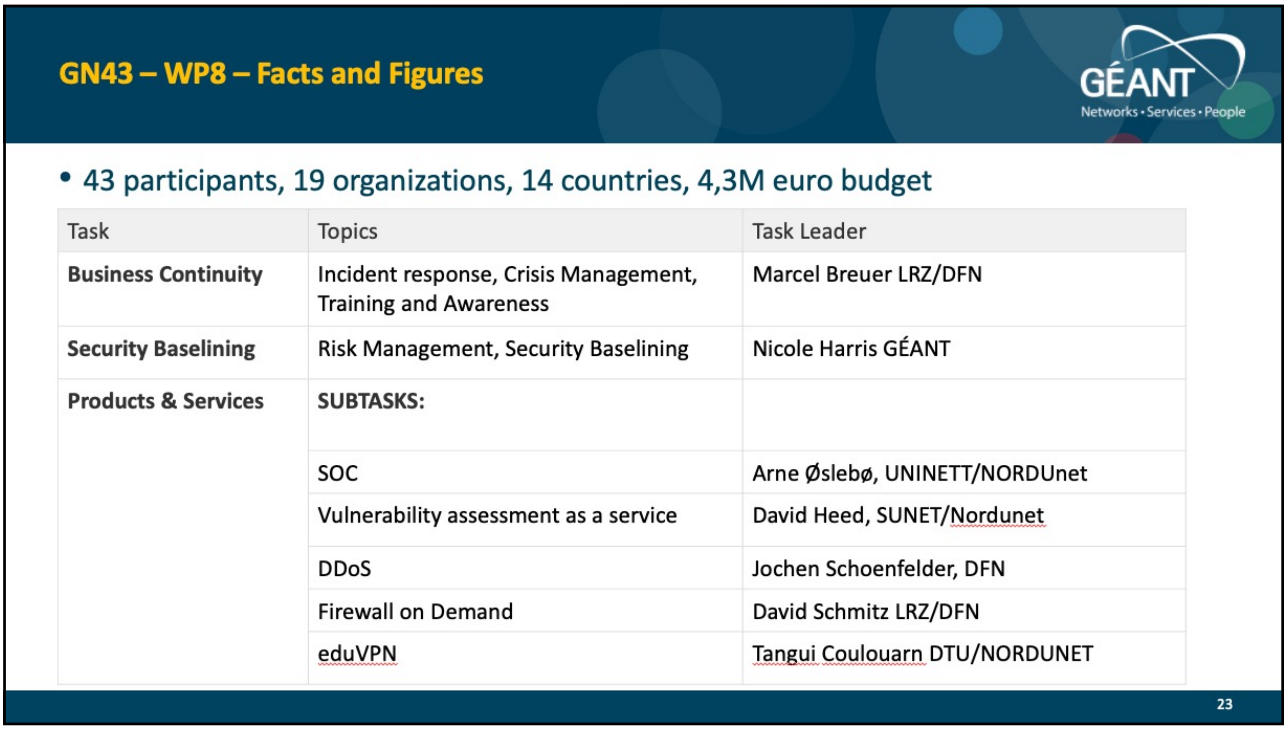
SECURITY

Alf Moens, GÉANT Association

February 2022

© GÉANT Association
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).

5



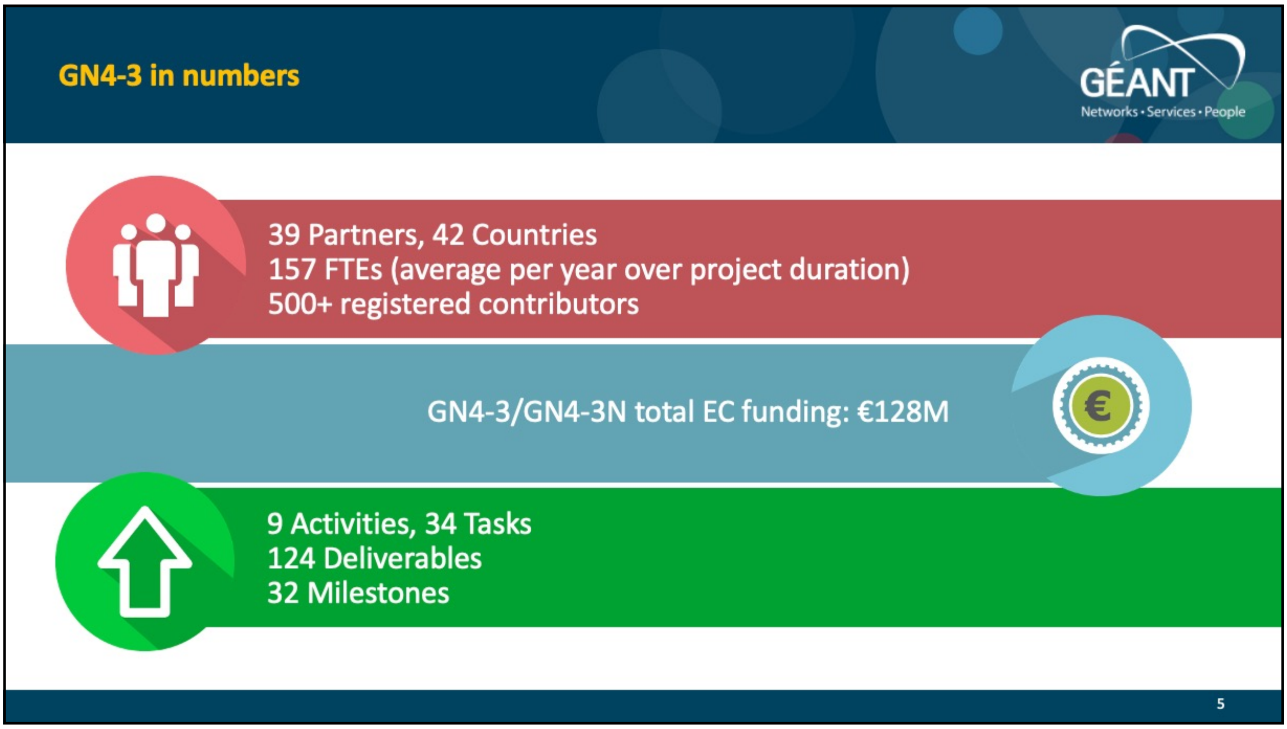
GN43 – WP8 – Facts and Figures

- 43 participants, 19 organizations, 14 countries, 4,3M euro budget

Task	Topics	Task Leader
Business Continuity	Incident response, Crisis Management, Training and Awareness	Marcel Breuer LRZ/DFN
Security Baselining	Risk Management, Security Baselining	Nicole Harris GÉANT
Products & Services	**SUBTASKS:**	
	SOC	Arne Øslebø, UNINETT/NORDUnet
	Vulnerability assessment as a service	David Heed, SUNET/Nordunet
	DDoS	Jochen Schoenfelder, DFN
	Firewall on Demand	David Schmitz LRZ/DFN
	eduVPN	Tangui Coulouarn DTU/NORDUNET

23

6



GN4-3 in numbers

GÉANT
Networks • Services • People

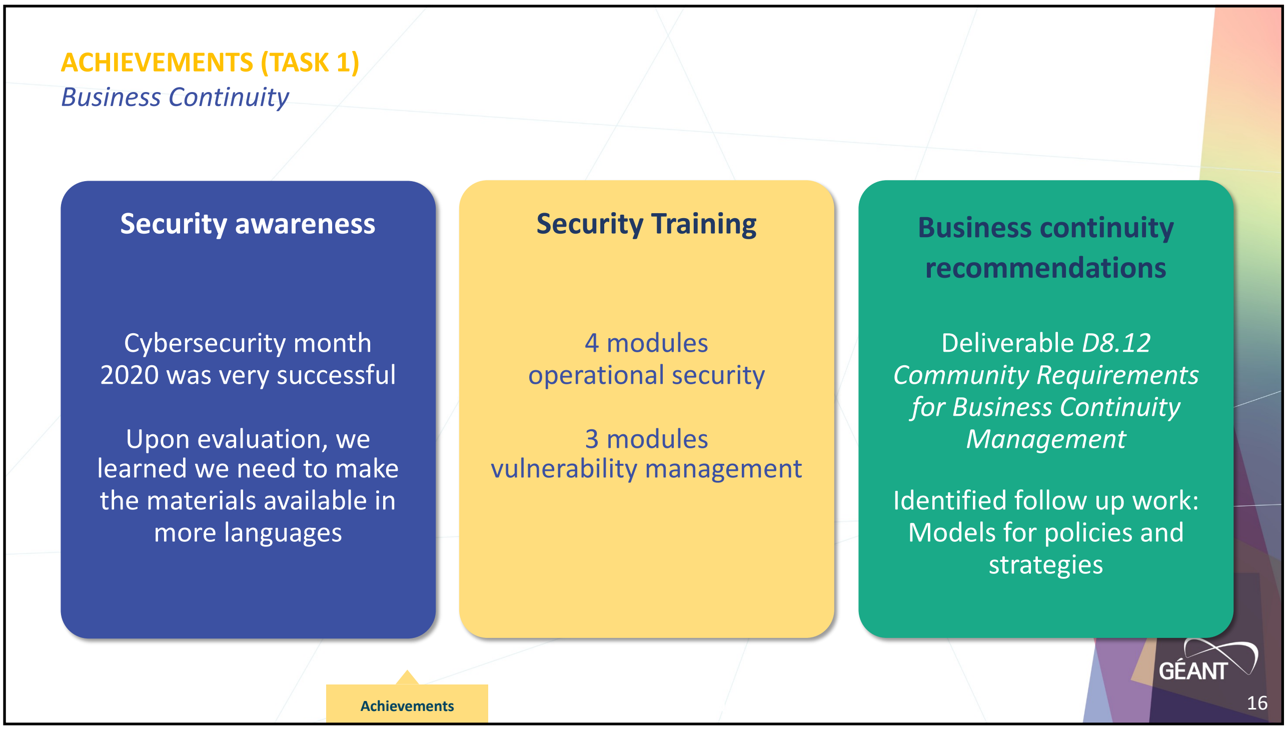
39 Partners, 42 Countries
157 FTEs (average per year over project duration)
500+ registered contributors

GN4-3/GN4-3N total EC funding: €128M

9 Activities, 34 Tasks
124 Deliverables
32 Milestones

5

7



ACHIEVEMENTS (TASK 1)

Business Continuity

Security awareness

Cybersecurity month 2020 was very successful

Upon evaluation, we learned we need to make the materials available in more languages

Security Training

4 modules operational security

3 modules vulnerability management

Business continuity recommendations

Deliverable *D8.12 Community Requirements for Business Continuity Management*

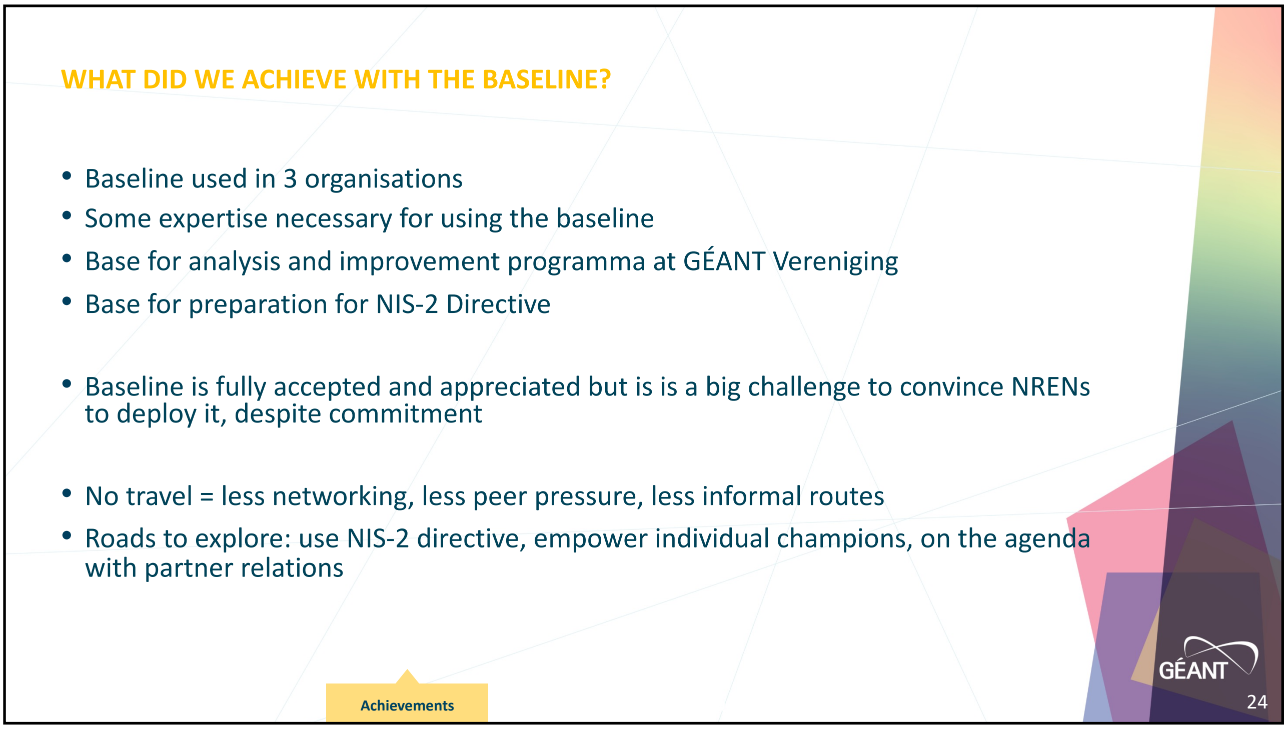
Identified follow up work: Models for policies and strategies

Achievements

GÉANT

16

8



WHAT DID WE ACHIEVE WITH THE BASELINE?

