

tnc23

DIGITAL GENERATIONS

TIRANA, ALBANIA | 5-9 JUNE 2023

GN5-1 WP3 T3 + Security Products and services

David Heed (Joint T3 tasklead / SUNET security center)

TNC23 Security Day 5 June 2023



Co-funded by
the European Union



Agenda

- A bit on the new GN5-1 project in regards to Security products and services
- Presentation on some tools provided to the academic community
- Local examples from NRENs
- Input for what is lacking in area (?)

GN4-3 WP8 in retrospective

Proud off:

- achieved all planned deliverables and milestones 😊
- Tool and products,
- Papers and blogs,
- Events, events, events

And above all: recognition



GN5-1 in numbers: 2023 - 2024

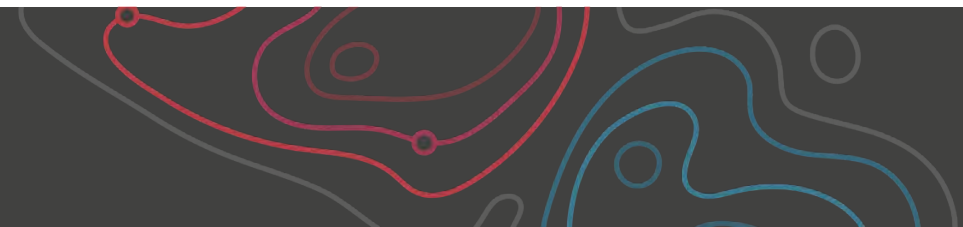


37 Partners (including GÉANT Association), 2 Associated Partners (SWITCH, JISC), 44 Countries
200+ FTEs (average per year over project duration)

GN5-1 total costs: € 82.64 M; EC funding: € 55M



9 Work Packages, 42 Tasks
36 Deliverables
46 Milestones



GN4-3 WP8

- 4 year project: 2019 – 2022
- 4,7 Meuro (including travel), 578 PM (144 /year)

GN5-1 WP8

- 2 year project: 2023 – 2024
- 2,8 Meuro (excluding travel), 376 PM (188 /year = ~ 18 fte)

GN5-2 WP8

- 2 year project: 2025 – 2026
- +50% budget (?)

GN5-1 WP8: Security – Overview of activity – ongoing and new

Task 1: Best Practices, Security Baseline

Task 4: Research

Securing High Speed networks

Security Incubator

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

Cyber Threat Intelligence

R&E Security Intelligence Hub

Task 2: Security Training 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

Main focus areas 2023 and 2024

- Threat intelligence
 - Mainstream developments are focused around threat intelligence
 - that means a SOC-integration focus for this part
 - Preventive, protective and responsive measures clustered in tools, processes and procedures, and security operations
 - Tooling and intelligence feeds in GÉANT network and in NREN networks
 - Playbook driven response processes
 - Share, Cooperate, Integrate (area of choice/input)
- Compliance
 - Strong focus in 2023 – 2025 for NIS-2 directive
 - Long term focus on compliance monitoring and auditing

Essentials

- Training
- Awareness
- Tooling
 - DDoS
 - SOCTools
 - eduVPN
 - Vulnerability
- Best practices
- Baseline
- Exercises
- Processes
- Procedures
- (managed) services

Task, subtask, activities.. WHAT IS THE PLAN!?

Task 3: Security Products and Services (Task Leader 1: Jochen Schönfelder – DFN-CERT, Task Leader 2: David Heed – SUNET)

The purpose of Task 3 is to:

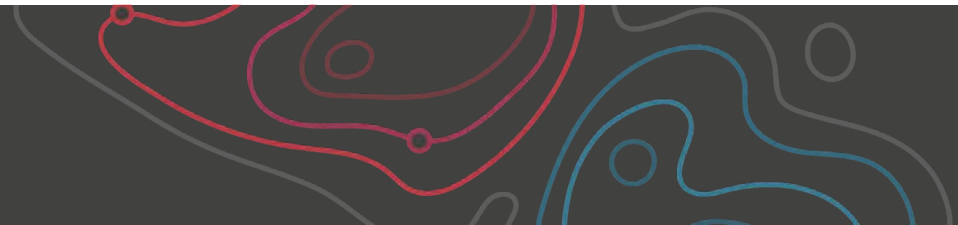
- Continue the development of GÉANT DDoS detection and mitigation (NeMo + FoD).
- Continue the support of the development and governance of eduVPN.
- Develop and implement new services for cyber threat analysis and cyber threat intelligence, building upon the results of SOCTools and Vulnerability as a Service (VaaS), with a strong emphasis on joint security operations and use of tools developed in the R&E community.
- Develop new cryptographic services as an addition to TCS, distinguish in types of certificates and investigate feasibility of a document signing service.
- Establish and maintain a joint view on the security threat landscape for research and education by analysing security intelligence, sharing analysis and translating security intelligence into actionable information.

+ we can skew priorities for tools and collaboration. More on that later...

