Information Sharing Agreements?

For sharing threat intel…

Roderick Mooi
Information Security Officer
GÉANT

SIG-ISM, Trondheim
4 May 2023

CTI

- “Cyber threat intelligence represents a **force multiplier** for organizations looking to update their response and detection programs to deal with increasingly sophisticated **advanced persistent threats**. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on **countering** those flexible and persistent **human threats with** empowered and trained **human defenders**.”
  - https://www.**sans**.org/cyber-security-courses/cyber-threat-intelligence/

Cyber Threat Intelligence

TTPs / MITRE ATT&CK

- “The **analysis** of an **adversary's intent, opportunity, and capability** to do harm is known as cyber threat intelligence. Intelligence is *not* a data feed, nor is it something that comes from a tool. Intelligence is **actionable information** that addresses an organization's key **knowledge gaps, pain points, or requirements**.”

  - https://www.**sans**.org/cyber-security-courses/cyber-threat-intelligence/

- “…is **systematic collection, analysis** and **dissemination** of information pertaining to a company’s operation in cyberspace and to an extent physical space. It is designed to inform all levels of **decision makers**. The analysis is designed to help keep **situational awareness** about current and arising **threats**.”

  - https://www.**first**.org/global/sigs/cti/curriculum/cti-introduction#A-working-definition-for-Cyber-Threat-Intelligence

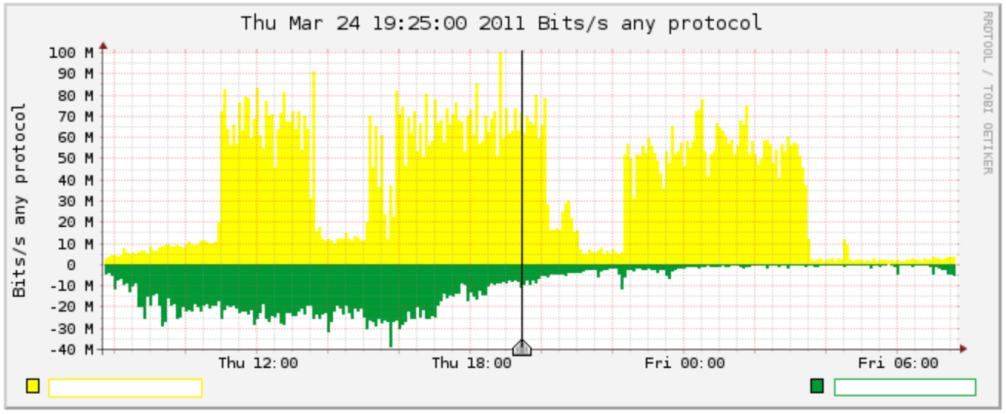
We all have staff and skill shortages, are we:

to ease the common burden?

Images source: unsplash.com
/@lennykuhne
/@airfocus
/@nicolesherrero

We have the data & tools

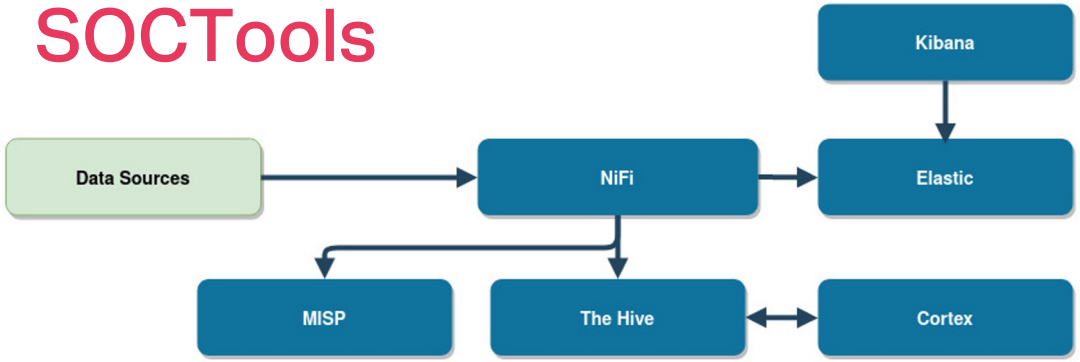
i



ii

iii

SOCTools



i: unsplash.com/@anvesh1616

ii: yurisk.info/Nfsen_custom_profile.png

iii. shadowserver.org/what-we-do/network-reporting/

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

How do we get to:

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

+

- Collaborating
- Communities
- Shared operations / managed services?
- Resources

= Getting ahead!

