WP8 T4 CTI (Cyber Threat Intelligence)

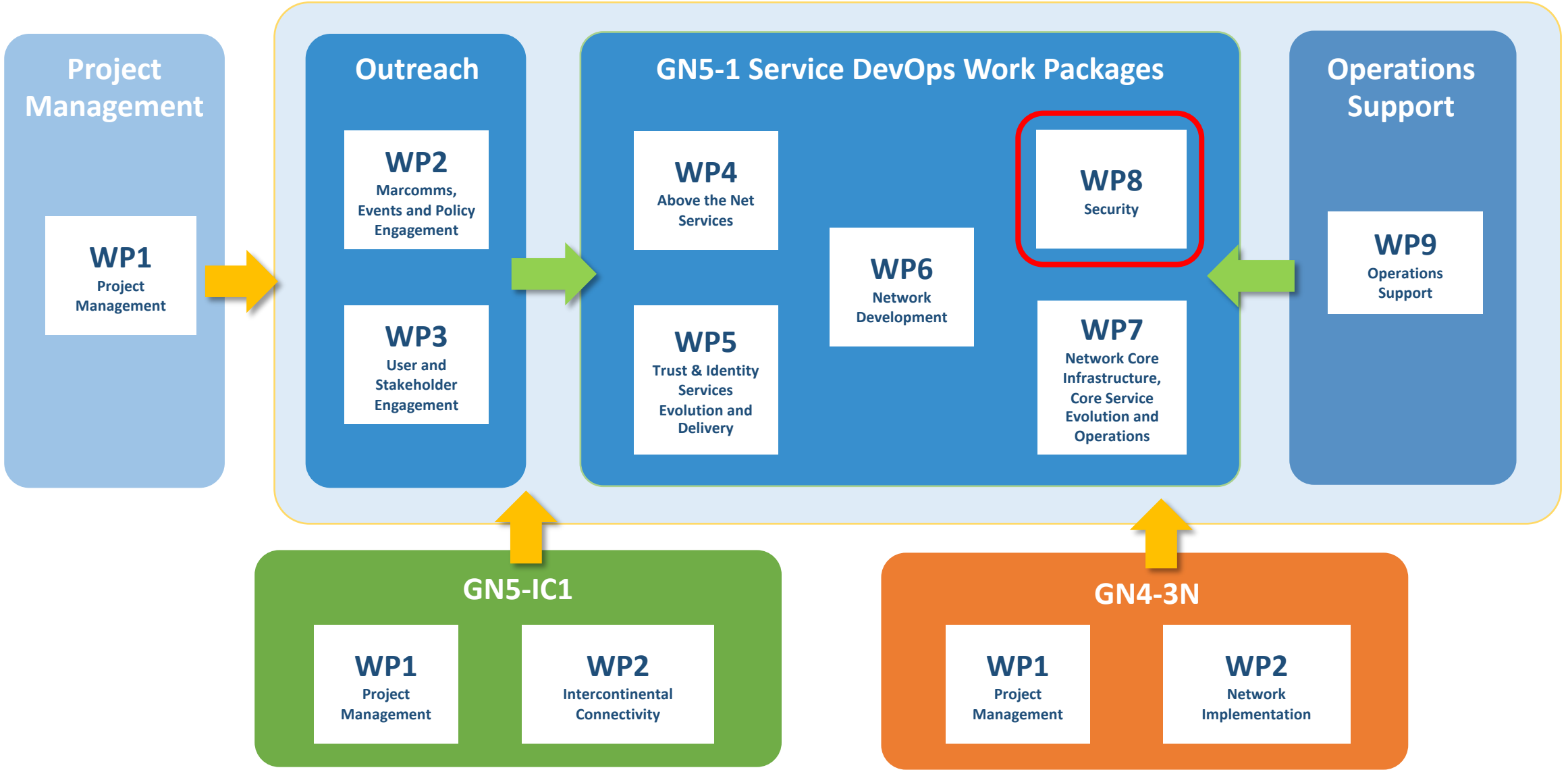
Summary

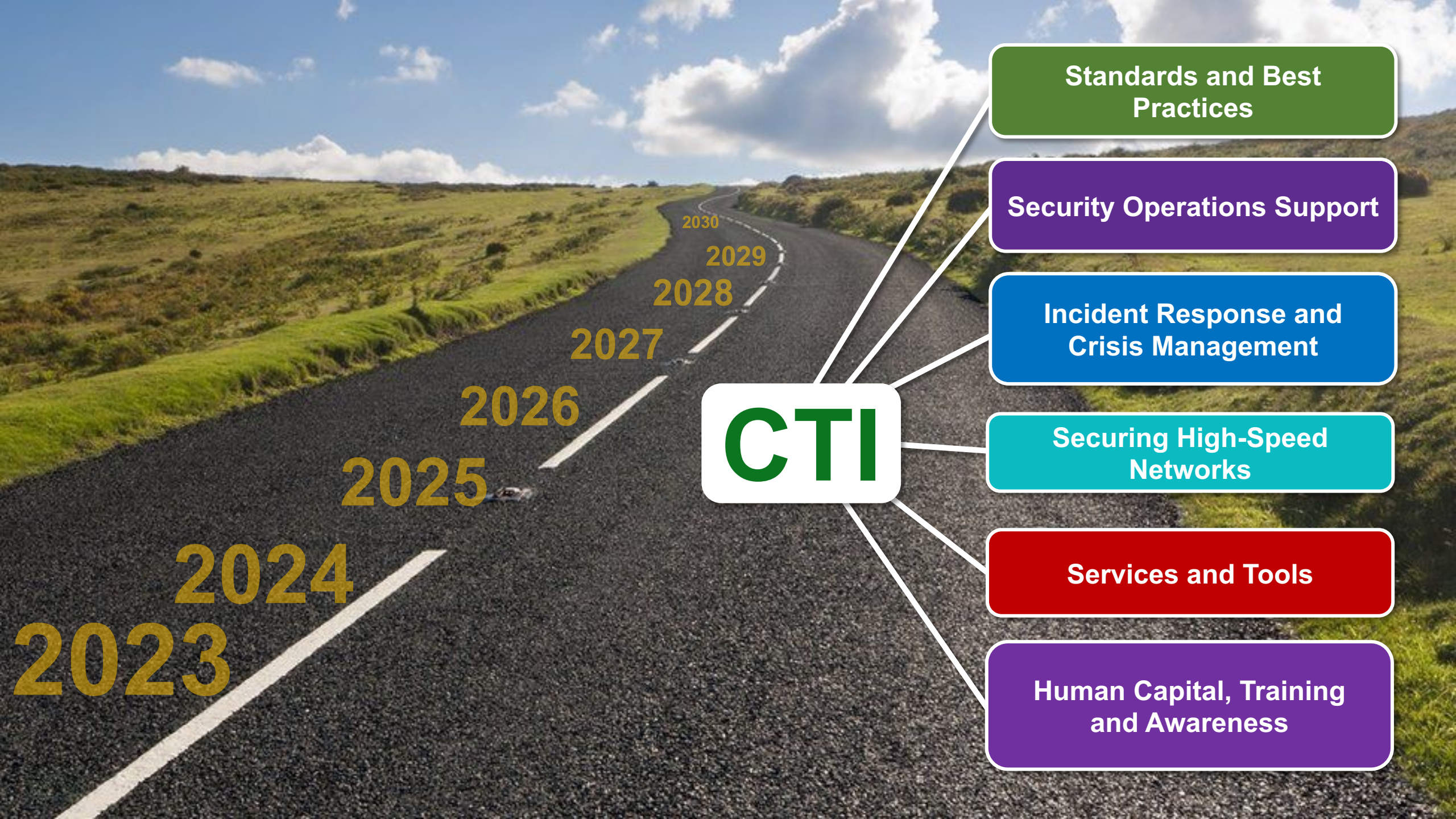
Roderick Mooi
T4 Task Lead

09 October 2024

SIG-ISM

GN5 Project Work Package elements




2030
2029
2028
2027
2026
2025
2024
2023
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

GN5-1 CTI 2023(-2024) journey

- In-person meetings at SURF Utrecht in May 2023, Security Days Prague April 2024 + next planned for Nov 2024
- Virtual meeting fortnightly to share experiences
- Delivered: Business model for R&E Security Intelligence Hub
- Identified MISP as de-facto tool for (most) information sharing
  - Especially IOCs + meta-data

