Security
.Days

<Prague.CZ>
<9-11 April 2024>

GÉANT

The R&E Security Intelligence Hub

Roderick Mooi - GÉANT

Co-funded by
the European Union

TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030

(Revised)

1
Supply chain compromise of software dependencies
2
Advanced disinformation campaigns
3
Rise of digital surveillance authoritarianism/ loss of privacy
4
Human error and exploited legacy systems within cyber-physical ecosystems
5
Targeted attacks enhanced by smart device data
6
Lack of analysis and control of space-based infrastructure and objects
7
Rise of advanced hybrid threats
8
Skill shortage
9
Cross-border ICT service providers as a single point of failure
10
Artificial Intelligence Abuse
THREATS 2030

1. **Supply Chain Compromise of Software Dependencies**
2. **Skill Shortage**
3. **Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems**
4. **Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [New in Top Ten]**
5. **Rise of Digital Surveillance Authoritarianism / Loss of Privacy**
6. **Cross-border ICT Service Providers as a Single Point of Failure**
7. **Advanced Disinformation / Influence Operations (IO) Campaigns**
8. **Rise of Advanced Hybrid Threats**
9. **Abuse of AI**
10. **Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [New in Top Ten]**

R&E Impact (1)

Digital Dependencies

- Growing reliance on technology
- Interconnected vulnerabilities

Ransomware & Email Threats

- More advanced, aggressive and persistent

Cloud Exploitation

- Cloud-conscious adversaries
- Identity vulnerabilities

Human Factor

- Shortage in skills and resources
- Competitors on the job market
- Human weakness exploitation

R&E Impact (2)

Network Threats

- Increasing DDoS attacks
- Threats on infrastructure (subsea cables)

Artificial Intelligence

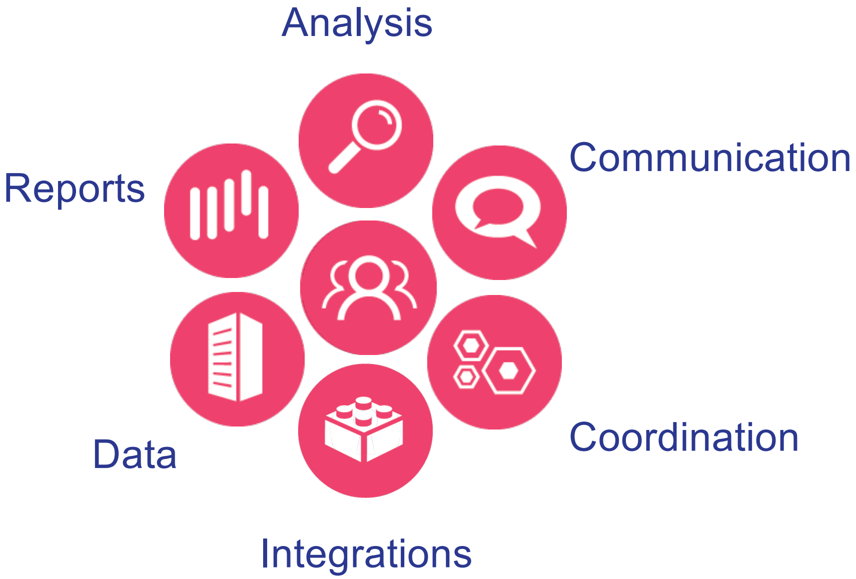
- AI-powered threats
- AI for improved cybersecurity