- Baseline used in 3 organisations
- Some expertise necessary for using the baseline
- Base for analysis and improvement programma at GÉANT Vereniging
- Base for preparation for NIS-2 Directive

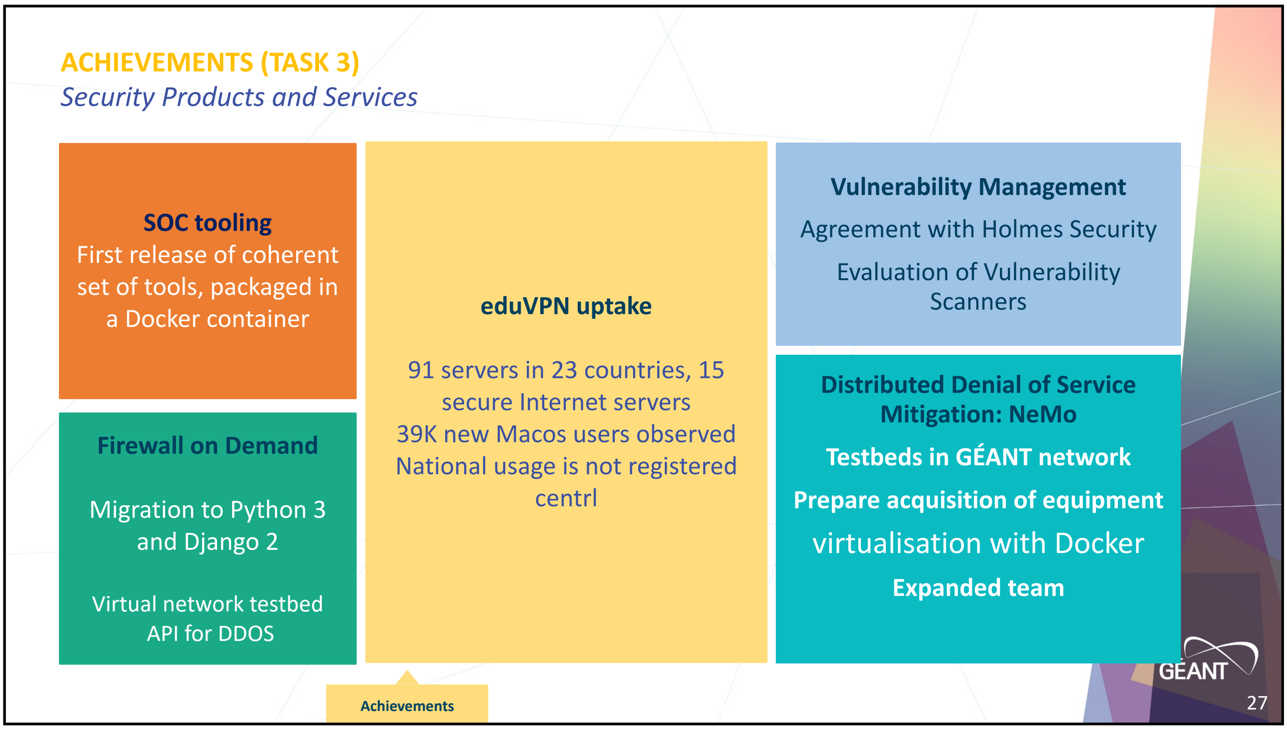
- Baseline is fully accepted and appreciated but is is a big challenge to convince NRENs to deploy it, despite commitment

- No travel = less networking, less peer pressure, less informal routes
- Roads to explore: use NIS-2 directive, empower individual champions, on the agenda with partner relations

Achievements

GÉANT

9



ACHIEVEMENTS (TASK 3)

Security Products and Services

SOC tooling
First release of coherent set of tools, packaged in a Docker container

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 centrl

Vulnerability Management

Agreement with Holmes Security

Evaluation of Vulnerability Scanners

Distributed Denial of Service Mitigation: NeMo

Testbeds in GÉANT network

Prepare acquisition of equipment

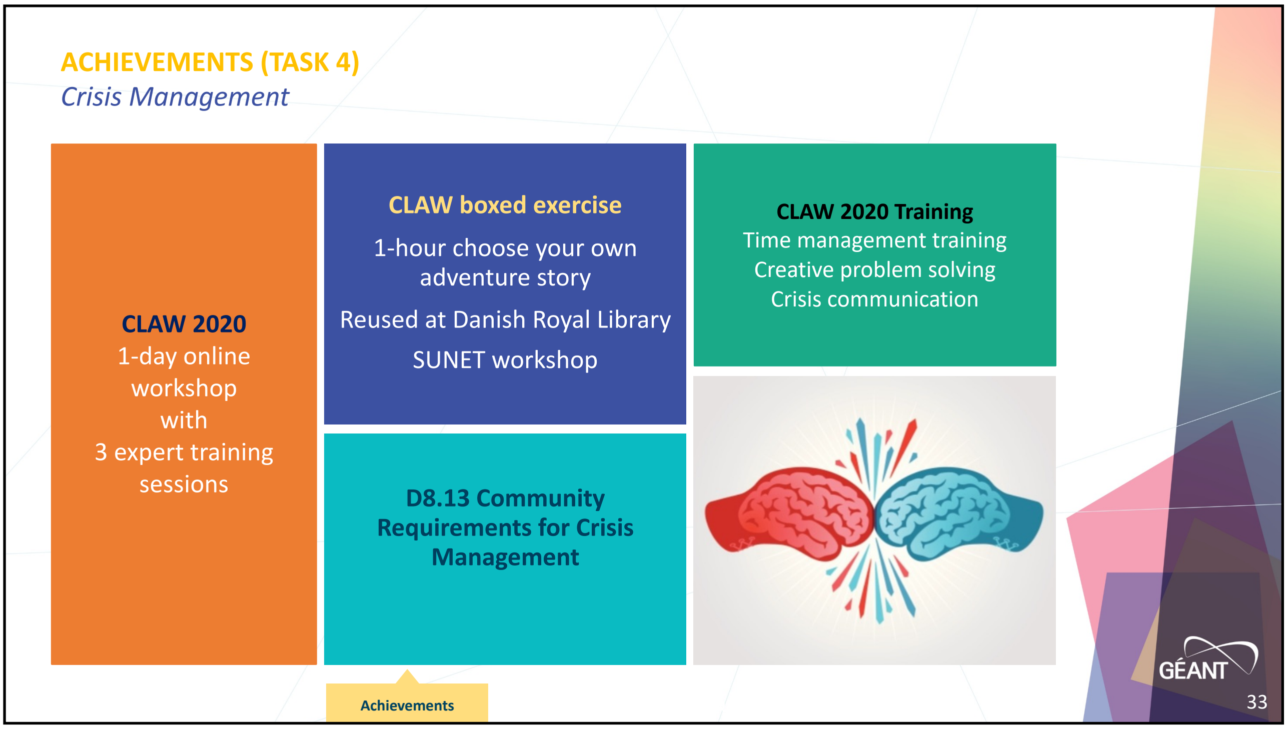
virtualisation with Docker

Expanded team

Achievements

GÉANT

10



ACHIEVEMENTS (TASK 4)

Crisis Management

CLAW 2020
1-day online workshop
with
3 expert training sessions

CLAW boxed exercise

1-hour choose your own adventure story

Reused at Danish Royal Library

SUNET workshop

CLAW 2020 Training
Time management training
Creative problem solving
Crisis communication

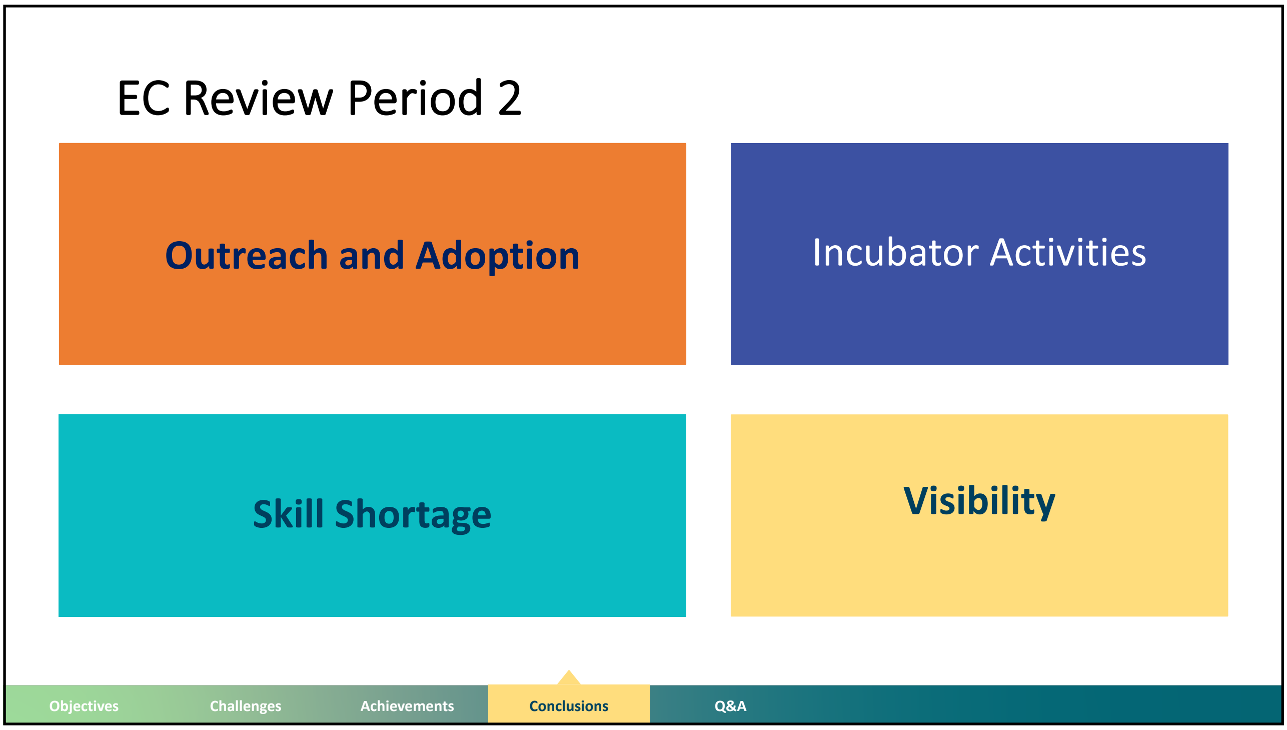
D8.13 Community Requirements for Crisis Management