R&E Security Intelligence Hub: The Concept

- ISAC-like virtual organisation
- Data + expertise
- Threat analysis
- Aggregation + correlation
- Communications coordination
- Trend reporting
- Uniting the R&E community!

https://resources.geant.org/project-output/gn5-1-milestones/ →

M8.2 Business Model for a European R&E Security Intelligence Hub

Published date | **27 October 2023**

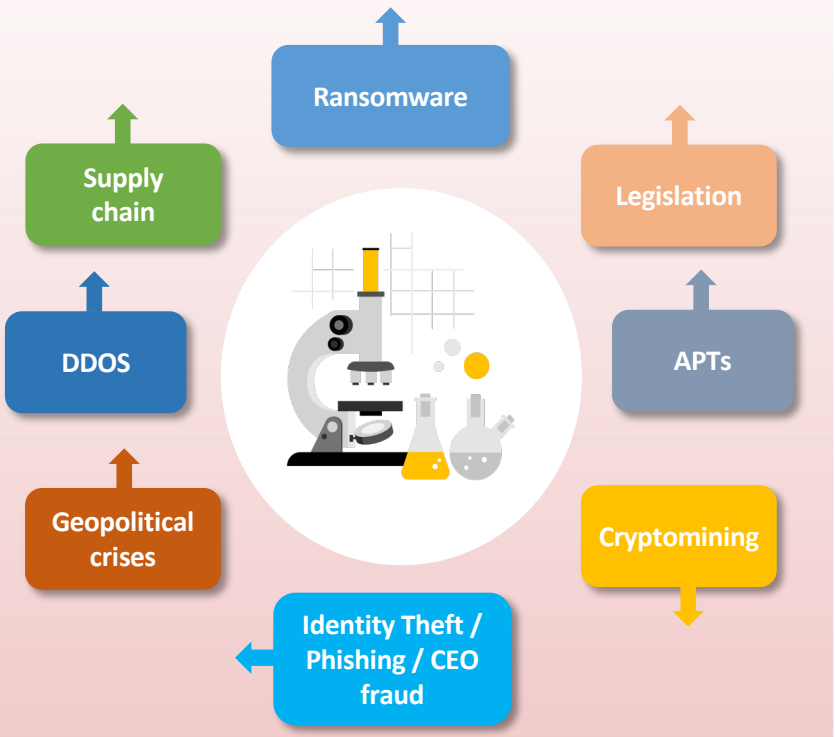
This white paper presents the business model of a Research and Education Security Intelligence Hub – a virtual organisation that seeks to create, collect, analyse, classify, and share actionable security intelligence for research and education. It highlights the key outcomes of a Business Model Canvas workshop, SWOT analysis and indicative information-sharing agreements, providing guidance for the next steps required towards establishing the Hub.

PDF

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

Trusted Collaboration

Data	Tools	Intelligence
Traffic monitoring Flow data Log analysis Indicators SIEM alerts Threat intel. Aggregation	DDoS mitigation Firewalling Vulnerability management Monitoring SOCTools Information sharing	Categorised Classified Analysed Enhanced Shared Timely Actionable

