31-10-2023

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

Contractual Date:	31-10-2023
Actual Date:	31-10-2023
Grant Agreement No.:	101100680
Work Package:	WP8
Task Item:	Task 3.4
Nature of Milestone:	White Paper
Dissemination Level:	PU (Public)
Lead Partner:	GÉANT Association
Document ID:	GN5-1-23-0ec7dc

Authors:	WP8 T3.4 CTI Team: Stephanos Andreou (CyNet); Tony Gray (HEAnet); Ergys Kajo (NORDUnet/DeiC); Melvin Koelewijn (SURF); Maciej Miłostan (PSNC); Roderick Mooi (GÉANT Association); Victor Näslund (NORDUnet/SUNET); Hank Nussbacher (IUCC); Fredrik Pettai (NORDUnet/SUNET)

Abstract

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.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This white paper presents the business model for 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. Following an introduction of the Hub as a concept, three phases of implementation are proposed with key objectives progressing according to GN5 project phases. The results of a Business Model Canvas workshop are presented providing input into the areas of customer segments, value propositions, channels, customer relationships, revenue streams, key resources, activities, partners, and costs, based on which the following activities have been identified for phase 1 (GN5-1):

- Identify and evaluate suitable tools to create and share cyber threat intelligence (CTI).
- Set up a preliminary/PoC ecosystem for sharing CTI between GÉANT and NRENs.
- Share threat intelligence from at least two project participants with the rest of the WP8 CTI sub-task.
- Illustrate the ability to action shared CTI through correlation with commonly available data sources (e.g. flow data).
- Evaluate selected external threat intelligence feeds.
- Engage with the broader NREN community through events and sharing outcomes.

The results of a SWOT analysis of the hub are presented next, highlighting key strengths of the Hub including a focus on R&E by R&E, reducing duplication of effort by sharing experiences, and funding secured for the initial phases. Conversely, resource limitations, particularly time and availability of sub-task team members, were identified as the Hub's primary weakness. The timing is right for CTI, which is currently gaining a lot of traction, and multiple opportunities were revealed in terms of organisations willing to share their own experiences of establishing similar initiatives (CIRCL, REN-ISAC) as well as for collaboration not just between NRENs but also with wider communities such as TF-CSIRT. Lastly, threats were identified related to competition from commercial competitors, financial sustainability, staff changes, and trust along with proposed mitigations.

An important consideration when dealing with cyber threat intelligence is the handling of sensitive information. To manage this, the team identified four 'circles' of trust starting from an 'inner circle' (most trust) comprised of GÉANT and partner NRENs and moving outward to subsequent circles characterised by decreasing levels of trust, from other R&E and trusted groups, to vendors and feed providers and, finally, to the rest of the world (least trust). For each trust group, appropriate types of information sharing agreements were identified to help protect any sensitive data that may be shared. These range from a code of conduct for GN5 project participants to MOUs/NDAs for vendors and feed providers. For data/intelligence that is shared publicly, it would be impossible to establish agreements and thus only the least sensitive information should be shared with the rest of the world.

In conclusion, the R&E Security Intelligence Hub empowers security teams to counter imminent cyber threats, bringing NRENs and GÉANT together to take their joint defences to the next level and facilitate the creation of a safe and secure environment for all R&E network users.

1 Introduction

The Research and Education (R&E) Security Intelligence Hub is a proposed *virtual organisation* – aka joint security intelligence expert workforce – that aims to create, collect, analyse, classify, and share security intelligence for research and education. Together with the security operations tools developed in partnership with the SOCTools subtask in WP8, as well as intelligence feeds and defined procedures, the Hub will gather actionable information for GÉANT, NRENs and NREN customers. Secondary activities in support of (and which may be facilitated by) the Hub include coordinating training, events, and workshops.