Legislation & Compliance

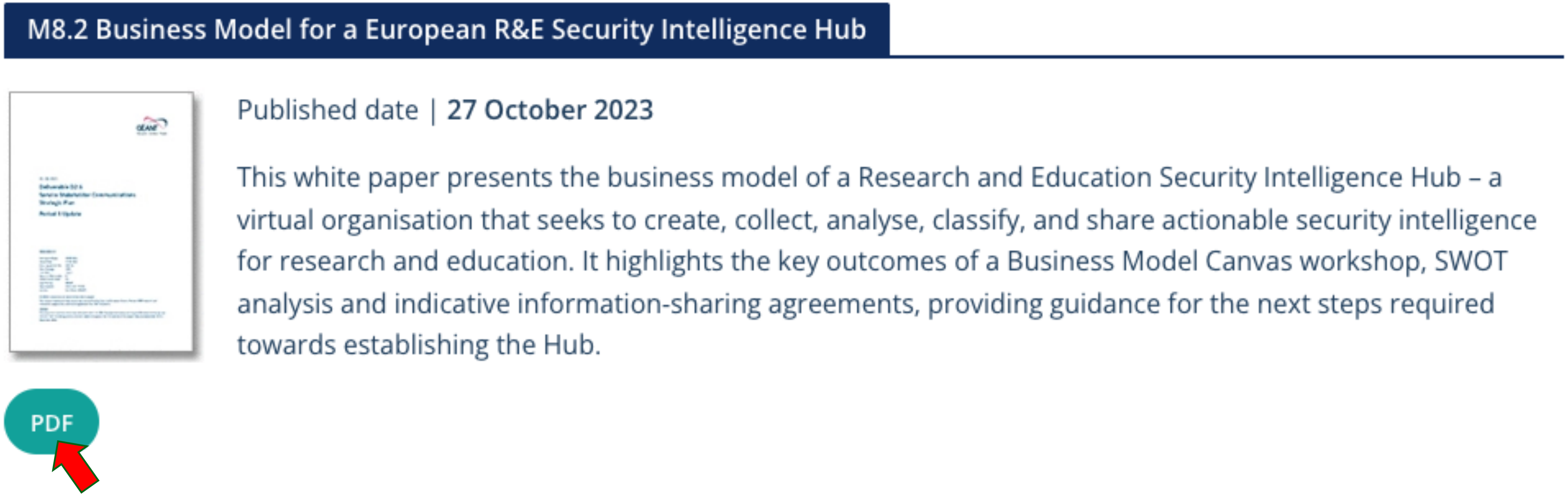
- NIS2 challenges & implications for NRENs
- Global reach of GDPR

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!



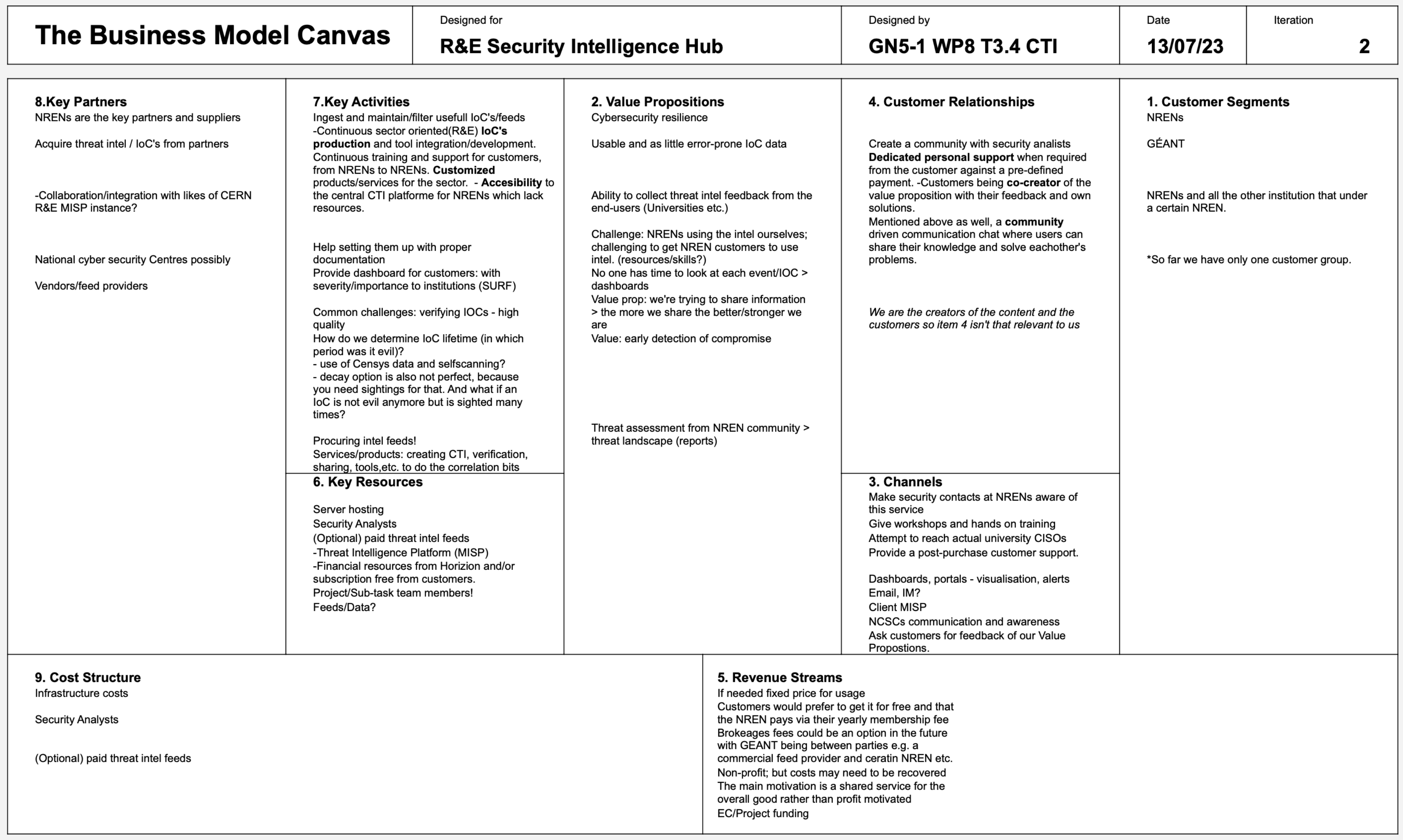
https://resources.geant.org/project-output/gn5-1-milestones/ →