Achievements

GÉANT

33

11



EC Review Period 2

Outreach and Adoption

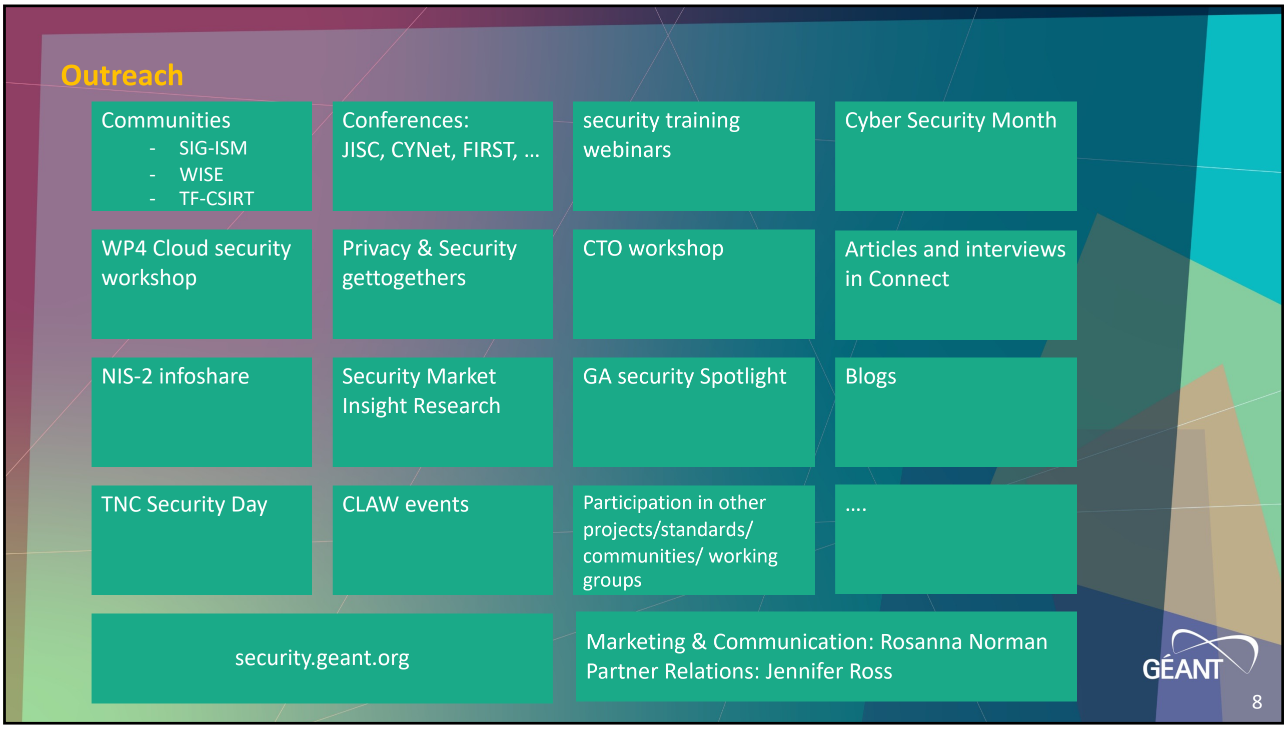
Incubator Activities

Skill Shortage

Visibility

Objectives | Challenges | Achievements | Conclusions | Q&A

12



Outreach

Communities - SIG-ISM - WISE - TF-CSIRT	Conferences: JISC, CYNet, FIRST, …	security training webinars	Cyber Security Month
WP4 Cloud security workshop	Privacy & Security gettogethers	CTO workshop	Articles and interviews in Connect
NIS-2 infoshare	Security Market Insight Research	GA security Spotlight	Blogs
TNC Security Day	CLAW events	Participation in other projects/standards/ communities/ working groups	….

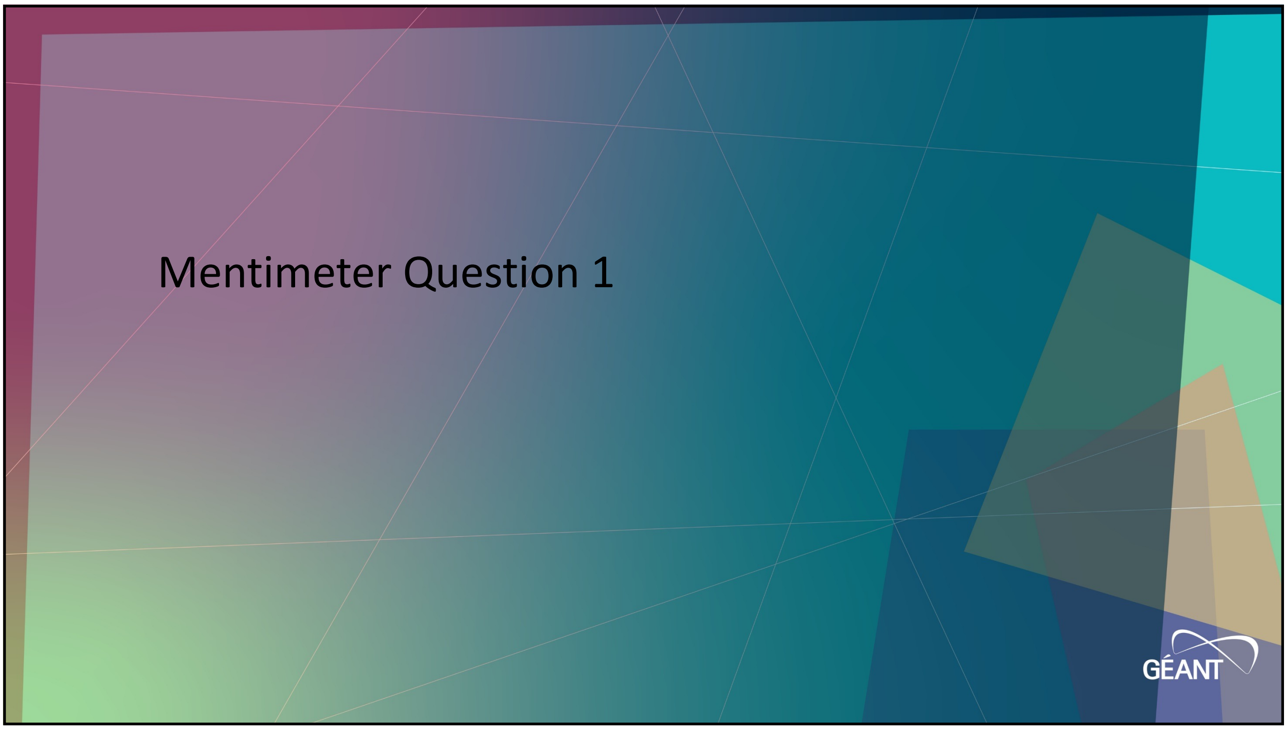
security.geant.org

Marketing & Communication: Rosanna Norman
Partner Relations: Jennifer Ross

GÉANT

8

13



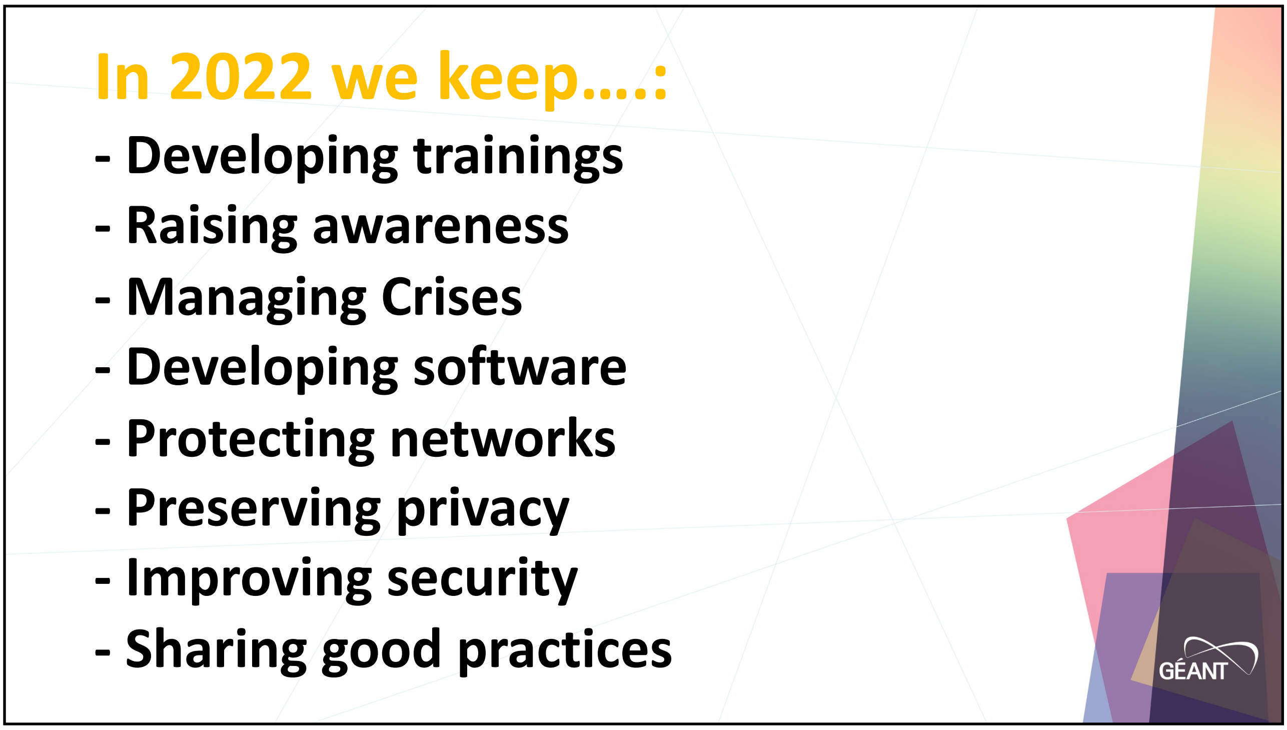
Mentimeter Question 1

GÉANT

14

2022

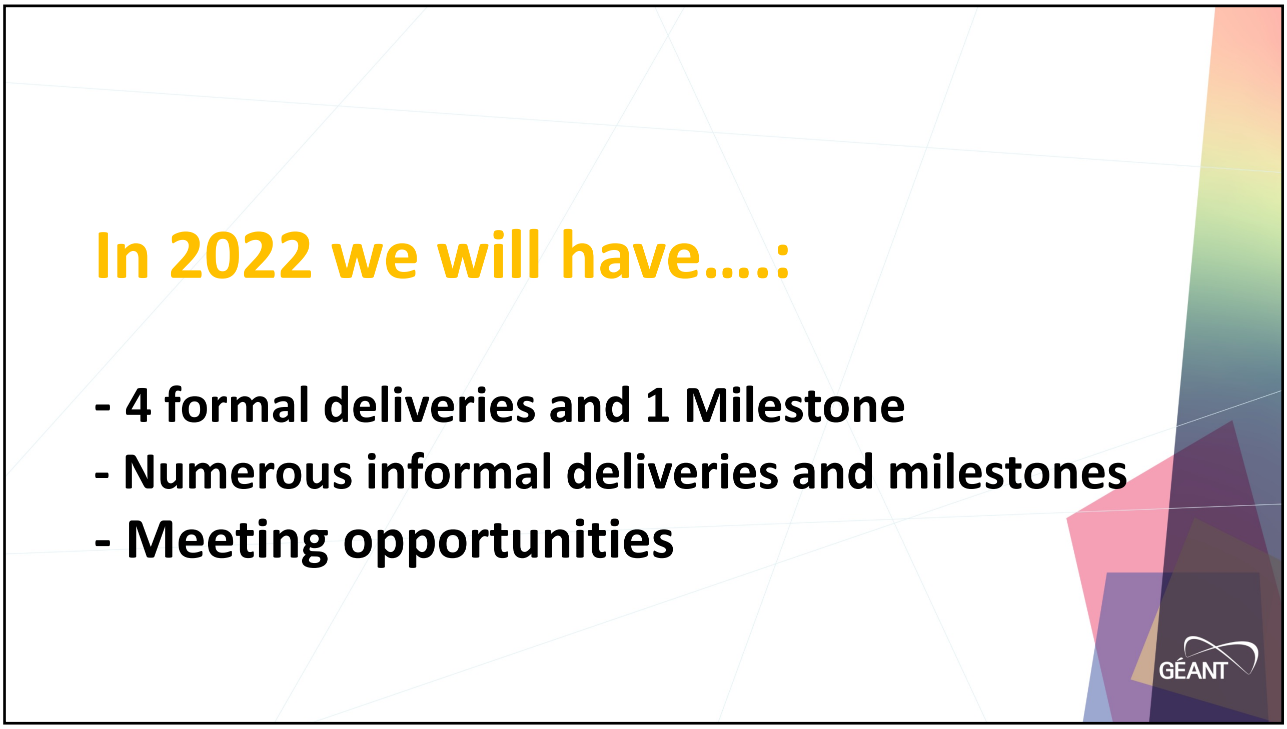
15



In 2022 we keep….:

- Developing trainings
- Raising awareness
- Managing Crises
- Developing software
- Protecting networks
- Preserving privacy
- Improving security
- Sharing good practices