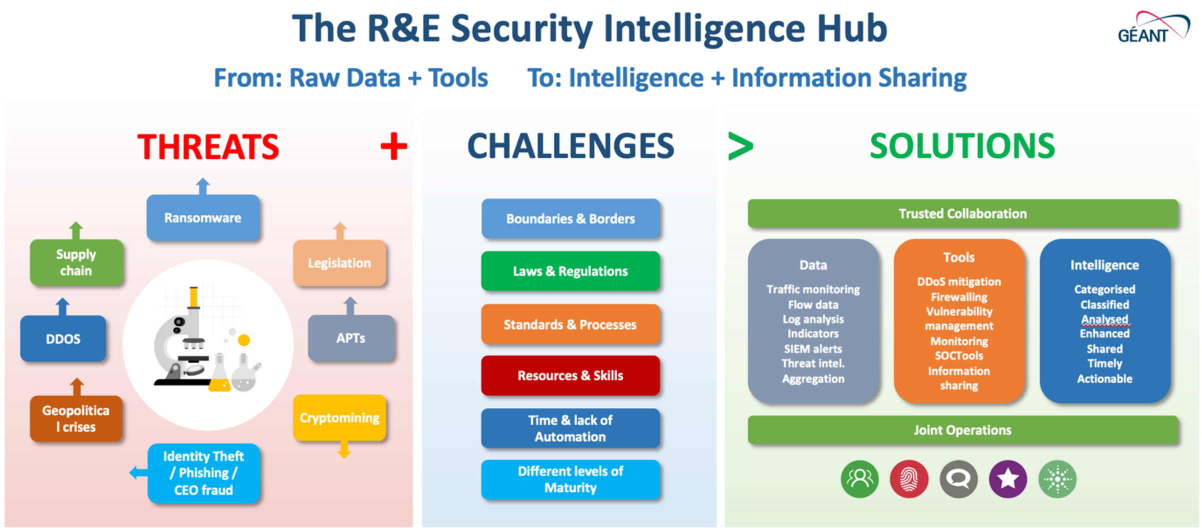

Figure 1.1: The R&E Security Intelligence Hub[1]

The R&E Security Intelligence Hub is intended to counter specific cyber threats and challenges with solutions centred around trusted collaboration and joint operations, transforming raw data with the help of specialised tools and analysts into intelligence that can be shared and acted on for the greater benefit of all participants.

The Hub can be likened to an information sharing community such as an Information Sharing and Analysis Centre/Organisation (ISAC/ISAO).

In order to explore potential business models for the Hub, a Business Model Canvas was populated by the GN5-1 WP8 T3.4 CTI team members. The implementation phases, Business Model Canvas, and SWOT analysis performed are summarised in the next section (2). Some conclusions and next steps are provided in section 3.

[1] https://tnc22.geant.org/posters/#c220

2 The Research and Education Security Intelligence Hub

2.1 Implementation Phases

It is envisioned that the R&E Security Intelligence Hub will be designed and implemented in at least three phases, over GN5-1 and potentially future projects under the GN5-FPA and beyond:

Phase 1 (GN5-1): The first phase of the Hub will be executed as a proof-of-concept by the CTI working group in WP8 T3.4. The primary objectives in this phase are to:

- Create and share CTI between the sub-task partner NRENs (and GÉANT).
- Investigate and set up experimental infrastructure for sharing CTI.
- Co-develop tools and integrations to make CTI actionable for NRENs and NREN customers.
- Discuss and propose possible information sharing agreements that may be needed to share CTI more broadly.
- Identify related initiatives, partners, vendors, etc. that could contribute towards Hub activities.

Phase 2 (future GÉANT projects): Phase-2 the objectives will be centred around formalising the organisational structure of the Hub and sharing CTI with more NRENs and possibly other R&E institutions:

- Create and share CTI between more project partners, GÉANT customers and other organisations in the R&E sector (with appropriate information sharing agreements).
- Collaborate with broader, global, information-sharing initiatives through forums such as FIRST, TF-CSIRT and ENISA.
- Arrange engagement workshops, training events, etc. to refine Hub activities and align them with R&E sector needs and requirements, as well as share experiences.