Joint Operations

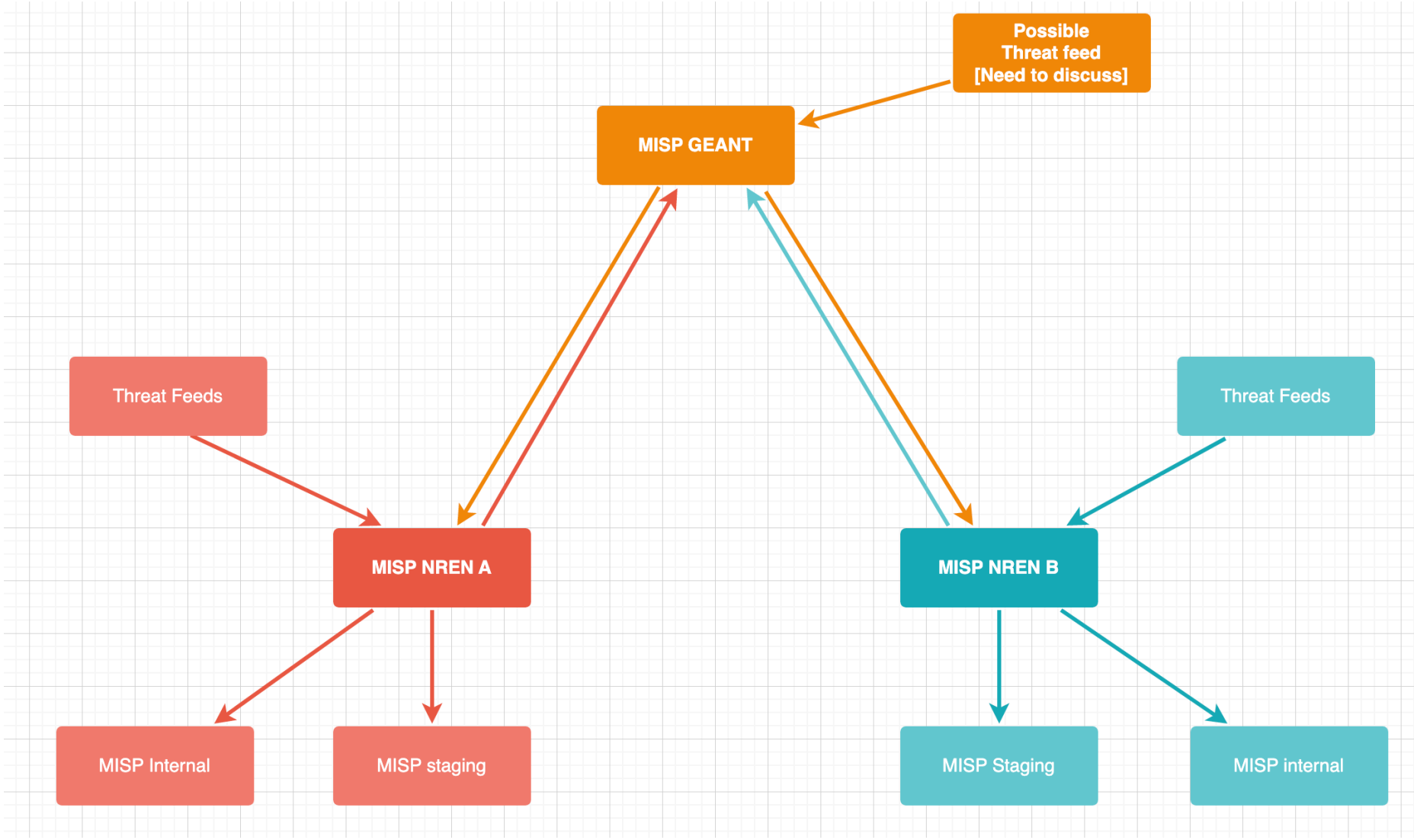
Value Propositions

- **Sharing** the **workload**
  - (reduce duplication of effort)
- Addressing **common challenges**
  - Together!
- **Distributing resources**