GN5-1, WP8 TASK 3: Security products and services


The purpose of Task 3 is:

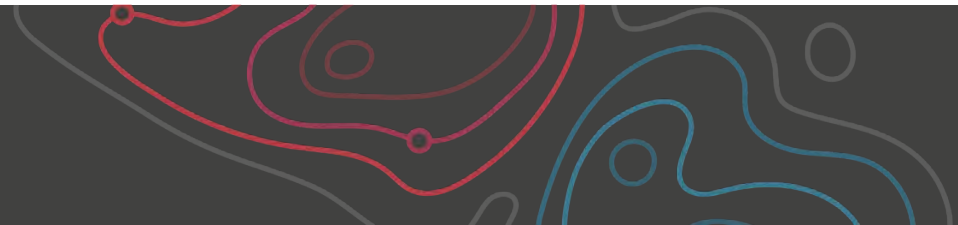
- Continue with the security products and services created in GN4-3
- Continue the support and engagement for NRENs and institutions to make use of the products and services
- Support the NRENs with sharing best practices and providing a place to interact for needed security related products and services (Security day and/or conferences)
- Create opportunities for NRENs to share data in an evolving threat landscape
- Support GÉANT's security services
 - ambition: have everything mature to a security service



Mile stones

<https://wiki.geant.org/display/GWP8/GN5-1+WP8+Milestones+and+Deliverables>

- 14 (M8.1) Workshop on Security Intelligence Operations 
- 15 (M8.2) Business Model for a European R&E Security Intelligence Hub (Whitepaper)
- 20 (M8.3) Business Model for Joint Delivery of Security Services
- 38 (M8.7) European R&E Security Conference
- 40 (M8.9) Business Model for Cryptographic Service
- 42 (M8.10) Toolset for Security Operations
- 45 (M8.12) DDoS Managed Service Offering



Firewall on Demand

Support BGP FlowSpec with IPV6

Good-bye to Python2

Improved REST-API for compatibility with NeMo

Docker ready

Support Ubuntu/Debian

14 NRENs



Firewall on Demand (ongoing work)

Foster cooperation/integration between NeMo and FoD

Early, basic visualization integration of FoD rule control into NeMo
leveraging FoD rule control API by NeMo.

Use locally running exabgp instead of using JUNOS-specific NETCONF for injecting FlowSpec rules to the routers.
This helps developers and testing. Enabling production not being restricted to JUNOS routers on the long-term.

Docker Compose was introduced as a concept to jointly run FoD container and freertr as test router."



Some users:

Countries in apps: Norway, Uganda, Pakistan, Finland, France, Sri Lanka, Morocco, Estonia, Albania

28 institutes in apps: Unit, EUR, PolSI, 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 over 130,000 unique App downloads

Example: Radboud University (NL) reported over June 2020: 3300 unique users, max 900 simultaneous users