Phase 3 (onwards): Future developments TBD:

- Expand the R&E Security Intelligence Hub service offerings.

2.2 Business Model Canvas

"The Business Model Canvas [BMC] is a strategic management template used for developing new business models and documenting existing ones. It offers a visual chart with elements describing a firm's or product's value proposition, infrastructure, customers, and finances, assisting businesses to align their activities by illustrating potential trade-offs."[2]

The CTI task team utilised the BMC template provided by Strategyzer [BMC Template] for inputs to this section.

[2] https://en.wikipedia.org/wiki/Business_Model_Canvas

2.2.1 Customer Segments

The customer segments considered for the R&E Security Intelligence Hub are:

- NRENs
- GÉANT
- NREN customers (mostly indirectly – via NRENs)

2.2.2 Value Propositions

The hub provides value in the following areas:

- De-duplicating work/effort – e.g. verifying IOCs, adding metadata to threat intel, etc.
- Sharing experiences (not re-inventing the wheel) and addressing common challenges together.
- Combining and sharing resources, particularly persons with specialised/scarce skills but also tooling, etc.
- Verified/vetted (and therefore actionable) data – e.g. IOCs.
- Creating intel specifically for / relevant to R&E – e.g. threat actor reports.
- Sharing collected intel within the GÉANT and NREN networks and with their customers.
- Collecting and sharing feedback from R&E threat intel consumers.
- Central contact point for R&E threat intel – Portal/dashboard(s) showing key intel and metrics for customers.
- Optimised architecture and implementation for CTI-related tooling – e.g. distributed/hub-and-spoke model for MISP, syncing of events, sightings, correlations, etc.
- Early(ier) warnings of possible compromise, vulnerabilities, etc.

All leading to an improved view of the R&E threat landscape.

2.2.3 Channels

The following channels can be utilised by the Hub.

For (near)real-time sharing of CTI:

- NREN and NREN customer security teams/contacts – including SOCs and CSIRTs, ISOs:
  - Portal/dashboard(s) (with visualisations and alerts)
  - Instant Messaging (e.g. Slack channel(s))
  - Tool synchronisation (e.g. MISP)
- Engagement with national/regional cybersecurity centres/projects, etc. E.g. NCSCs:
  - Various mechanisms, particularly syncing of threat feeds

For Hub developments, trends, information sharing:

- GÉANT Project task-forces and special interest groups (e.g. TF-CSIRT and SIG-ISM).
- NREN engagement forums:
  - Events – workshops, training events, conferences
  - GÉANT CTO workshops
  - Individual engagements

- Email (incl. mailing lists).

2.2.4 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.

2.2.5 Revenue Streams

The initial funding for the Hub activities is (predominantly) provided via the GN5-1 project and potentially subsequent GÉANT projects under the GN5-FPA. Future sustainability might need to be considered at a later stage. Alternative/additional (future) revenue streams could include:

- Subscription/membership fees
- Paid-for threat intel feeds

It is noted that the main drive behind the Hub is the intention to provide a shared service for the greater good rather than profit. However, costs may need to be recovered.

2.2.6 Key Resources

The key resources that are required for the Hub (as identified at this stage) include:

- People – security analysts, engineers, etc.
- Servers (likely virtual)
- Threat feeds
- CTI tooling – e.g. MISP
- Funding (to cover costs / as per revenue streams)

2.2.7 Key Activities

For Phase 1, the key activities that have been identified include:

- Evaluate the various tools available for collecting and analysing IOCs and feeds – thus far [MISP] has emerged as the de-facto standard within the information security sharing community; for workflows and automation, [IntelMQ] may also be useful.
- Investigate, design, and implement an appropriate infrastructure setup for sharing CTI between sub-task member organisations.
- Together with WP8 T3.3 SOCTools, identify illustrative use cases for CTI.
- Share threat intelligence from at least two project participants with the rest of the sub-task.
- Evaluate selected external threat intelligence feeds.