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:

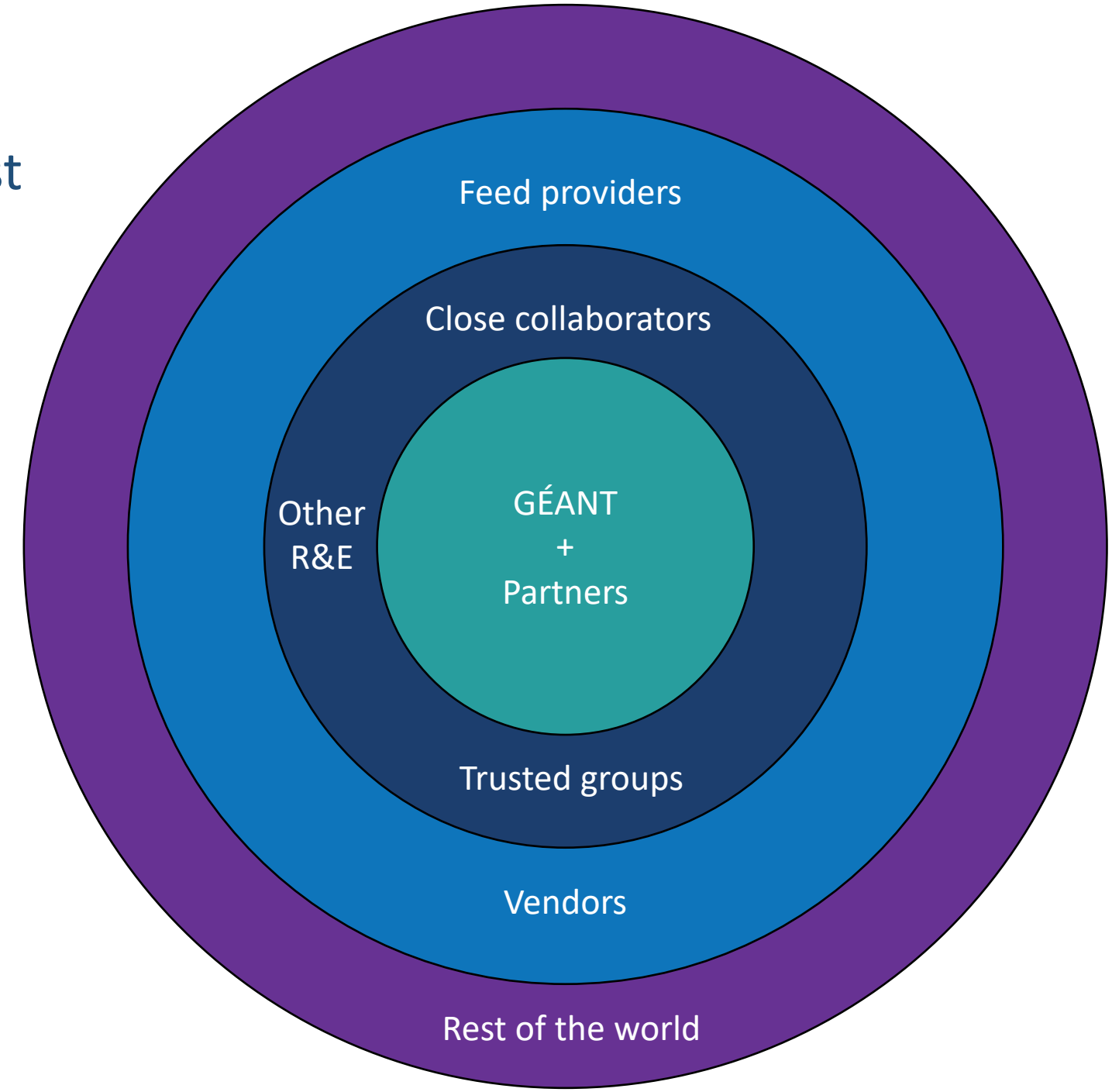
- DDOS detection & mitigation: NeMo + FoD
- Support for eduVPN
- Tools for security operations
- Cryptographic services
- Broker (NREN) security services
- Cyber Threat Intelligence