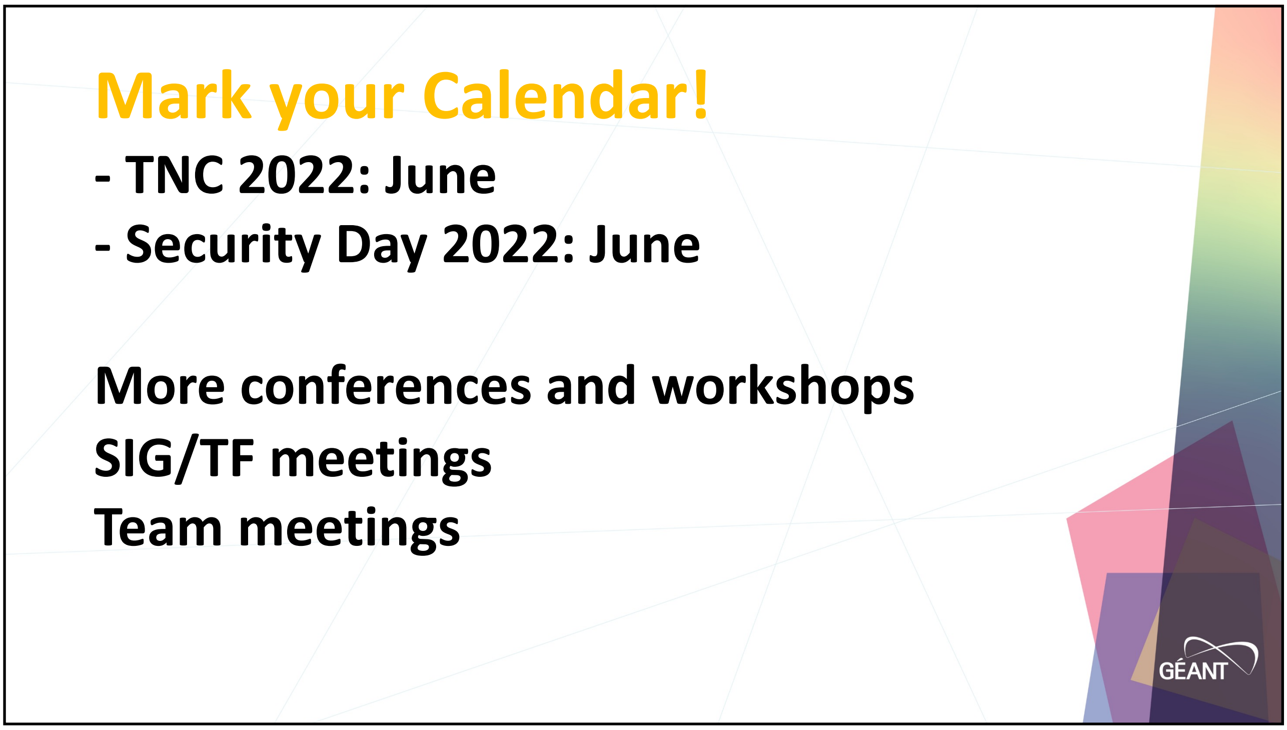
16



In 2022 we will have….:

- 4 formal deliveries and 1 Milestone
- Numerous informal deliveries and milestones
- Meeting opportunities

17



Mark your Calendar!

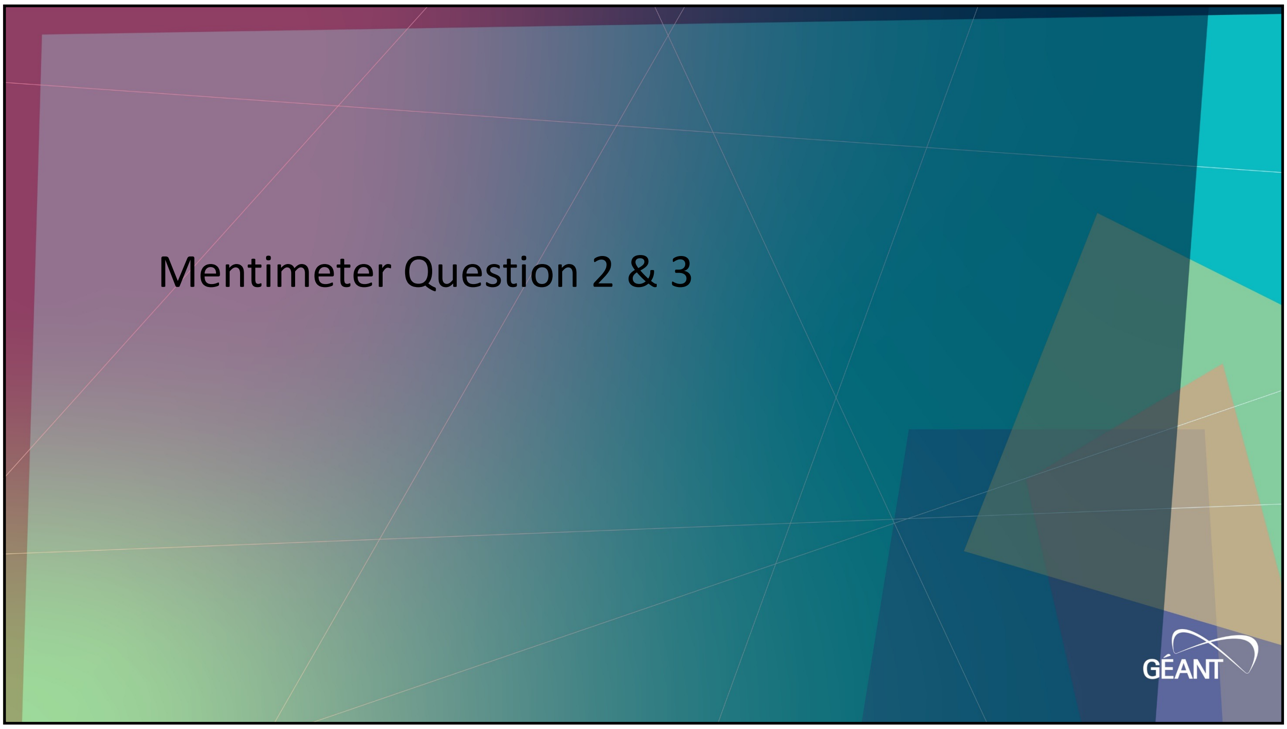
- TNC 2022: June
- Security Day 2022: June