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.



The Business Model Canvas

Designed for
R&E Security Intelligence Hub

Designed by
GN5-1 WP8 T3.4 CTI

Date
13/07/23

Iteration
2

8.Key Partners

NRENs are the key partners and suppliers

Acquire threat intel / IoC's from partners

-Collaboration/integration with likes of CERN R&E MISP instance?

National cyber security Centres possibly

Vendors/feed providers

7.Key Activities

Ingest and maintain/filter usefull IoC's/feeds
-Continuous sector oriented(R&E) **IoC's production** and tool integration/development.
Continuous training and support for customers, from NRENs to NRENs. **Customized** products/services for the sector. - **Accesibility** to the central CTI platforme for NRENs which lack resources.

Help setting them up with proper documentation
Provide dashboard for customers: with severity/importance to institutions (SURF)

Common challenges: verifying IOCs - high quality
How do we determine IoC lifetime (in which period was it evil)?
- use of Censys data and selfscanning?
- decay option is also not perfect, because you need sightings for that. And what if an IoC is not evil anymore but is sighted many times?

Procuring intel feeds!
Services/products: creating CTI, verification, sharing, tools,etc. to do the correlation bits

6. Key Resources

Server hosting
Security Analysts
(Optional) paid threat intel feeds
-Threat Intelligence Platform (MISP)
-Financial resources from Horizion and/or subscription free from customers.
Project/Sub-task team members!
Feeds/Data?

2. Value Propositions

Cybersecurity resilience

Usable and as little error-prone IoC data

Ability to collect threat intel feedback from the end-users (Universities etc.)

Challenge: NRENs using the intel ourselves; challenging to get NREN customers to use intel. (resources/skills?)
No one has time to look at each event/IOC > dashboards
Value prop: we're trying to share information > the more we share the better/stronger we are
Value: early detection of compromise

Threat assessment from NREN community > threat landscape (reports)

4. Customer Relationships

Create a community with security analists
Dedicated personal support when required from the customer against a pre-defined payment. -Customers being **co-creator** of the value proposition with their feedback and own solutions.
Mentioned above as well, a **community** driven communication chat where users can share their knowledge and solve eachother's problems.

We are the creators of the content and the customers so item 4 isn't that relevant to us

3. Channels

Make security contacts at NRENs aware of this service
Give workshops and hands on training
Attempt to reach actual university CISOs
Provide a post-purchase customer support.

Dashboards, portals - visualisation, alerts
Email, IM?
Client MISP
NCSCs communication and awareness
Ask customers for feedback of our Value Propostions.

1. Customer Segments

NRENs

GÉANT

NRENs and all the other institution that under a certain NREN.

*So far we have only one customer group.

9. Cost Structure

Infrastructure costs

Security Analysts

(Optional) paid threat intel feeds

5. Revenue Streams

If needed fixed price for usage
Customers would prefer to get it for free and that the NREN pays via their yearly membership fee
Brokeages fees could be an option in the future with GEANT being between parties e.g. a commercial feed provider and ceratin NREN etc.
Non-profit; but costs may need to be recovered
The main motivation is a shared service for the overall good rather than profit motivated
EC/Project funding

Ref: https://www.strategyzer.com/library/the-business-model-canvas

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.