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



125+


Servers in


26+

countries

19+

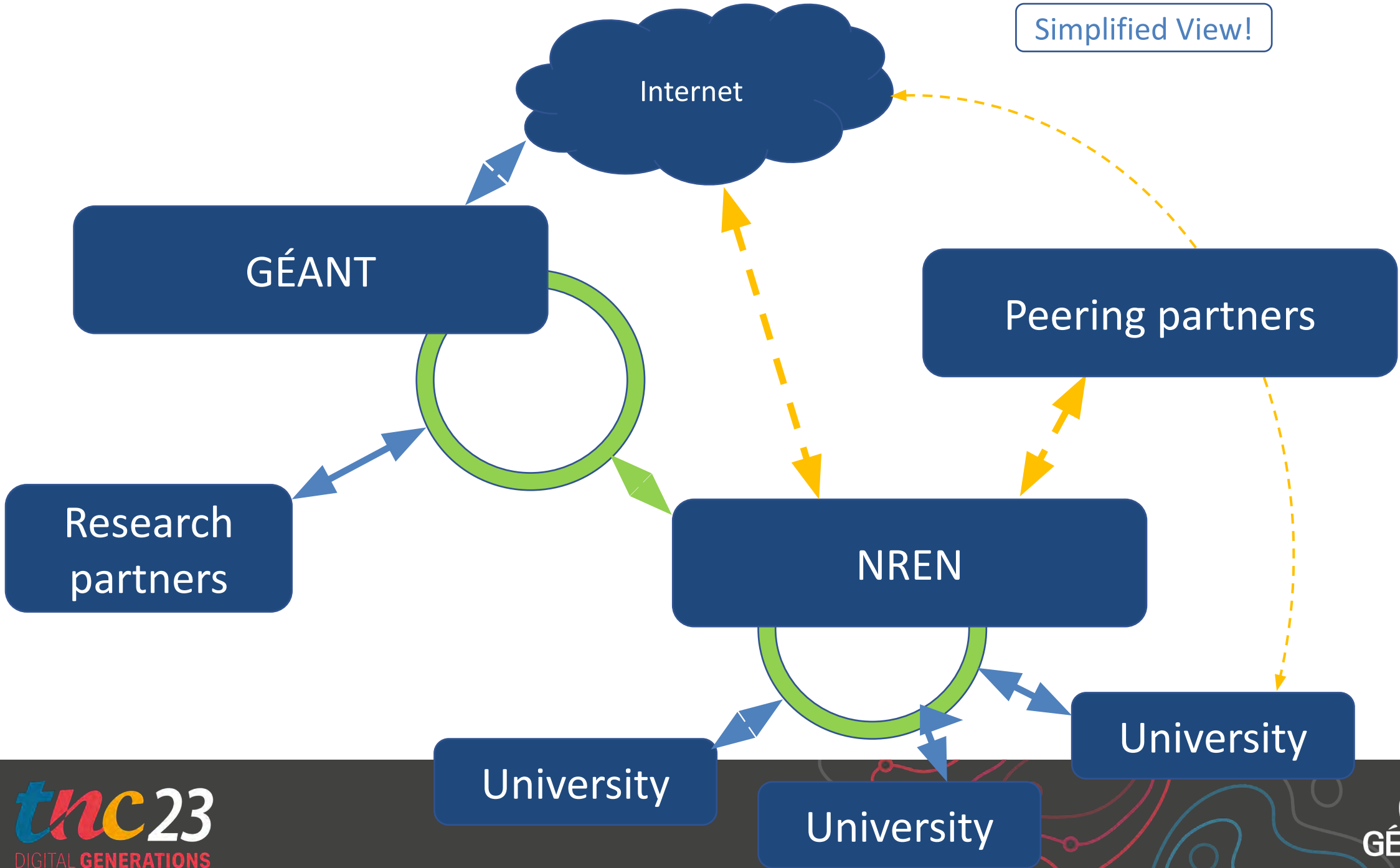
Secure internet
servers

 Institute access

 Secure internet

DDoS

Simplified View!



3 Flavors of NeMo

Protecting The Network

- NeMo detection servers: operational
- API integration with Galaxy A10: Testing
- NeMo integration with FoD: ready-to-use
- NeMo mitigation servers: Servers installed this month, ready for testing
- Training OC teams planned
- Preparing pilot migration

Protecting Your Network

- Run your own NeMo
- Install and run on your own hardware
- Protect all your uplinks
- Support model under investigation
- Available now

Managed Service

- Run NeMo in your network
- Protect all your uplinks
- Feasibility study
 - Cost
 - Service levels
 - Sourcing (who?)
 - Market
 - Distributed/solo
 - Part of GN5-1

SOCtools

Initial use-cases with common usage, ease of integration and previous local examples

- Passive/active asset discovery (aka Shodan, Censys)
- Best practices around logging. e.g. how and what should we log from Active Directory or a multitude of cloud solutions.
- IoC to block rule, e.g. solutions like RPZ, endpoint protection systems and so on. Sigma2 is in scope.