- Illustrate the actionability of collected CTI by implementing processes/tools/integrations to correlate IOCs, etc. with readily available data sources (e.g. Flow data).
- Monthly customised R&E sector (/academia) report on threats/incidents, etc.

Key activities for Phase 2 would follow on from these and include:

- Validating intel feeds (possibly including procuring commercial feeds).
- Obtaining CTI from additional R&E sources (e.g. RPZ feed for DNS filtering).
- Arranging events, training, etc.
- Creating and maintain central platform/portal/dashboard(s) and making this available to customers.
- Supporting customers in accessing the above platform, related queries, etc.
- Sharing within the community.

2.2.8 Key Partners

The key partners of the R&E Security Intelligence Hub include:

- 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.

2.2.9 Costs

Hub costs include:

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

2.3 SWOT

In addition to the business model canvas, the T3.4 team also performed a Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis focussing on the immediate challenges and opportunities presented by the R&E Security Intelligence Hub, as well as the team's readiness to tackle them. The results of the SWOT analysis were used to help prioritise activities and provide focus for the Hub implementation team.

These results are summarised in Table 2.1 below.

Strengths (internal, positive factors)	Weaknesses (internal, negative factors)
• Experienced staff within R&E sector • Focused on the R&E sector • Secured funding (at least for initial phases) • Most NRENs have CSIRT teams who are actively looking at security and threats • Wealth of valuable data	Resource constraints – particularly time, prioritisation
Opportunities (external, positive factors)	**Threats (external, negative factors)**
• Knowledge/Sharing: Some R&Es have already successfully implemented different use-cases • Use TF-CSIRT (not only) meetings/workshops for training, getting feedback etc. • Providing integrations of MISP with other tools • Collaboration with similar initiatives within the R&E sector or other sectors • Establish/strengthen GÉANT and NREN relationships with the CTI Teams of R&E CSIRTs • Access to R&E sector data and ability to create valuable CTI from it	• Commercial competitors with 'unlimited' resources. Possible data exfiltration • No finances for keeping the service alive when the Project ends (risk of financial sustainability) • Tools turn commercial or are no longer supported • Sub-task members leave • Lack of trust in broader community

Table 2.1: SWOT Analysis for the R&E Security Intelligence Hub

Starting with internal, the primary *strength* factor of the Hub is that it is created by R&E for R&E. Furthermore, it is relevant to mention that the CTI sub-task in GN5-1 WP8 is composed of experienced members from the sector. This enables the team to combine focus with experience. Furthermore, funding has been secured though the GN project for the initial phases and CTI work is expected to continue in future projects.

The main *weakness* has been identified as resource constraints – sub-task team members have other responsibilities within their organisations and at times these demand more attention which could result in project tasks being neglected / de-prioritised in the face of more immediate day-to-day concerns.

At the same time, there are many identified *opportunities* for the Hub – building on "for R&E, by R&E", the team has access to multiple forums, including TF-CSIRT and FIRST, with organisations willing to share experiences in setting up similar initiatives – CIRCL and REN-ISAC being two key examples. Collaboration with other WP8 sub-tasks, particularly SOCTools, as well as with NRENs not directly participating in the sub-task but willing to contribute to it is also a significant opportunity.

Lastly, there are some *threats* to the success of the R&E Security Intelligence Hub, namely:

- Commercial competitors – This is largely mitigated by the GÉANT project's unique focus on the R&E sector as well as non-profit goal.
- Financial sustainability – Should project funding no longer be available, other viable models can be explored to ensure that the Hub's activities are able to continue. This could include membership/subscription fees (as used by other ISACs).
- Staff changes and lack of resources within the project tasks – The primary mitigation for this is that the onus is on the individual participant (NREN/GÉANT) to meet their committed project resources.