Channels (communication)

For (near)real-time sharing of CTI:

- Security teams
  - Portal/dashboards
  - IM
  - Tool Sync (e.g. MISP events)
- With other national teams (e.g. NCSCs)
  - Various, predominantly sharing feeds/events

Channels (communication)

For Hub developments, trends, information sharing, etc.:

- Project team(s), Infoshares, STFs, SIGs, etc.
- NREN engagement forums:
  - Events – workshops, training events, conferences
  - GÉANT CTO workshops
  - Individual engagements
  - Email (incl. mailing lists)

Customer Relationships

The Hub can act as **coordinator** for an *information sharing community*, establishing (and maintaining) R&E CTI- related SIGs/working groups, expert groups, discussion forums (chat platform, mailing lists), conferences/symposia, training events, etc.

Existing GÉANT-NREN-NREN customer relationships can be reutilised by the Hub.

Specific channels, communities, interest/working groups can be established as needed.

Key Partners

- Stakeholders: GÉANT, European NRENs
- Other global NRENs (or related communities – e.g. REN-ISAC)
- National CERTs/ISACs/NCSCs.
- “Sharing” partners:
  - FIRST, TF-CSIRT and similar communities
  - Academic/research orgs. aside from NRENs – e.g. specific universities, CERN, etc.
- Vendors:
  - Tool developers – e.g. CIRCL (MISP)
  - Feed providers
- European Commission (project funding)
- Possibly ENISA / similar bodies.

Costs

- Staff – analysts, engineers, researchers, etc.
- Hosting infrastructure
- Commercial feeds (if/as applicable)
- Commercial tooling (if/as applicable)

Revenue Streams

- Initially: EC via GN5-FPA
- Possible future/complementary options:
  - Subscription/membership fees
  - Paid-for threat intel feeds

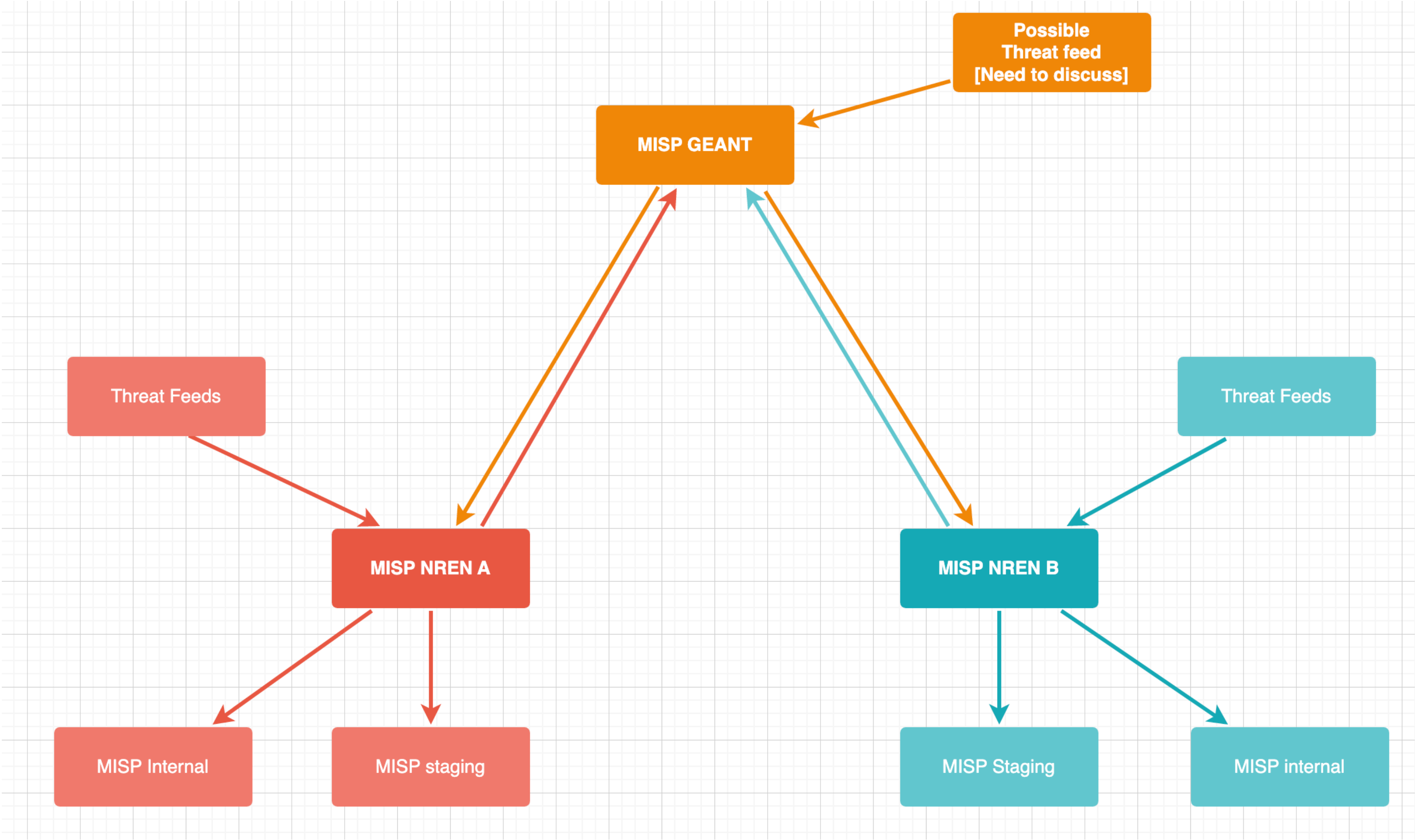
Shared resouces?