- Looking up IoCs and acting upon them, e.g. reporting phishing websites

Vulnerability assessment scanner

Procured and contract just started!

Winner was Outpost24 with Outscan.
Local, NREN and Cloud scanning available

Continued collaboration with Holm Security on feed for open source alternative

(we are fixing the eduGAIN federated logon anyday now...)

General service description

Scan both internal & internet based hosts for known vulnerabilities

Self service portal for the whole Research and Education
(but subscriptions through NRENs)

No subscription fee. Pay per scanned host per month

A host that is not scanned is not invoiced

A host that is scanned multiple times is only invoiced once

Based on the commercial Outpost24 service

Technical details

Investigate and resolve issues the tool reports.

Keep track of common vulnerabilities within IT assets of the NREN or their constituents

Create deltas between scans.

Externally facing assets are scanned from the cloud

Internally facing assets are scanned from a VM. Results go to the cloud

Export to XML, PDF or CSV

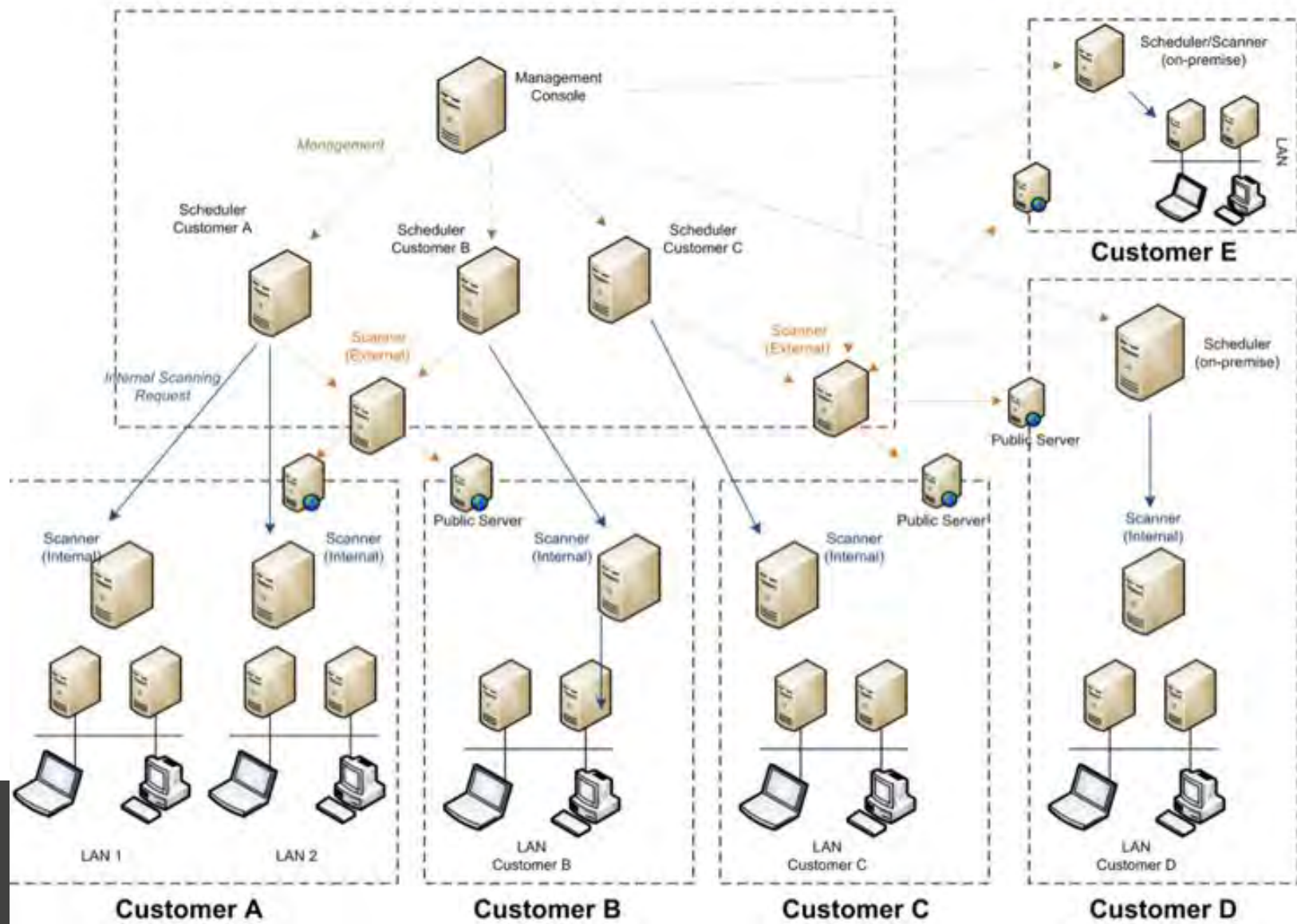
An API and some 3rd party integrations exist