- Trust is earned over time – As the Hub team networks with the communities and proves the value of its services, trust should follow. It is however important to remember the importance of trust and not to break this (e.g. violate code of conduct / MoU / NDAs) under any circumstance.

2.4 Information-Sharing Agreements

The T3.4 CTI team has identified four circles characterised by different levels of trust for the purposes of information sharing. The 'inner' (L1 – most trusted) circle consists of the GN5-1 project partners – GÉANT and NRENs. Moving outward from the inner circle, the next layer (L2) includes close collaborators, trusted groups/forums, and other R&E stakeholders. The next group (L3) includes feed providers and other vendors/service providers. Finally, the outermost ring consists of everyone else. These 'circles of trust' are depicted in the following diagram.

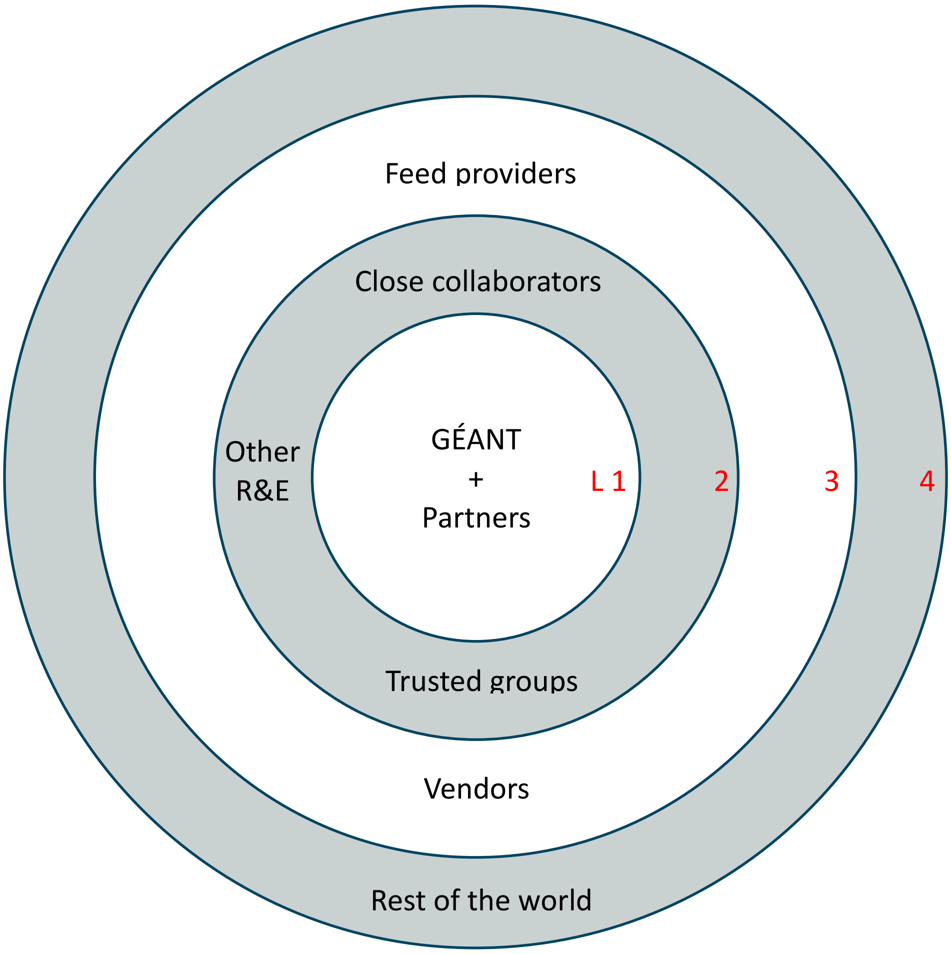

Figure 2.1: R&E Security Intelligence Hub circles of trust

Various types of information-sharing agreements are described in *Guidelines to setting up an information sharing community such as an ISAC or ISAO; CIRCL, X-ISAC* [ISAC Guidelines] and can be summarised as follows:

- Subscriber agreement:
  - legally binding
  - private entities / commercial activities
- Confidentiality agreement / NDA:

  - establishes what (type of) information can be considered confidential.
  - use of Traffic Light Protocol (TLP) / similar
  - can also set obligations for the recipient of the confidential information.
- Code of Conduct:
  - not legally binding
  - standard community practices / guidelines for behaviour
- MoU
  - bilateral agreement – between information-sharing community and external entity
  - framework for cooperation
- Informal agreement
- Trust-based

These agreements are needed to ensure acceptable protection and safeguarding of sensitive information as well as legal compliance (e.g. GDPR if/when dealing with PII).

The following agreements have been identified as being most relevant to each circle of trust[3]:

Level	Trust Group	Sharing agreement
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 [TLP] (i.e. non-sensitive) information

Table 2.2: Sharing agreements for each trust group

For Phase 1 (GN5-1) of the R&E Security Intelligence Hub, the team will focus on Level 1 and the identified Code of Conduct (project contract terms are already in place and sufficient). In Phase 2 (GN5-2), Level 2 and possibly Level 3 will be included.

[3] This was done in consultation with the Special Interest Group on Information Security Management (SIG-ISM).

3 Conclusions and Next Steps

The Research and Education (R&E) Security Intelligence Hub is a game changer for cybersecurity defenders, empowering R&E network teams across Europe and beyond to keep informed of and act decisively to counter imminent cyber threats. The Hub unites experts from the GÉANT and NREN community to create, collate, verify, and share a range of threat intelligence as well as experience in utilising that intelligence effectively in network defences. This intelligence and the resulting actions will give the community an edge over threat actors and attackers, facilitating the creation of a safe and secure environment for all R&E network users.

For the remainder of GN5-1 in 2023-24, the following activities leading towards the establishment of the R&E Security Intelligence Hub will be in focus:

- Create and share CTI between GÉANT and at least 3 NRENs.
- Perform a PoC of selected tools to share CTI between partners, particularly MISP.
- Share experiences of correlating IOCs, etc. with commonly available data such as flow data for further dissemination and knowledge sharing
- Investigate use cases for appropriate actions that NRENs can perform using threat intelligence.
- Develop appropriate information-sharing agreement templates for the identified 'circles of trust'.
- Closely follow CTI developments in related forums such as TF-CSIRT and FIRST by participating in the TF-CSIRT CTI working group and attending the FIRST CTI Conference as a minimum
- (Co-)organise one or more workshops to gather requirements and discuss the next steps / priorities for the Hub.

This will set a solid basis for expanding and formalising the Hub in the future.

References

[BMC Template]	https://www.strategyzer.com/library/the-business-model-canvas
[ISAC Guidelines]	https://www.x-isac.org/assets/images/guidelines_to_set-up_an_ISAC.pdf
[MISP]	https://www.misp-project.org/
[IntelMQ]	https://github.com/certtools/intelmq#welcome-to-intelmq
[TLP]	https://www.first.org/tlp/

Glossary

CIRCL	Computer Incident Response Center Luxembourg
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CTO	Chief Technology Officer
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
IOC	Indicator of Compromise
ISAC	Information Sharing and Analysis Centre
ISAO	Information Sharing and Analysis Organisation
MISP	Malware Information Sharing Platform
MoU	Memorandum of Understanding
NCSC	National Cyber Security Centre
NDA	Non-Disclosure Agreement
NREN	National Research and Education Network
PoC	Proof of Concept
R&E	Research and Education
REN-ISAC	Research and Education Network Information Sharing Analysis Center
RPZ	Response Policy Zone
SIG-ISM	Special Interest Group – Information Security Management
SOC	Security Operations Centre
SWOT	Strengths, Weaknesses, Opportunities, Threats
TF-CSIRT	Task-Force CSIRT
TLP	Traffic Light Protocol