- Core team in GÉANT (supported by operational budget)
- Distributed NREN team members

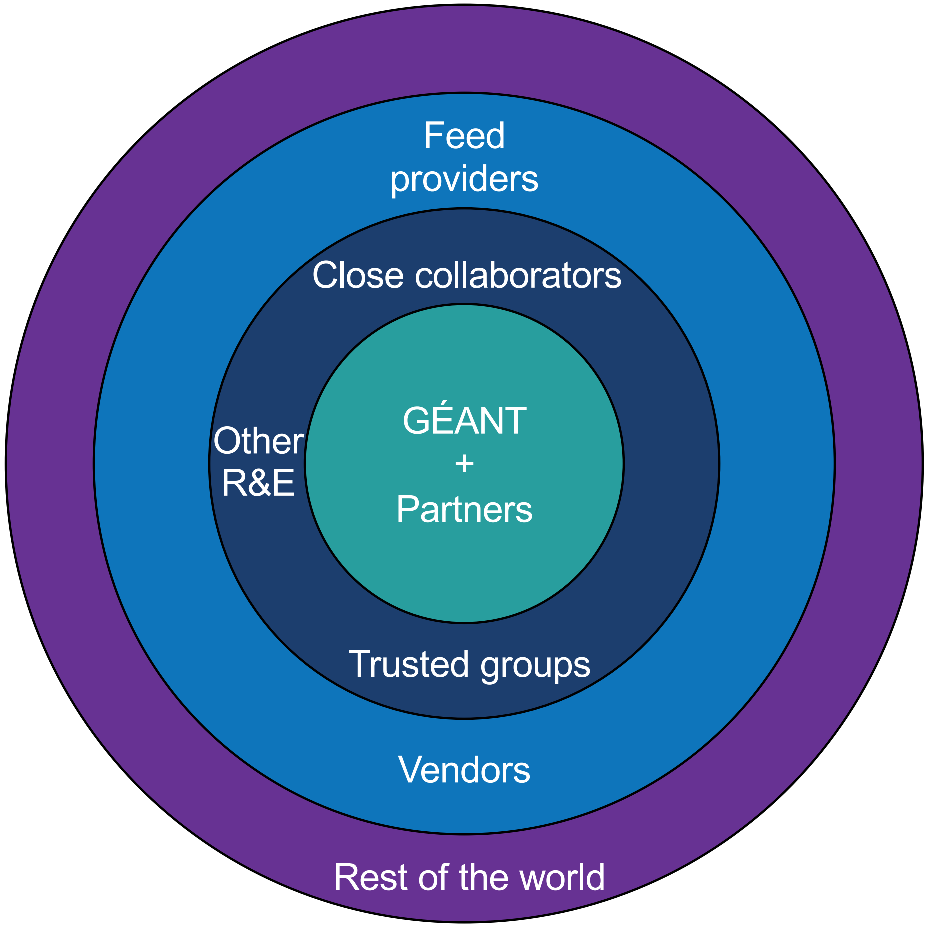
2023-2024 journey so far (activities)

- Identified MISP as de-facto tool for (most) information sharing
  - Especially IOCs + meta-data
- Exploring means to correlate IOCs with network traffic / flow data / logs / DNS, etc.
- Meeting fortnightly to share experiences; held an in-person meeting at SURF Utrecht on 15 May 2023 (next planned for Sep 2024)
- Information Sharing Agreements study
- Delivered: *Business model for R&E Security Intelligence Hub*

R&E Hub: MISP Setup



Information Sharing Agreements: Circles of Trust



Feed providers

Close collaborators

Other R&E

GÉANT + Partners

Trusted groups

Vendors

Rest of the world

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

2024 (remaining)

- Sync events between GÉANT and NREN MISP instances
- Setup feeds of NREN generated threat data
- Commence feed evaluation
- Continue with individual matching, alerting, dashboards, etc.
- Share experiences!