Outscan - MSSP on a local level

Contract/Admin from each partner

- Delegated admin to sub-org
- Aggregated reports
- Non-invasive scanning
- Local scanning

Read more:
www.outpost24.com/about



How to subscribe

Subscriptions via NRENs through GÉANT Partner Relations
Later through Partner Portal

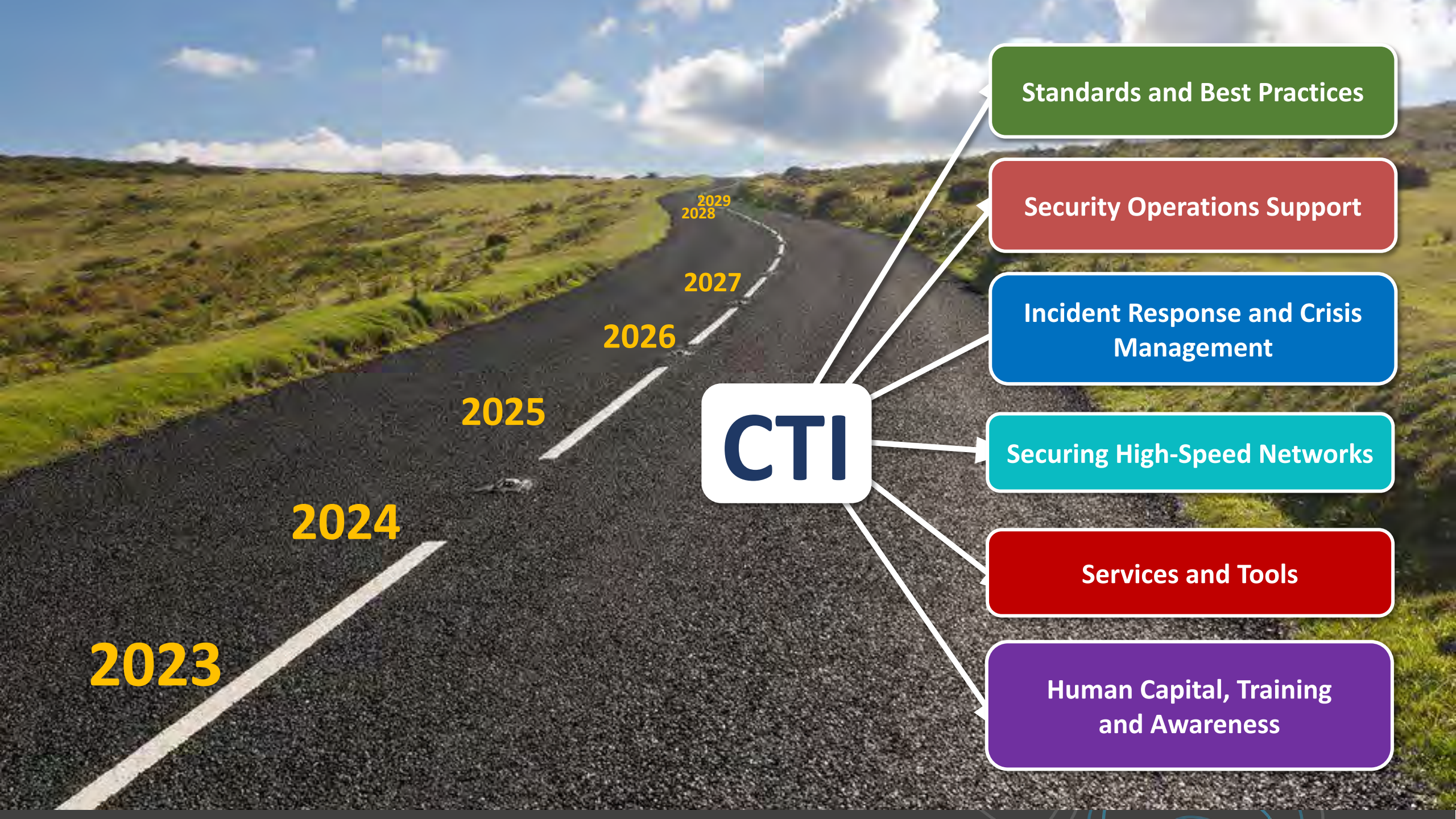
A (free) test run can be requested on a /24 block of IP addresses