More conferences and workshops

SIG/TF meetings

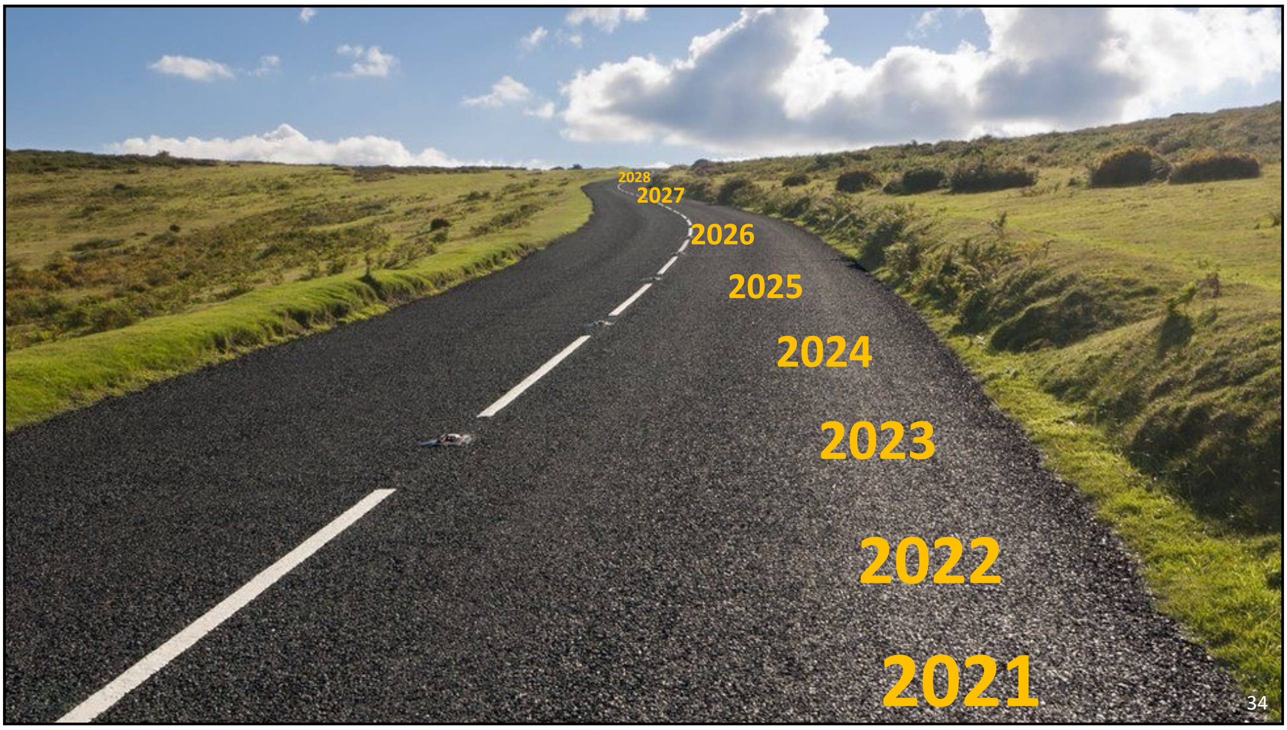
Team meetings

18

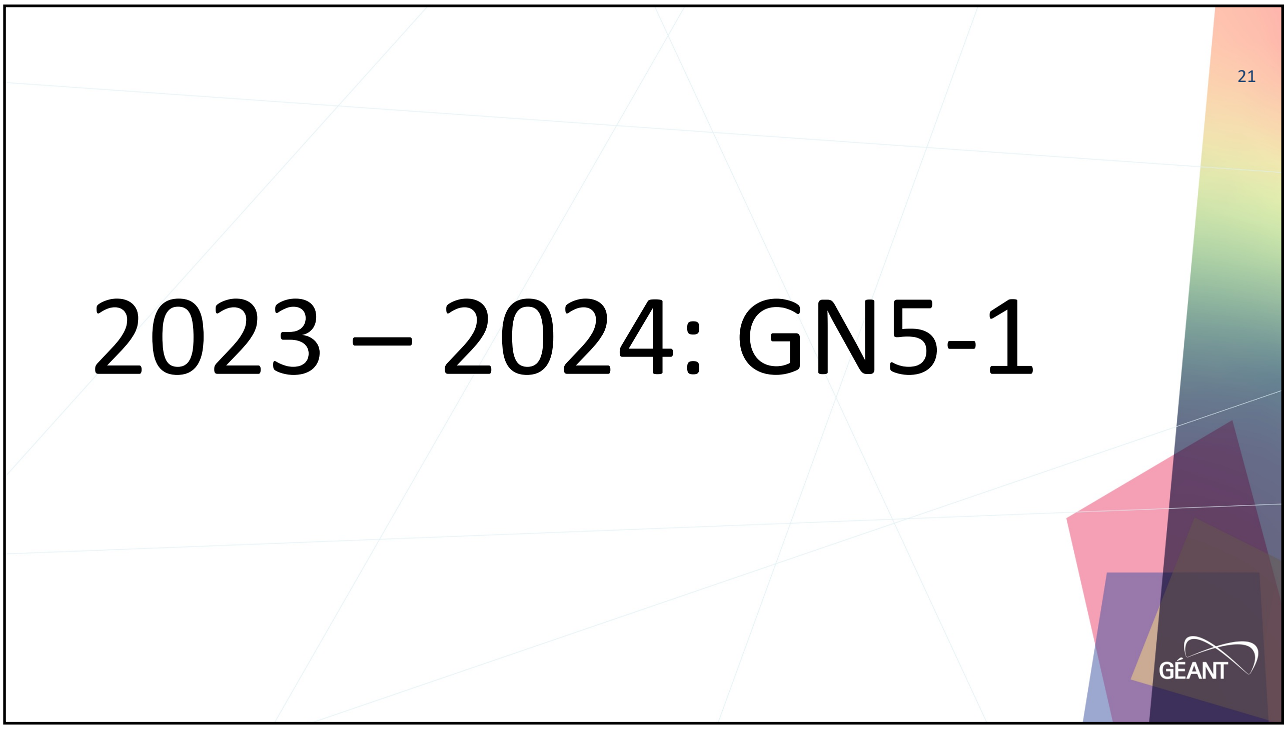


Mentimeter Question 2 & 3

19



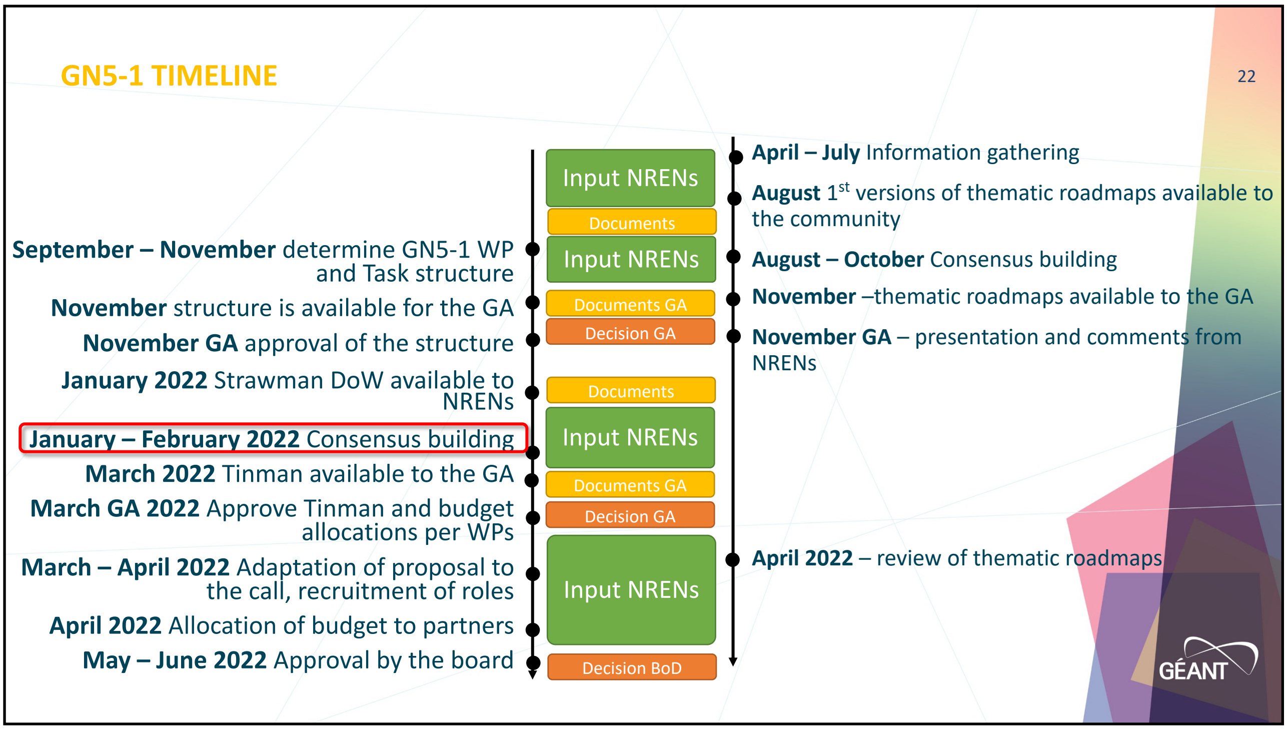
20



21

2023 – 2024: GN5-1

21



GN5-1 TIMELINE

22

September – November determine GN5-1 WP and Task structure

November structure is available for the GA

November GA approval of the structure

January 2022 Strawman DoW available to NRENs

January – February 2022 Consensus building

March 2022 Tinman available to the GA

March GA 2022 Approve Tinman and budget allocations per WPs

March – April 2022 Adaptation of proposal to the call, recruitment of roles

April 2022 Allocation of budget to partners

May – June 2022 Approval by the board

Input NRENs

Documents

Input NRENs

Documents GA

Decision GA

Documents

Input NRENs

Documents GA

Decision GA

Input NRENs

Decision BoD

April – July Information gathering

August 1st versions of thematic roadmaps available to the community

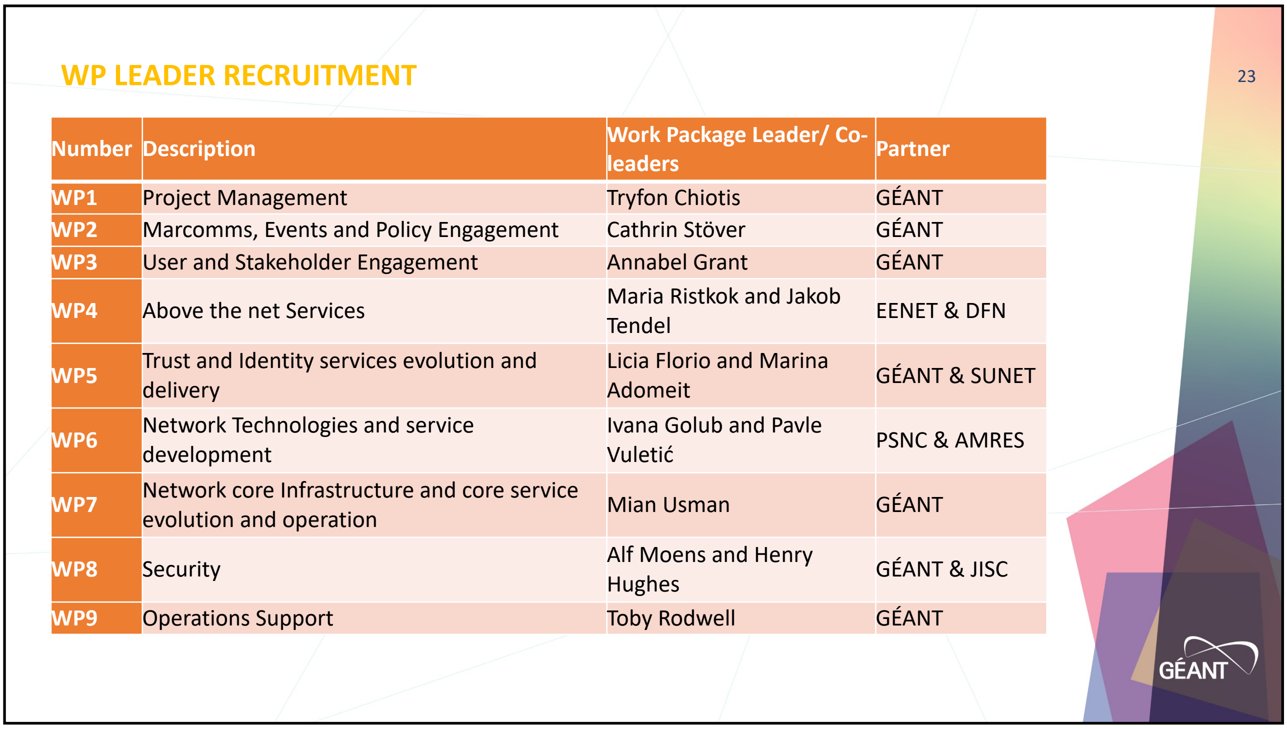
August – October Consensus building

November –thematic roadmaps available to the GA

November GA – presentation and comments from NRENs

April 2022 – review of thematic roadmaps

22

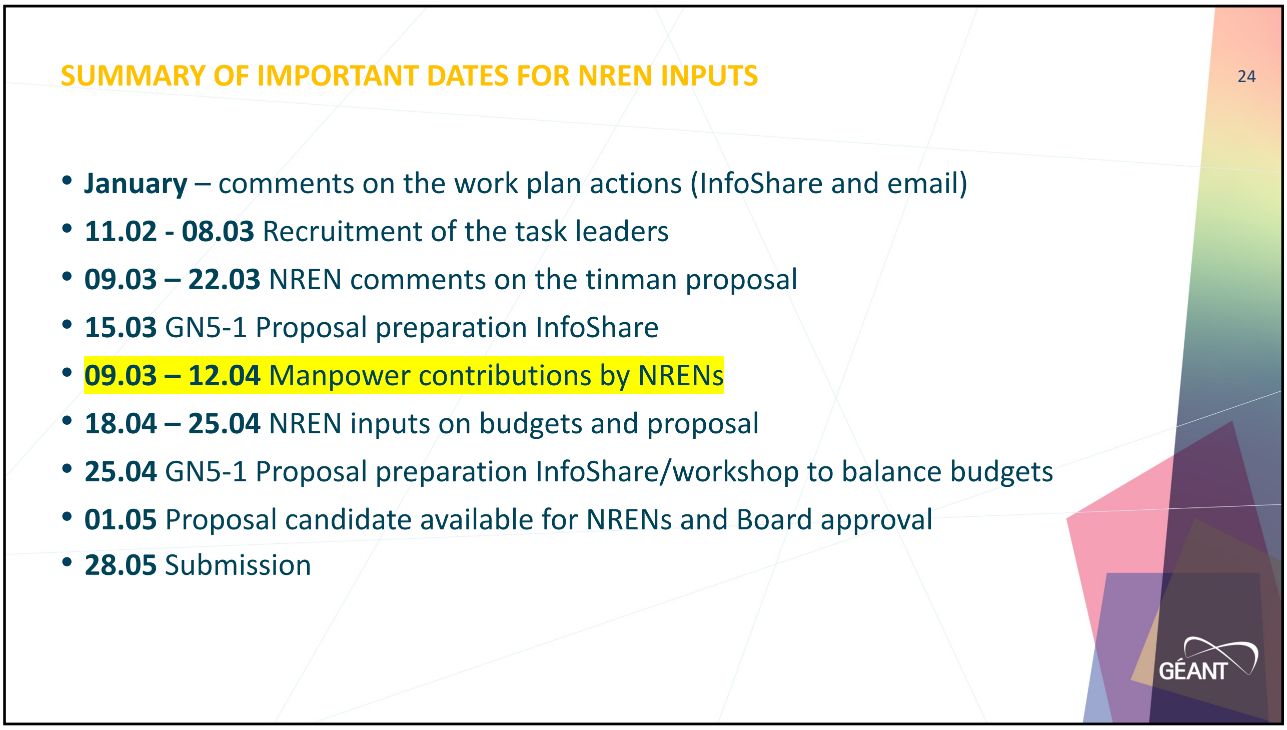


WP LEADER RECRUITMENT

23

Number	Description	Work Package Leader/ Co-leaders	Partner
WP1	Project Management	Tryfon Chiotis	GÉANT
WP2	Marcomms, Events and Policy Engagement	Cathrin Stöver	GÉANT
WP3	User and Stakeholder Engagement	Annabel Grant	GÉANT
WP4	Above the net Services	Maria Ristkok and Jakob Tendel	EENET & DFN
WP5	Trust and Identity services evolution and delivery	Licia Florio and Marina Adomeit	GÉANT & SUNET
WP6	Network Technologies and service development	Ivana Golub and Pavle Vuletić	PSNC & AMRES
WP7	Network core Infrastructure and core service evolution and operation	Mian Usman	GÉANT
WP8	Security	Alf Moens and Henry Hughes	GÉANT & JISC
WP9	Operations Support	Toby Rodwell	GÉANT

23



SUMMARY OF IMPORTANT DATES FOR NREN INPUTS

24

- **January** – comments on the work plan actions (InfoShare and email)
- **11.02 - 08.03** Recruitment of the task leaders
- **09.03 – 22.03** NREN comments on the tinman proposal
- **15.03** GN5-1 Proposal preparation InfoShare
- **09.03 – 12.04** Manpower contributions by NRENs
- **18.04 – 25.04** NREN inputs on budgets and proposal
- **25.04** GN5-1 Proposal preparation InfoShare/workshop to balance budgets
- **01.05** Proposal candidate available for NRENs and Board approval
- **28.05** Submission

24

WP8: Security

Alf Moens (GÉANT), Henry Hughes (Jisc)