R&E Security Intelligence Hub

Benefits:

- Shared expertise
- Distributed resources
- Effort deduplication
- Actionable intelligence
- Sector-level perpective
- Increased trust

BY: R&E
4: R&E
☺

GN5-2 WP8 T4 CTI

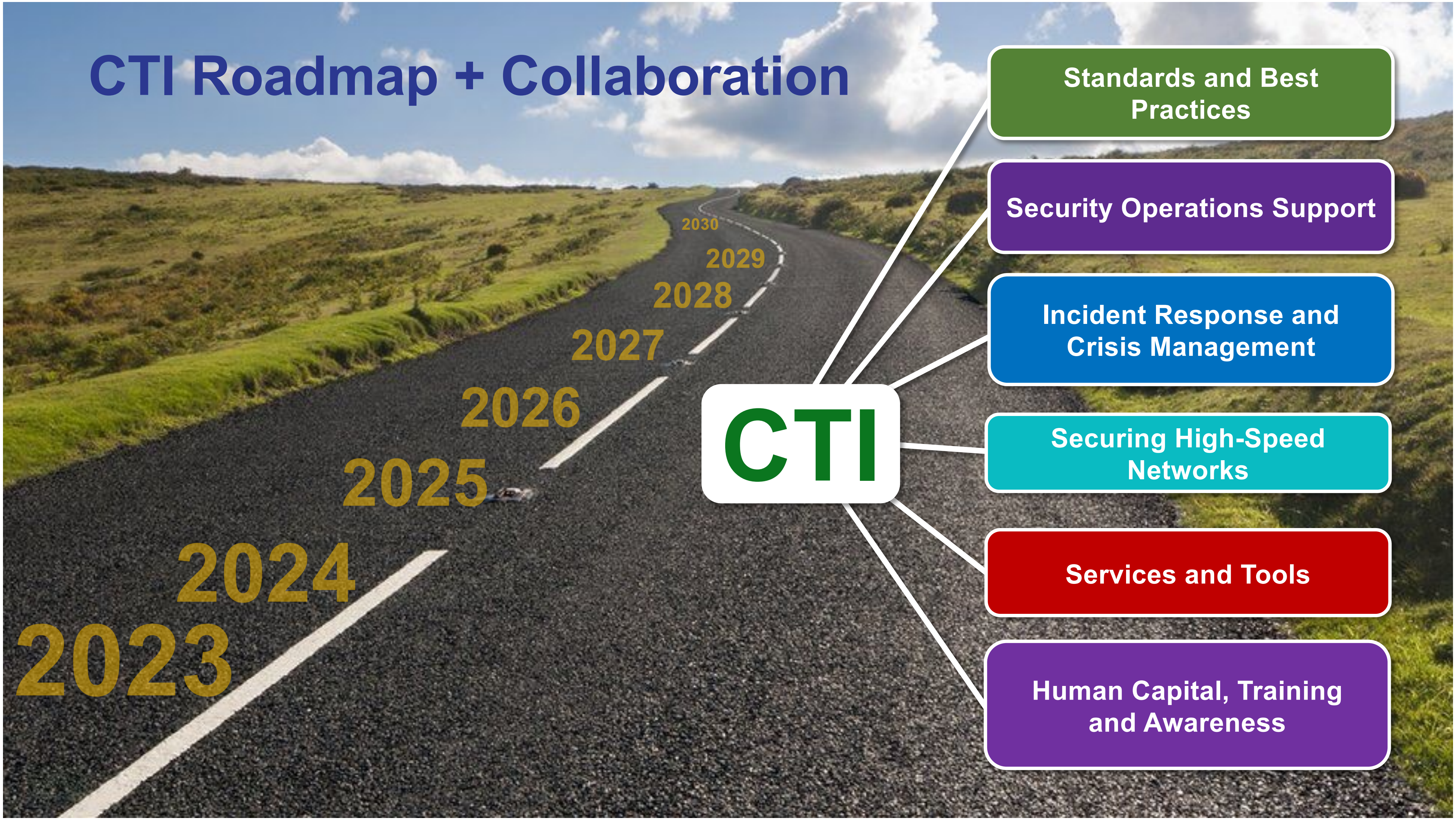
Objectives:

- Improve visibility of threats, particularly those facing our sector
- Collectively share experiences in dealing with these threats
- Enhance detection and response actions accordingly

Aims:

- Deliver selected intelligence feeds
- Share intelligence between participating (N)RENs
- Reporting on the threat landscape

CTI Roadmap + Collaboration

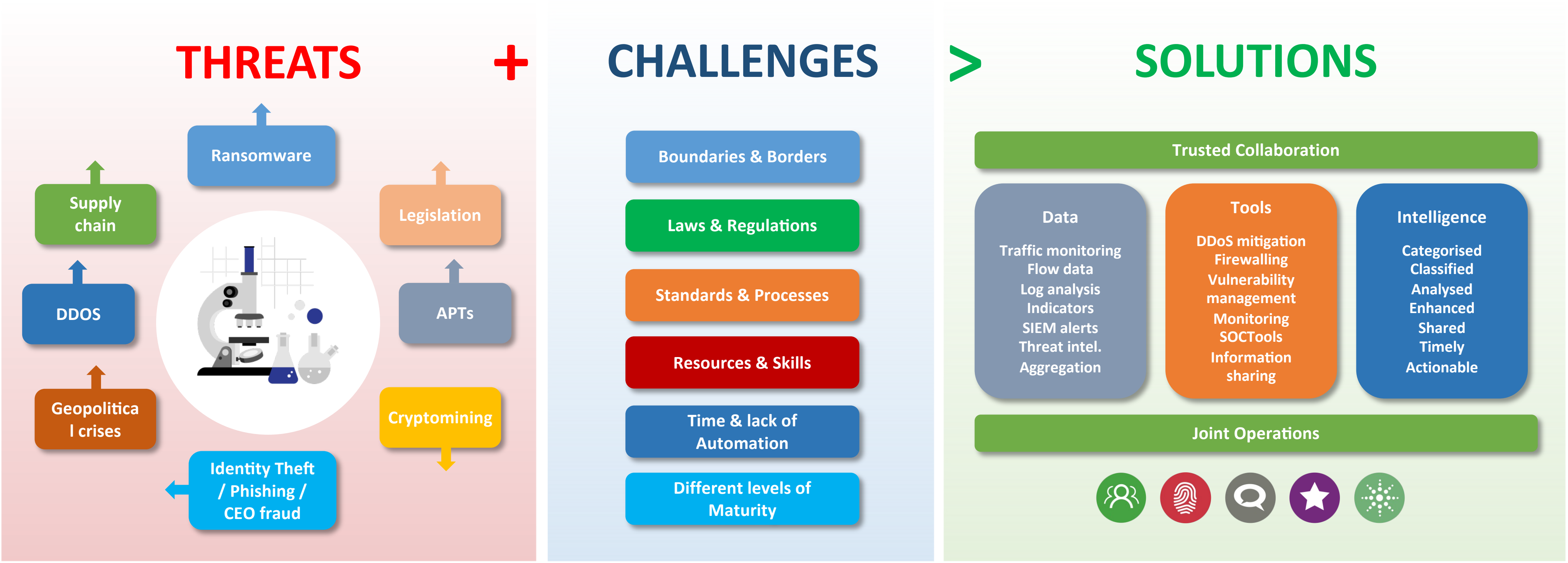


CTI

- Standards and Best Practices
- Security Operations Support
- Incident Response and Crisis Management
- Securing High-Speed Networks
- Services and Tools
- Human Capital, Training and Awareness

The R&E Security Intelligence Hub

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



THREATS +

Ransomware

Supply chain

Legislation

DDOS

APTs

Geopolitical crises

Cryptomining

Identity Theft / Phishing / CEO fraud

CHALLENGES >

Boundaries & Borders

Laws & Regulations

Standards & Processes

Resources & Skills

Time & lack of Automation

Different levels of Maturity

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

GÉANT

Thank you!

Questions/comments?