Should be part of R&E within the GÉANT community

WHOIS data should be easy to match to your organisation name

Results will be sent to you in .pdf file format

Requests can be sent to: security@geant.org and partner.relations@geant.org copied in with in the subject line: “VMS trial”



2023

2024

2025

2026

2027

2028
2029

CTI

Standards and Best Practices

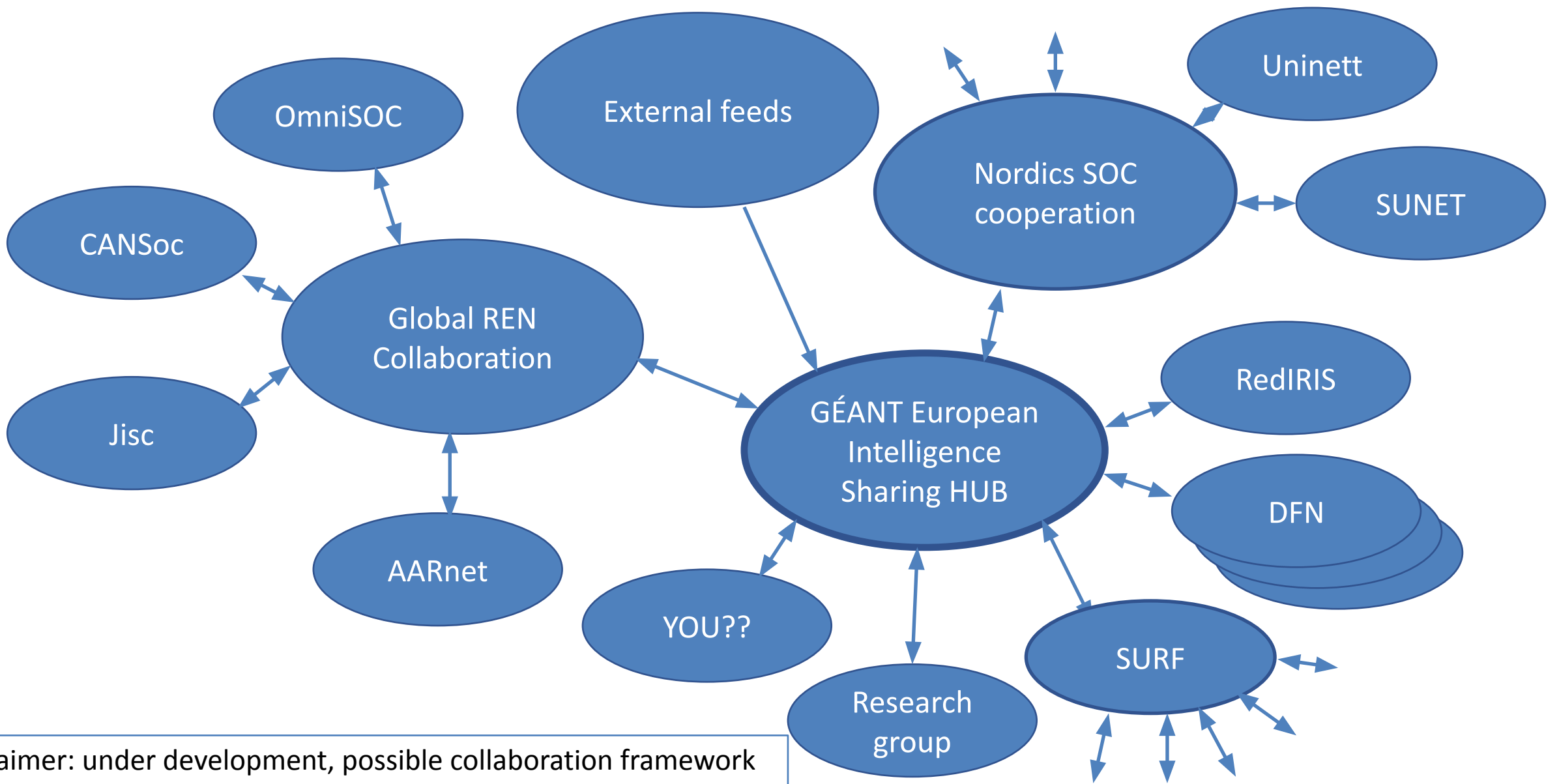
Security Operations Support

Incident Response and Crisis Management

Securing High-Speed Networks

Services and Tools

Human Capital, Training and Awareness



Sharing threat intell between organisations

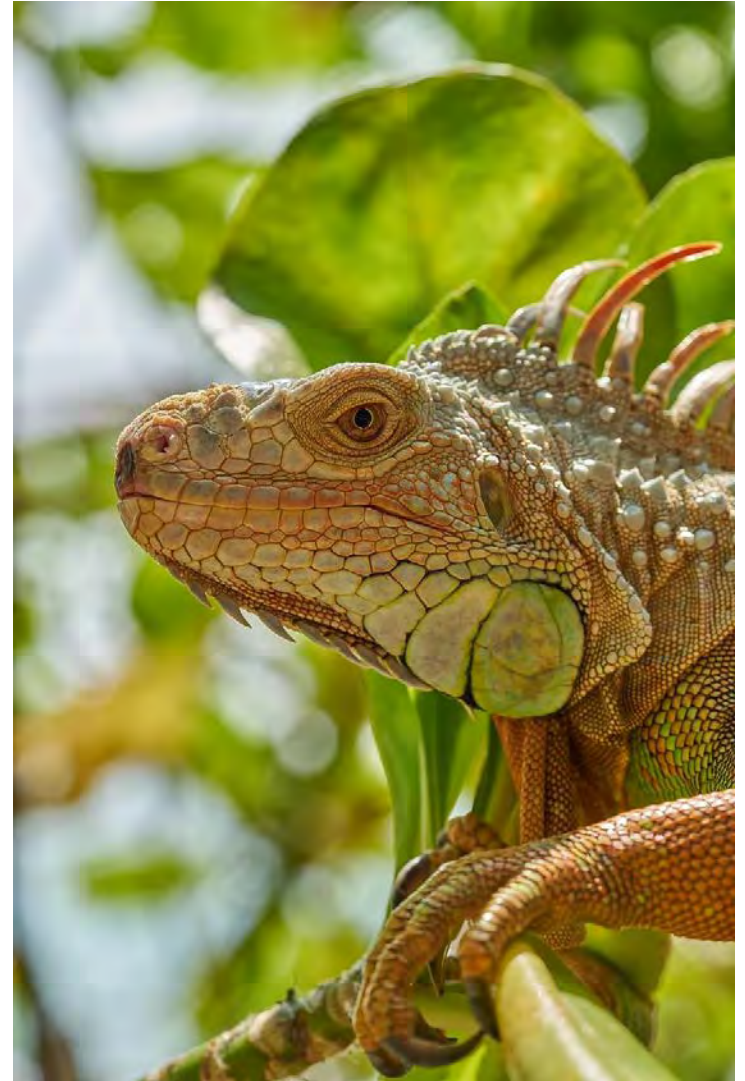
How do we get to:

- Creating, verifying and sharing CTI
- that is trusted, timely and actionable?

By:

- Collaborating
- Building communities
- Sharing operational capabilities & resources

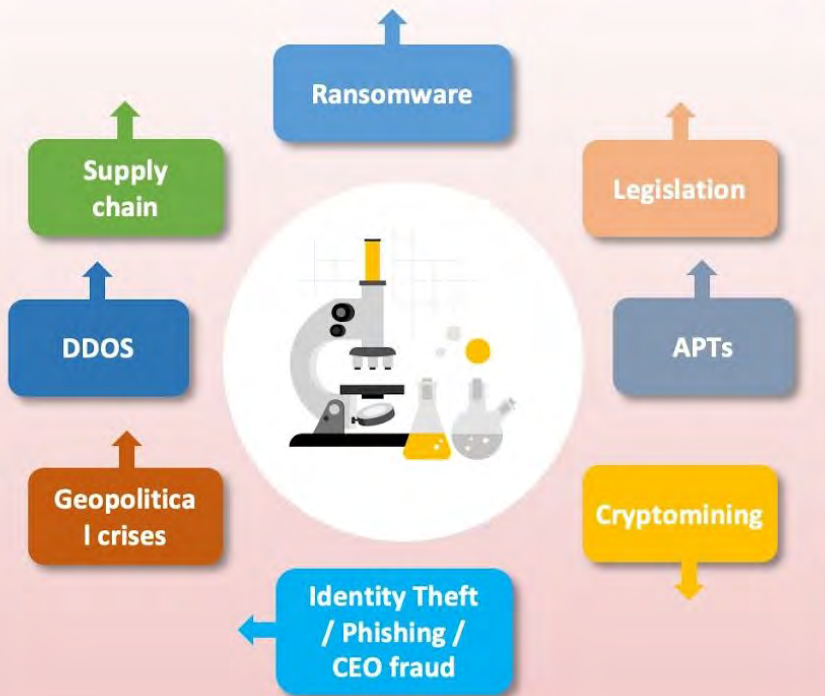
We can get ahead!