GN5-1 Proposal Development Infoshare
27 January 2022

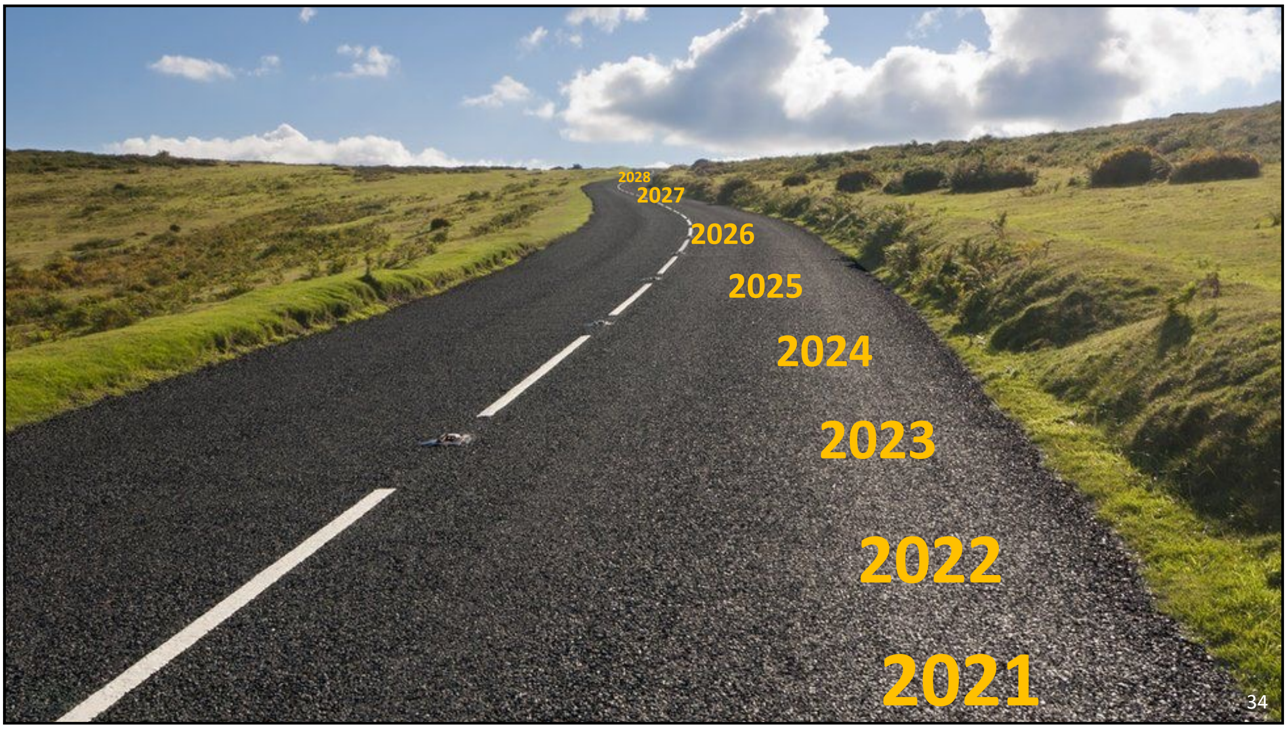
WP8: Security
Overview and objectives

WP8 Overview

- Development and delivery of security products, services and expertise

WP8 Objectives

- Support NRENs and GÉANT to provide a safe and secure infrastructure and services for Research and Education on national, European and global level, reducing the likelihood of major disruptions to services or loss of data.
- Develop human capital on the subject of security, both general knowledge and expert level
- Identify security services and intiatives in R&E and promote sharing and cross usage



2028

2027

2026

2025

2024

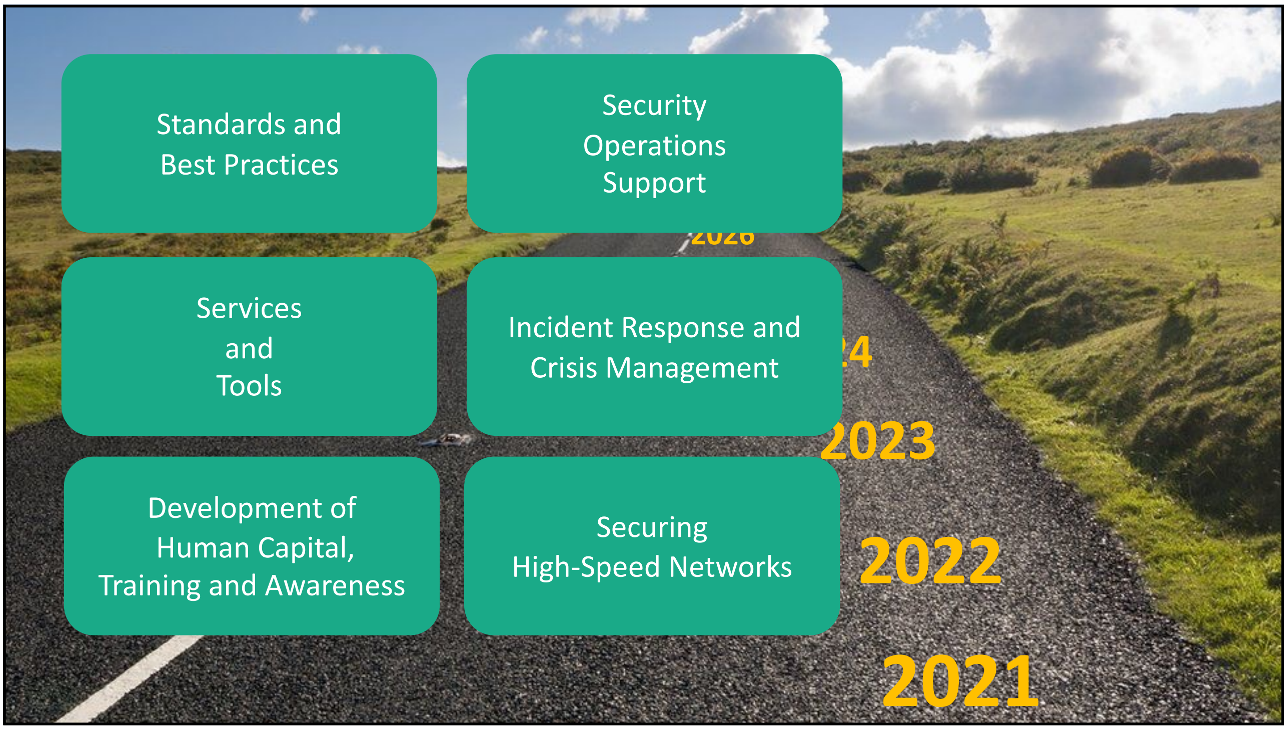
2023

2022

2021

34

27



Standards and Best Practices

Security Operations Support

Services and Tools

Incident Response and Crisis Management

Development of Human Capital, Training and Awareness

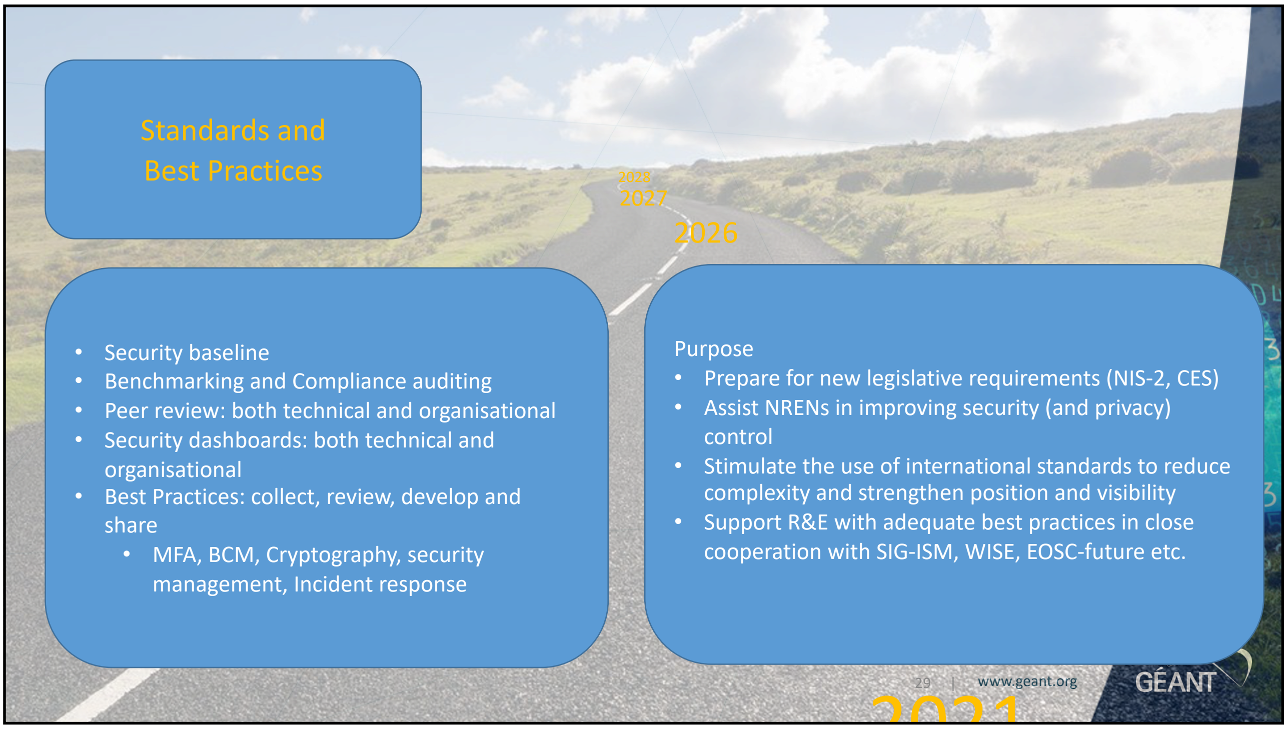
Securing High-Speed Networks

2023

2022

2021

28

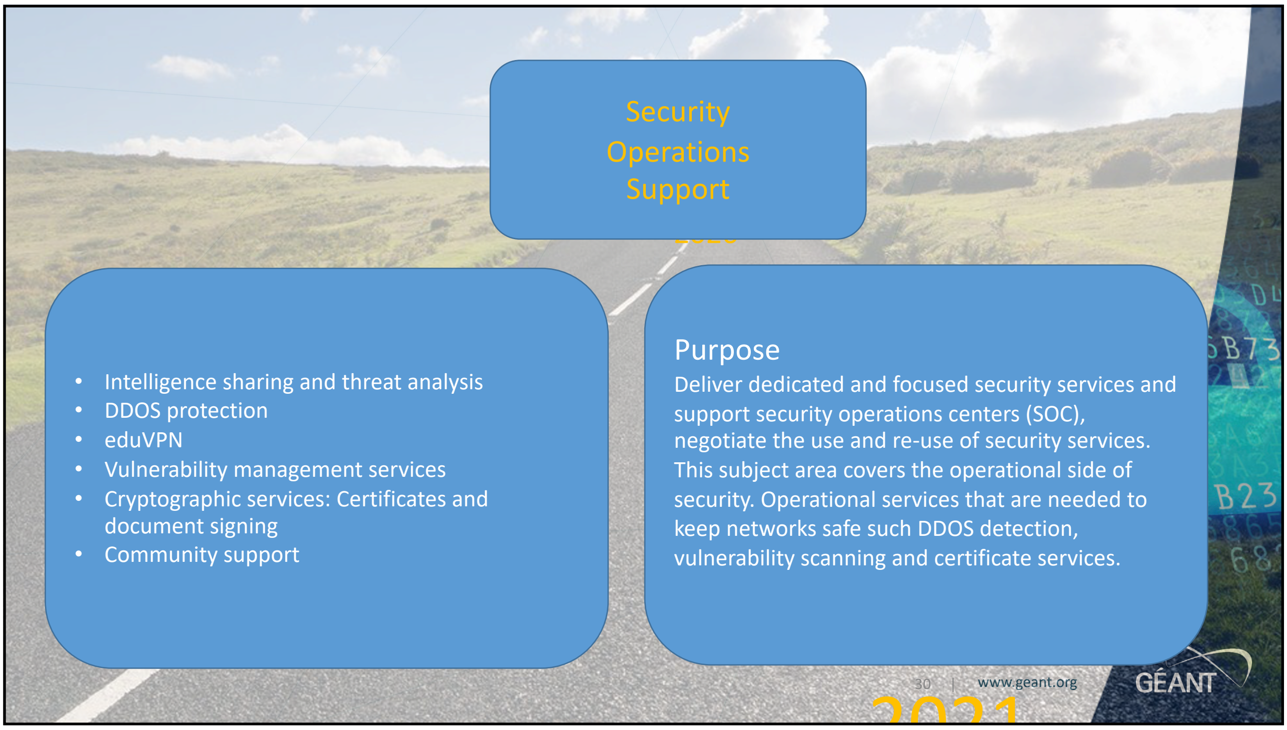

2028
2027
2026
29
www.geant.org
GÉANT
2021

Standards and Best Practices

- Security baseline
- Benchmarking and Compliance auditing
- Peer review: both technical and organisational
- Security dashboards: both technical and organisational
- Best Practices: collect, review, develop and share
  - MFA, BCM, Cryptography, security management, Incident response

Purpose

- Prepare for new legislative requirements (NIS-2, CES)
- Assist NRENs in improving security (and privacy) control
- Stimulate the use of international standards to reduce complexity and strengthen position and visibility
- Support R&E with adequate best practices in close cooperation with SIG-ISM, WISE, EOSC-future etc.