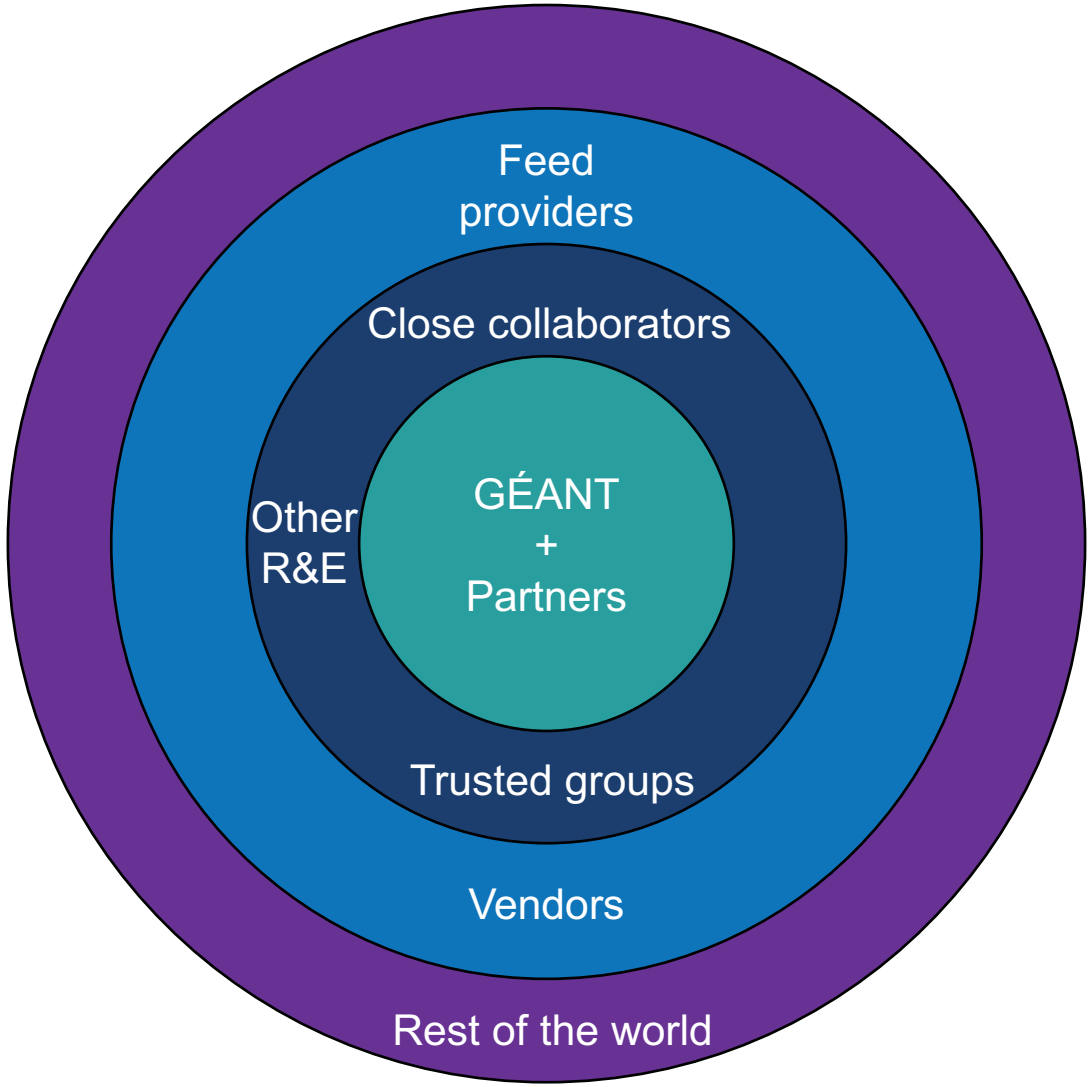
→ improved view of the R&E threat landscape

- Verified (and therefore **actionable) data** – e.g. IOCs
- Creating **intel specifically for / relevant to R&E** – e.g. threat actor reports
- **Sharing consumed intel** within our own networks and constituencies
- **Central contact point** for R&E CTI
- **Trends and statistics** – e.g. Portal/dashboard(s) showing key intel and metrics for customers
- **CTI-related tooling blueprint** (optimised architecture and implementation)
- **Early(ier) warnings** of possible compromise, vulnerabilities, etc.

R&E Hub: MISP Setup



Information Sharing Agreements: Circles of Trust



Information Sharing Agreements

Level	Trust Group	Sharing agreement(s)
1	GÉANT + Partners	Code of conduct + existing GN project contracts
2	Trusted groups Close collaborators Other R&E	MoU / NDA (depending on the parties involved)
3	Vendors Feed providers	Subscriber agreement (or equivalent contract)
4	Rest of the world	N/A. Probably only TLP:CLEAR and GREEN (i.e. non-sensitive) information

GN5-1 CTI (2023-)2024 journey

- Exploring means to correlate IOCs with network traffic / flow data / logs / DNS, etc.
- 4 NRENs sharing + 4 more joining in 2025
- <details redacted>

GN5-2 CTI Task Objectives

- Implement the R&E Security Intelligence Hub
- KPI: 4 organisations participating in joint security intelligence operations in 2025 and 6 in 2026
- Procure and provide selected intelligence feeds for distribution
- 2 Milestones:
  M13/8.2 Quarterly Trend Reports R&E Threat Landscape (M8)
  M36/8.9 Six NRENs actively participating in R&E security intelligence hub / intelligence sharing (M20)

Key Activities

- Feed evaluation, (procurement,) configuration and sharing
- Information sharing infrastructure (MISP, etc.) + integrations
- Threat intelligence + trend reports

Thank You

Any questions?

www.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).