The R&E Security Intelligence Hub

From: Raw Data + Tools To: Intelligence + Information Sharing

THREATS



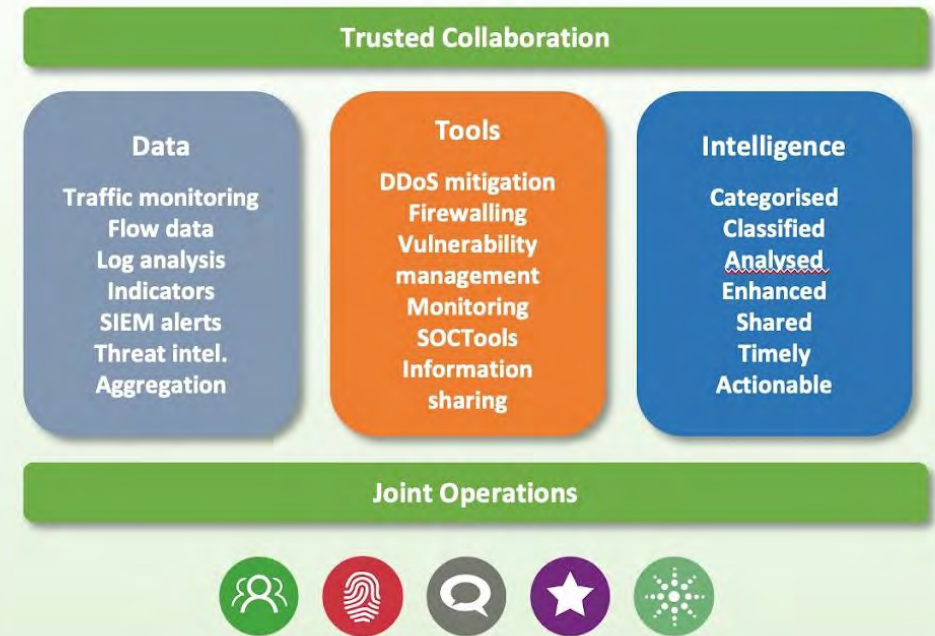
+

CHALLENGES

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

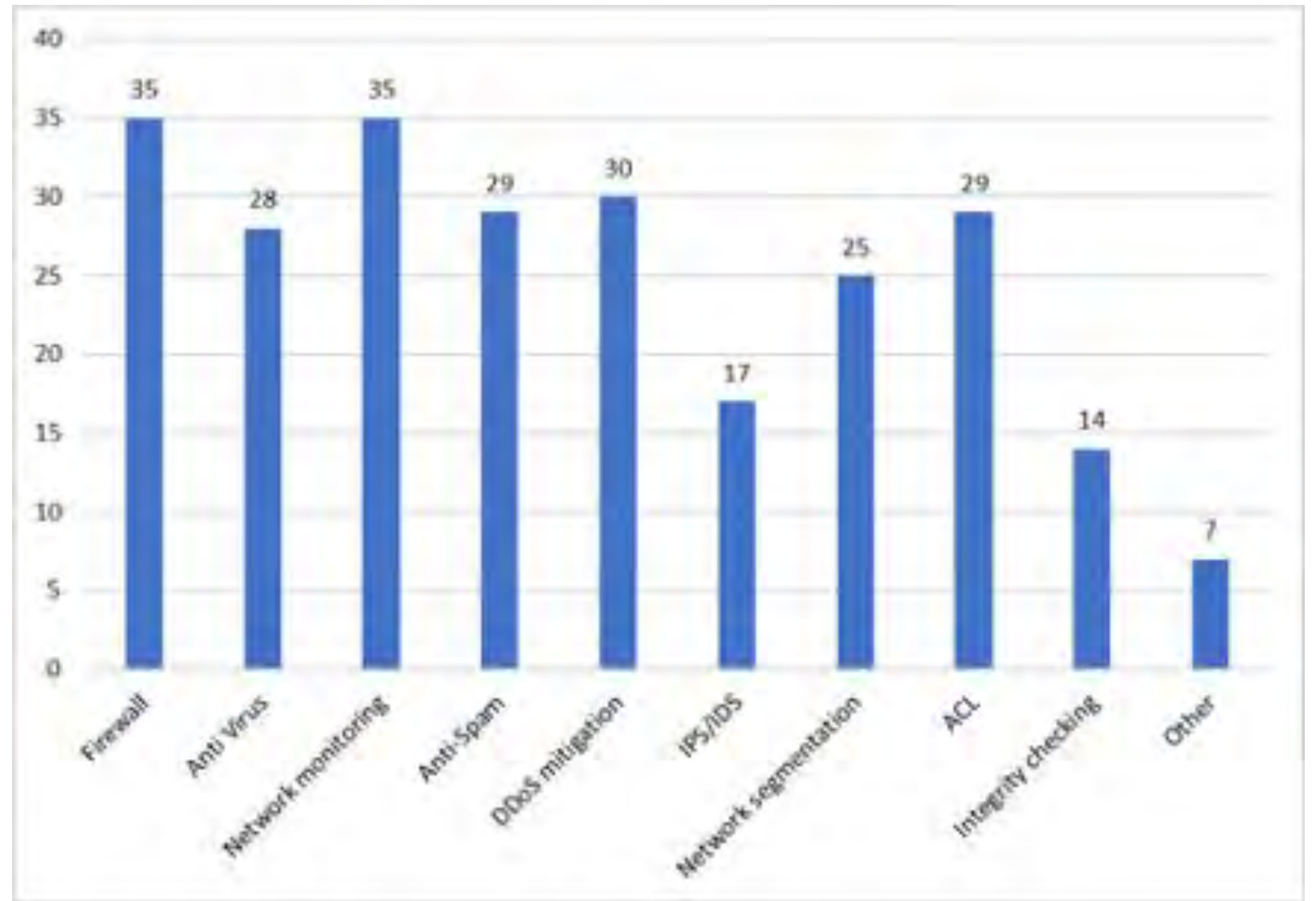
>

SOLUTIONS



- MISP as de-facto standard tool for (most) information sharing
 - Especially IOCs + meta-data
 - Collect, Curate, Verify, Analyse, Tag + Share
 - TTPs?
- Identify and evaluate potential feeds; make these accessible and useful/actionable
- Complement / supplement quality feeds with ***our own data, analyses + intel.***
 - Information Sharing Agreements
- Explore means to correlate IOCs with network traffic / flow data / logs / DNS, etc.
- Profiles for threat actors specifically targeting R&E?