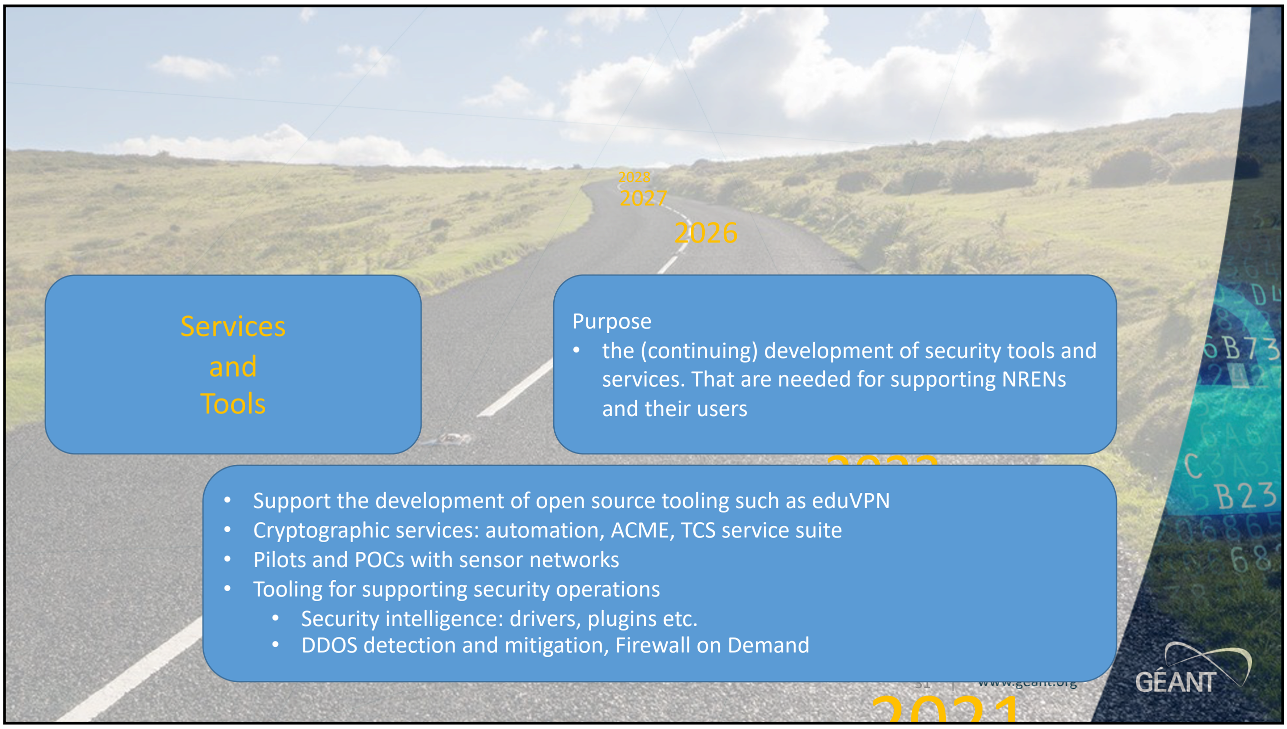

30
www.geant.org
GÉANT
2021

Security Operations Support

- Intelligence sharing and threat analysis
- DDOS protection
- eduVPN
- Vulnerability management services
- Cryptographic services: Certificates and document signing
- Community support

Purpose

Deliver dedicated and focused security services and support security operations centers (SOC), negotiate the use and re-use of security services. This subject area covers the operational side of security. Operational services that are needed to keep networks safe such DDOS detection, vulnerability scanning and certificate services.


2028
2027
2026
2021
www.geant.org
GÉANT

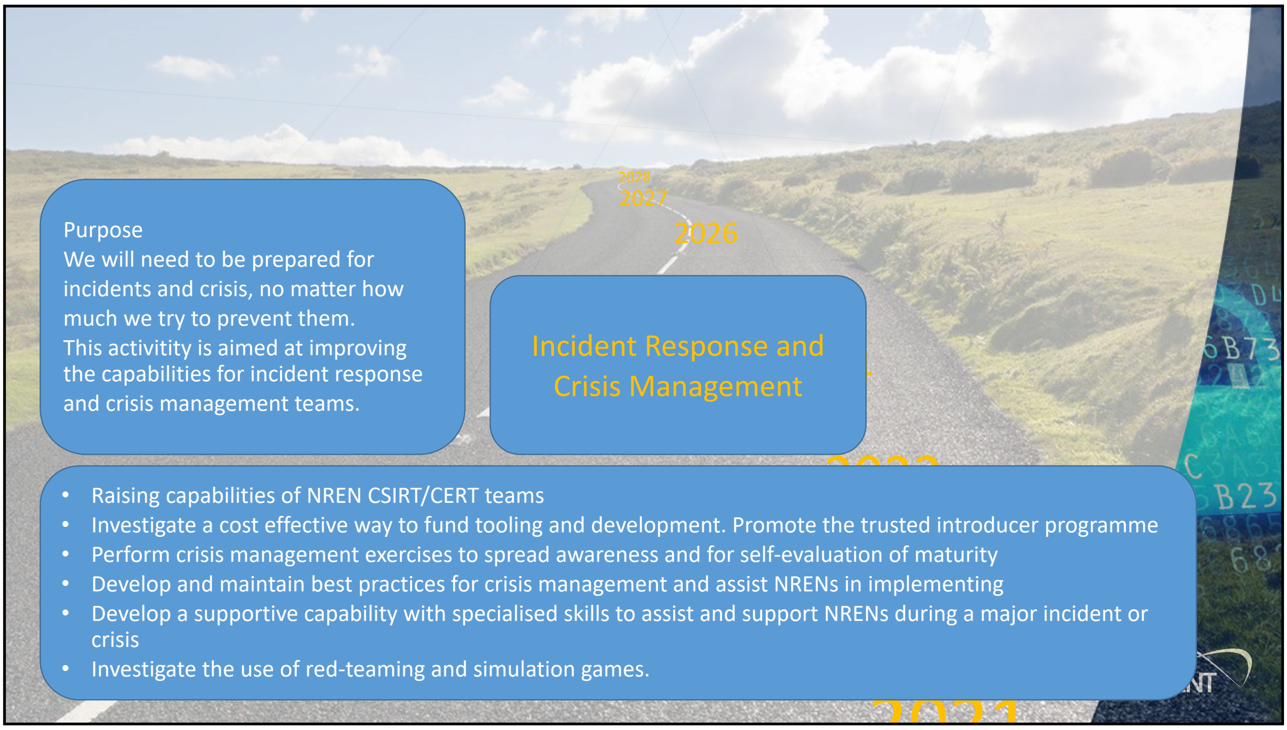
Services and Tools

Purpose

- the (continuing) development of security tools and services. That are needed for supporting NRENs and their users

- Support the development of open source tooling such as eduVPN
- Cryptographic services: automation, ACME, TCS service suite
- Pilots and POCs with sensor networks
- Tooling for supporting security operations
  - Security intelligence: drivers, plugins etc.
  - DDOS detection and mitigation, Firewall on Demand

31

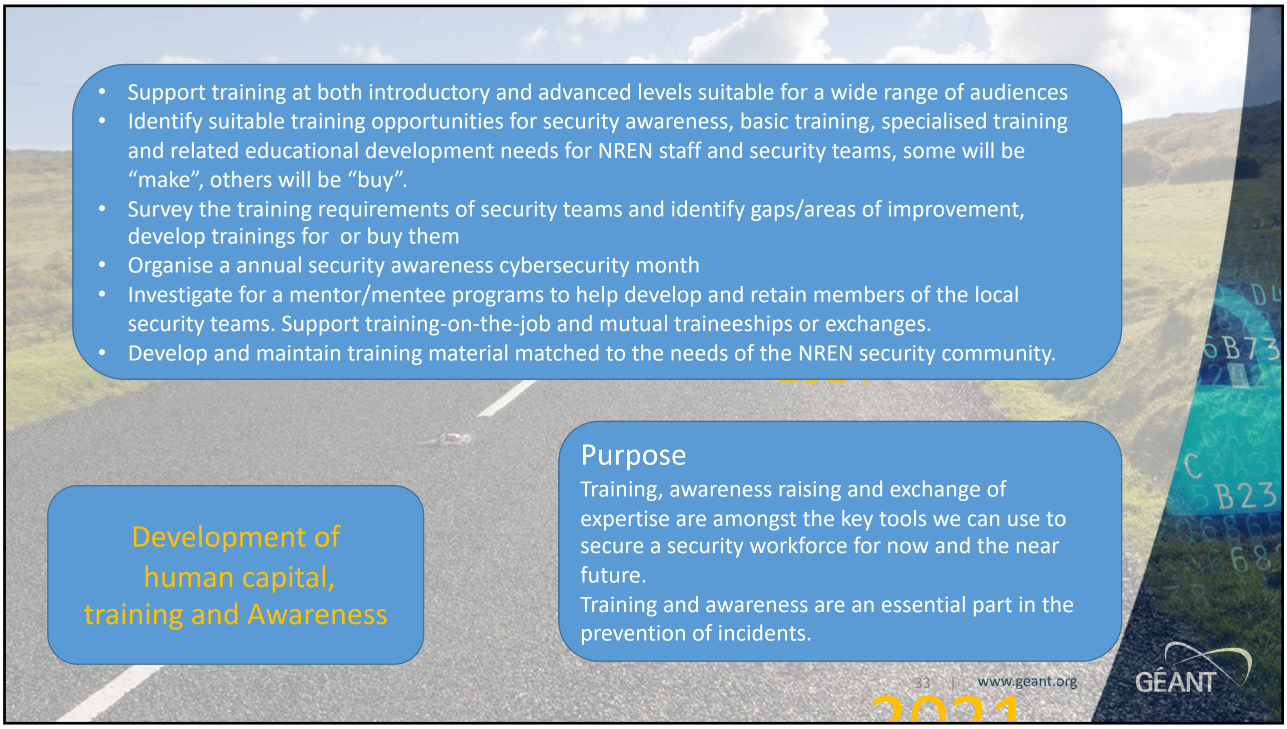

2028
2027
2026
2021

Purpose
We will need to be prepared for incidents and crisis, no matter how much we try to prevent them.
This actitivity is aimed at improving the capabilities for incident response and crisis management teams.

Incident Response and Crisis Management

- Raising capabilities of NREN CSIRT/CERT teams
- Investigate a cost effective way to fund tooling and development. Promote the trusted introducer programme
- Perform crisis management exercises to spread awareness and for self-evaluation of maturity
- Develop and maintain best practices for crisis management and assist NRENs in implementing
- Develop a supportive capability with specialised skills to assist and support NRENs during a major incident or crisis
- Investigate the use of red-teaming and simulation games.

32



- Support training at both introductory and advanced levels suitable for a wide range of audiences
- Identify suitable training opportunities for security awareness, basic training, specialised training and related educational development needs for NREN staff and security teams, some will be “make”, others will be “buy”.
- Survey the training requirements of security teams and identify gaps/areas of improvement, develop trainings for or buy them
- Organise a annual security awareness cybersecurity month
- Investigate for a mentor/mentee programs to help develop and retain members of the local security teams. Support training-on-the-job and mutual traineeships or exchanges.
- Develop and maintain training material matched to the needs of the NREN security community.