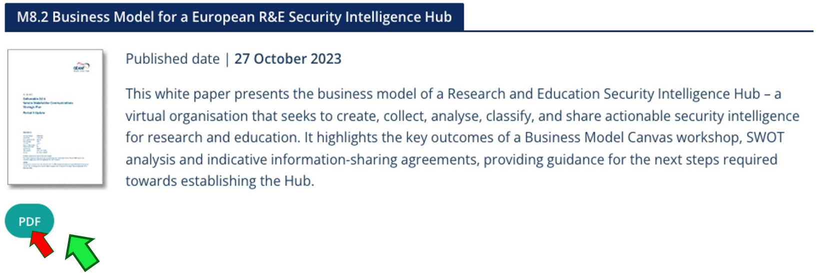
(your inputs are welcome ☺)

Security
.Days

Co-funded by
the European Union

Easter eggs

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



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

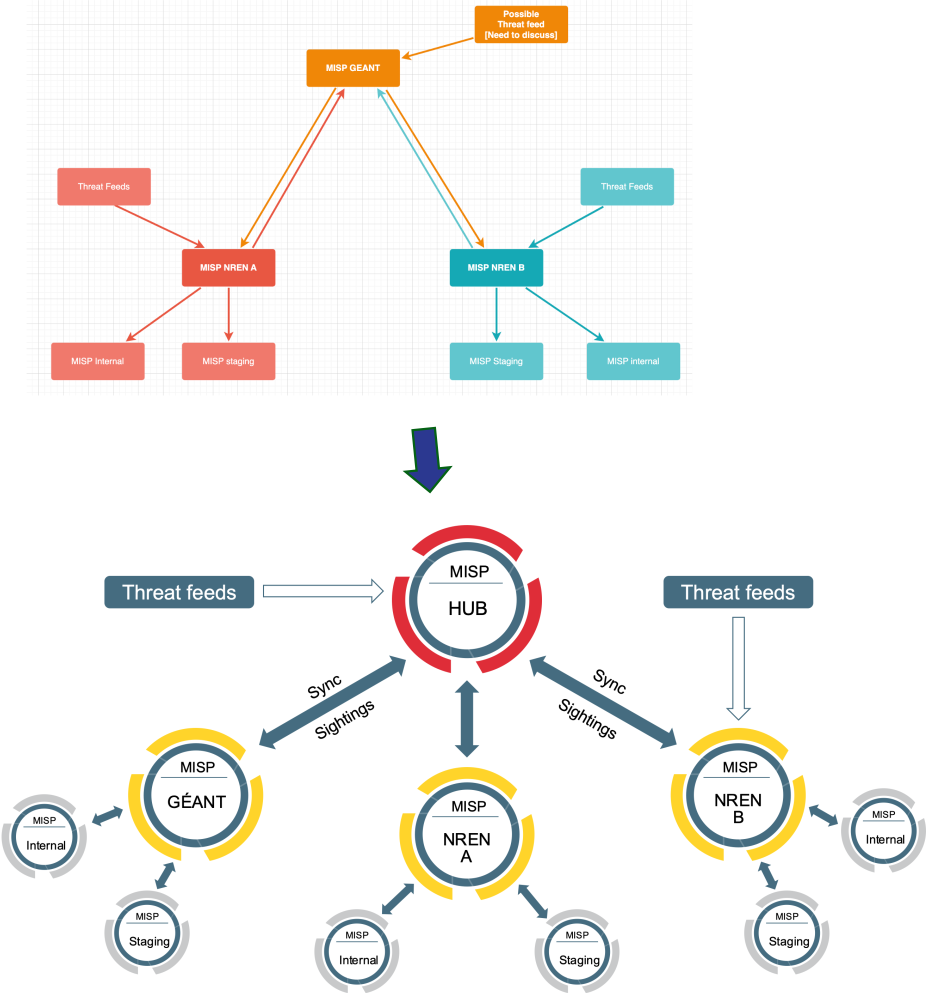
Published date | 27 October 2023

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.

2024 (remaining)

- Sync events between GÉANT and NREN MISP instances
- Setup feeds of NREN generated threat data
- Commence feed evaluation
- Continue with individual matching, alerting, dashboards, etc.
- Share experiences!

R&E Hub: MISP Setup



Possible Threat feed [Need to discuss]
MISP GEANT
Threat Feeds
Threat Feeds
MISP NREN A
MISP NREN B
MISP Internal
MISP staging
MISP Staging
MISP internal
Threat feeds
MISP HUB
Threat feeds
Sync
Sightings
Sync
Sightings
MISP GÉANT
MISP NREN A
MISP NREN B
MISP Internal
MISP Staging
MISP Internal
MISP Staging
MISP Internal
MISP Staging