Generic tools used by NRENs



Getting your input!?!?

We are agile enough to focus on quick wins for the community* . Be it organising a workshop or perhaps doing integration for a commonly used tool.

Here is your chance to give us some direct feedback on the project !!!

**we will release most/all as open-source*

INPUT GATHERING

RESULTS WILL BE SHARED ON THE PROJECT WIKI OR AT NEXT OCCURANCE

PARTICIPATE?

GÉANT Innovation
Programme

Products and services:
eduVPN
Firewall on demand

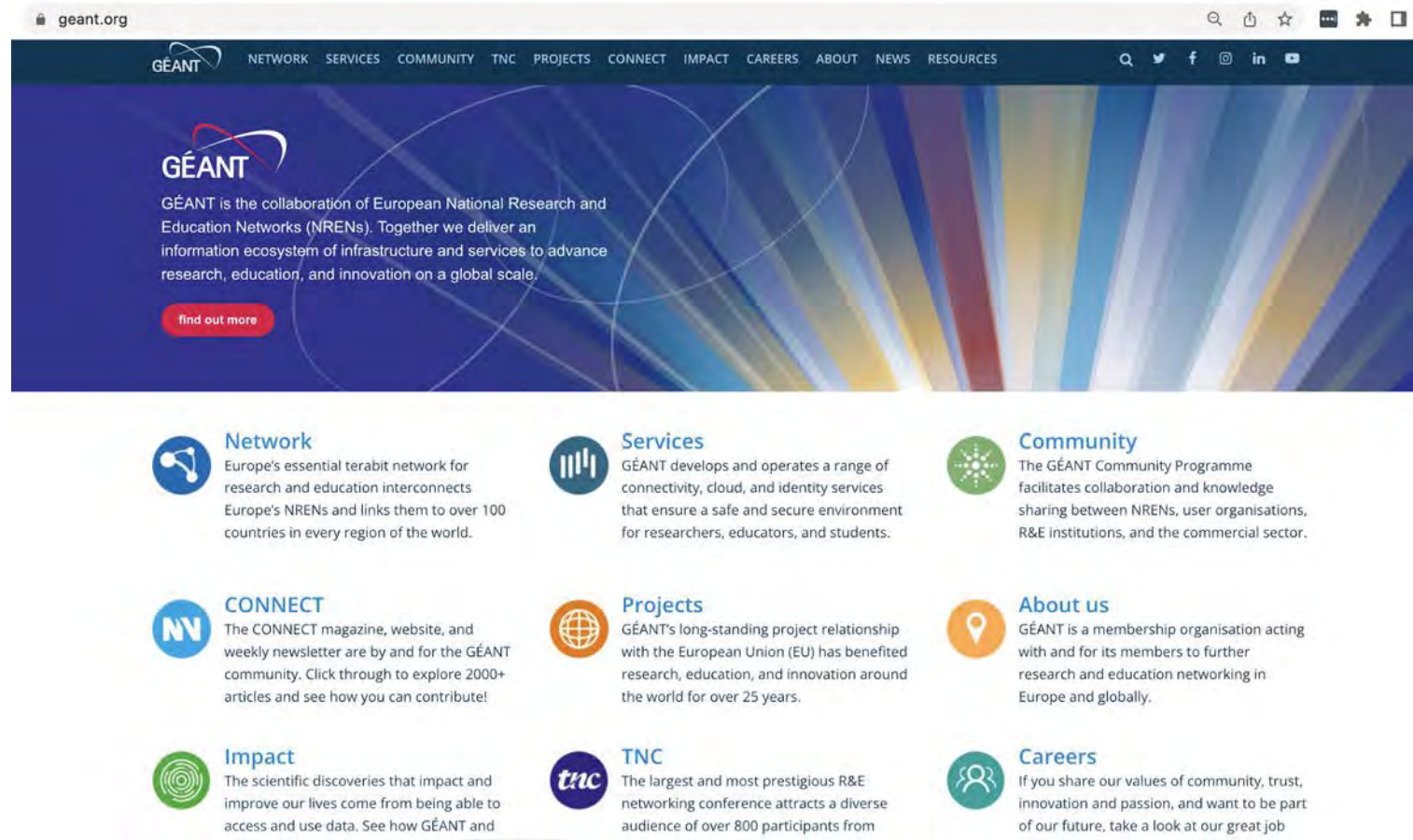
Best practices:
Business continuity
Crisis management

Crisis exercises:

Security Training

Security Awareness

Trusted Certificate Service



tnc23

DIGITAL GENERATIONS

TIRANA, ALBANIA | 5-9 JUNE 2023

Thank you

room for questions and discussion...!

david@sUNET.se



Co-funded by
the European Union