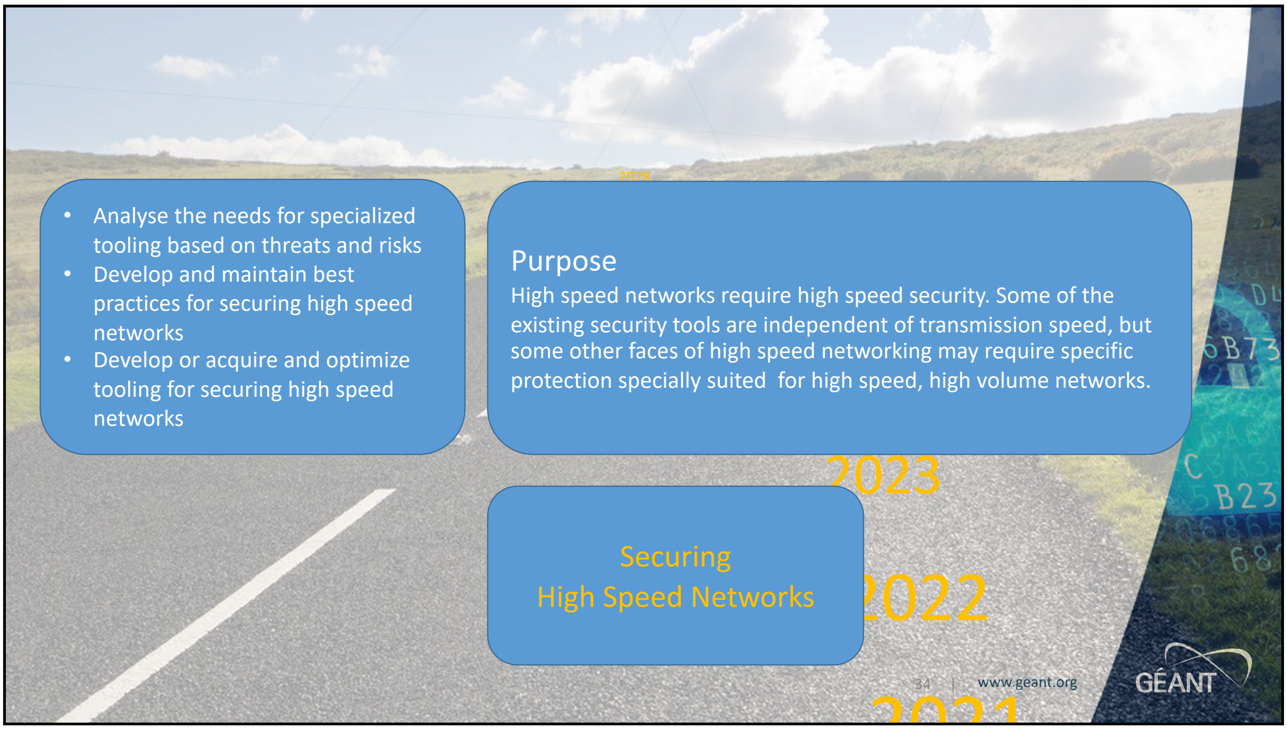
Development of human capital, training and Awareness

Purpose

Training, awareness raising and exchange of expertise are amongst the key tools we can use to secure a security workforce for now and the near future.

Training and awareness are an essential part in the prevention of incidents.

33



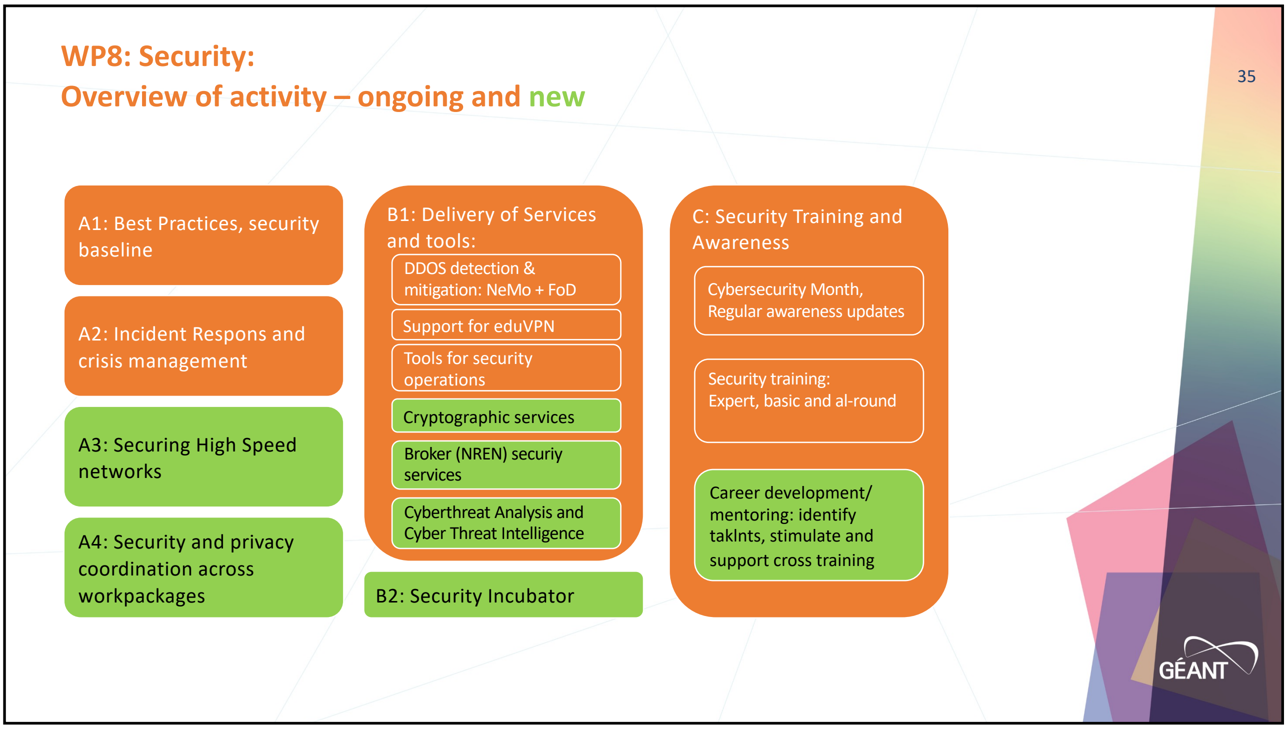
- Analyse the needs for specialized tooling based on threats and risks
- Develop and maintain best practices for securing high speed networks
- Develop or acquire and optimize tooling for securing high speed networks

Purpose

High speed networks require high speed security. Some of the existing security tools are independent of transmission speed, but some other faces of high speed networking may require specific protection specially suited for high speed, high volume networks.

Securing High Speed Networks

34



WP8: Security:
Overview of activity – ongoing and new

A1: Best Practices, security baseline

A2: Incident Respons and crisis management

A3: Securing High Speed networks

A4: Security and privacy coordination across workpackages

B1: Delivery of Services and tools:

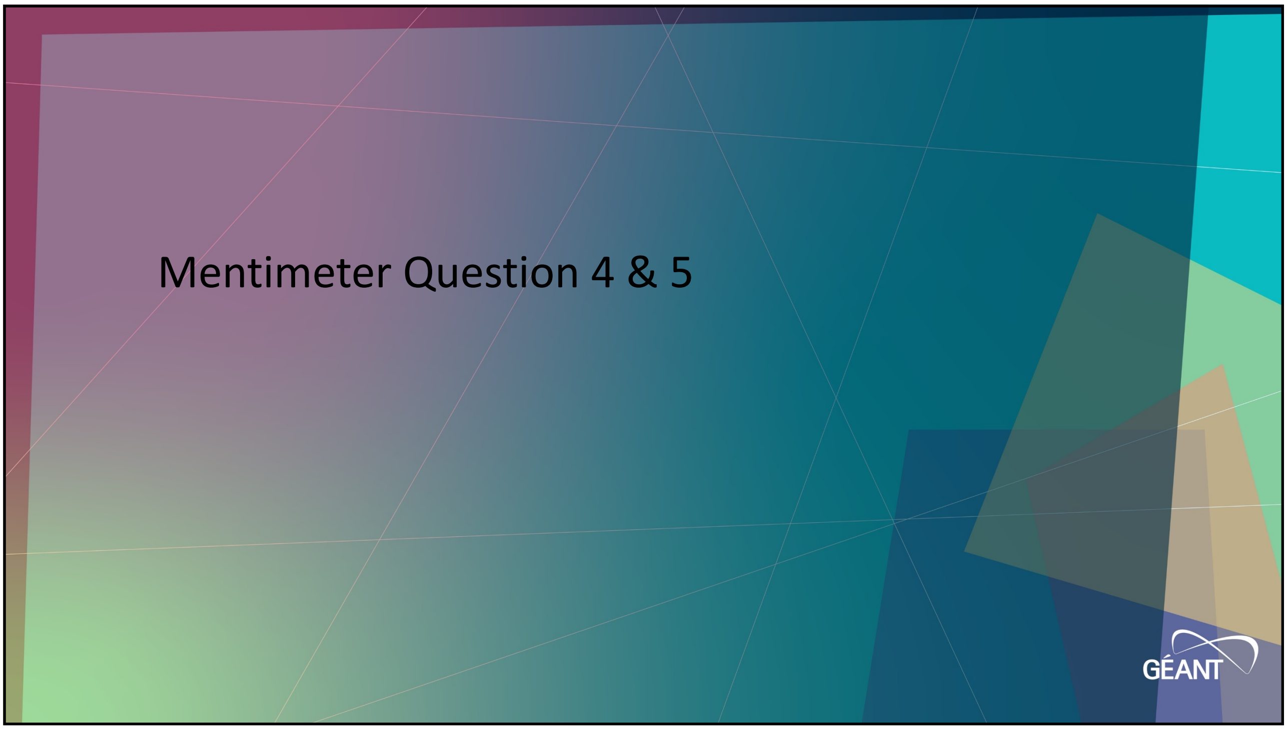
- DDOS detection & mitigation: NeMo + FoD
- Support for eduVPN
- Tools for security operations
- Cryptographic services
- Broker (NREN) securiy services
- Cyberthreat Analysis and Cyber Threat Intelligence

B2: Security Incubator

C: Security Training and Awareness

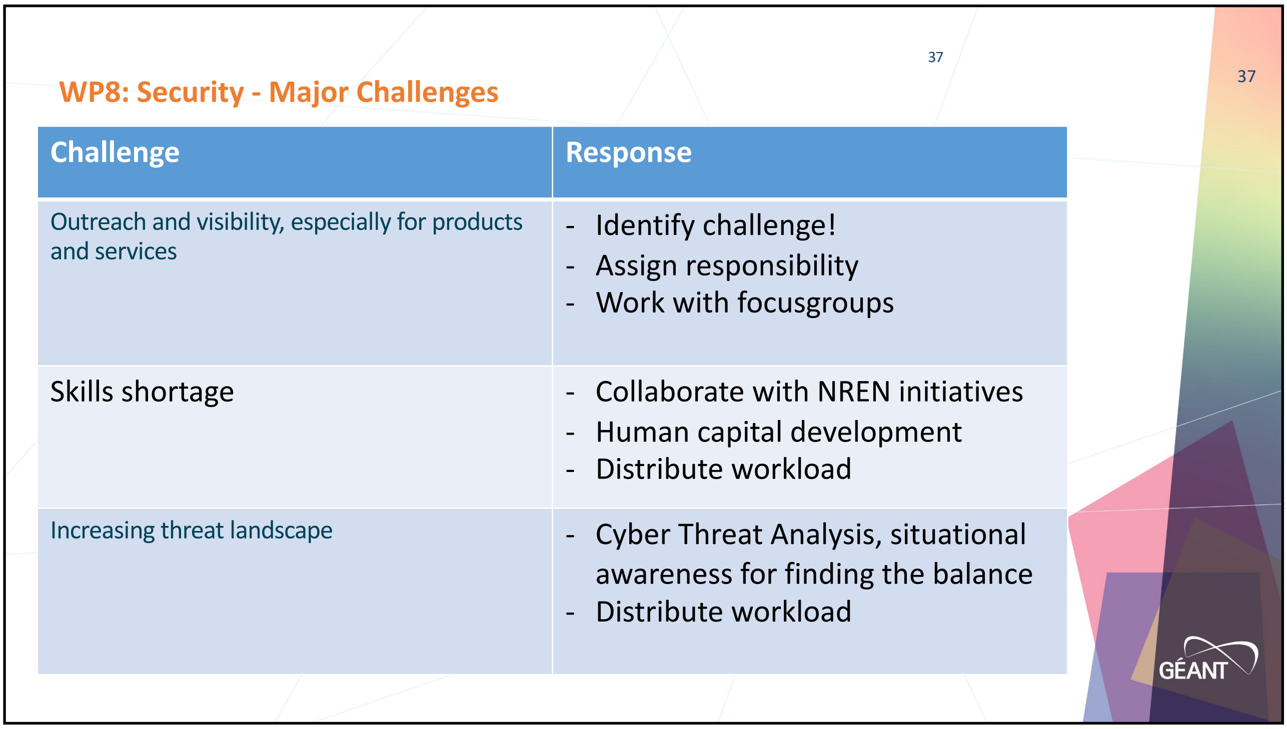
- Cybersecurity Month, Regular awareness updates
- Security training: Expert, basic and al-round
- Career development/ mentoring: identify taklnts, stimulate and support cross training

35



Mentimeter Question 4 & 5

36



WP8: Security - Major Challenges

Challenge	Response
Outreach and visibility, especially for products and services	- Identify challenge! - Assign responsibility - Work with focusgroups
Skills shortage	- Collaborate with NREN initiatives - Human capital development - Distribute workload
Increasing threat landscape	- Cyber Threat Analysis, situational awareness for finding the balance - Distribute workload

37

Thank you!

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).

38