Task 2: Security Training and 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

European R&E security Intelligence Hub

Circles of Trust



Potential types of agreements [i]

- Subscriber agreement
  - legally binding
  - private entities / commercial activities
- Confidentiality/NDA agreement
  - establishes what (type of) information can be considered as confidential
  - use of 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

i. Guidelines to setting up an information sharing community such as an ISAC or ISAO; CIRCL, X-ISAC

Agreements on information sharing	Use	Type
NDA	Usually bi-lateral, often used with law enforcement or government bodies	
Code of conduct	Usually multi-lateral, provides straightforward instructions on the standard practices and guide the behaviour of the members of the organisation	Usually not legally binding but in written form
MoU	Usually bi-lateral, often used with law enforcement or government bodies	Usually not legally binding but in written form
Informal agreement	Based on trust of the members of the organisation. It does not require any formalisation and usually takes oral form	Usually in oral form

Potential types of agreements

- Subscriber agreement (GÉANT + NRENs already have)
  - GN5 Consortium / Framework Partnership Agreement
  - + Specific Grant Agreement
- Confidentiality/NDA agreement
  - included in above
- * Code of Conduct (TF-CSIRT, FIRST, etc.)
  - not legally binding
  - standard community practices / guidelines for behaviour
  - * more specific than FPA / SGA – e.g. include TLP
- * MoU
  - bilateral agreement – between information sharing community and external entity
  - framework for cooperation
- Informal agreement
  - trust-based

GN5 Framework Partnership Agreement

10. **Data Protection** (+ privacy policy) → personal data

10.1. Each Party will comply with all applicable requirements of all data protection and privacy legislation in force from time to time in the countries in which they operate or are established (the "**Data Protection Legislation**"). This Article 10 is in addition to, and does not relieve, remove or replace, a Party's obligations or rights under the Data Protection Legislation.

10.2. As and when required by the applicable Data Protection Legislation the Parties shall enter into bilateral or multilateral data sharing and/or data processing agreements between them in relation to any personal data that they share between them.

12. **Non-disclosure of information** → confidential data

12.1. All information in whatever form or mode of transmission, which is disclosed by a Consortium member (the "Disclosing Party") to any other Consortium member (the "Recipient") in connection with a Project during its implementation and which has been explicitly marked as "confidential", or when disclosed orally, has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within 15 days from oral disclosure at the latest as confidential information by the Disclosing Party, is "Confidential Information".

12.2. The Recipients hereby undertake, in addition and without prejudice to any commitment of non-

GN5-1 Grant Agreement

ARTICLE 13 — CONFIDENTIALITY AND SECURITY

13.1 Sensitive information

The parties must keep confidential any data, documents or other material (in any form) that is identified as sensitive in writing ('sensitive information') — during the implementation of the action and for at least until the time-limit set out in the Data Sheet (see Point 6).

If a beneficiary requests, the granting authority may agree to keep such information confidential for a longer period.

Unless otherwise agreed between the parties, they may use sensitive information only to implement the Agreement.

The beneficiaries may disclose sensitive information to their personnel or other participants involved in the action only if they:

☆ (a) need to know it in order to implement the Agreement and

☆ (b) are bound by an obligation of confidentiality.

GN5-1 Grant Agreement

ARTICLE 15 — DATA PROTECTION

15.1 Data processing by the granting authority

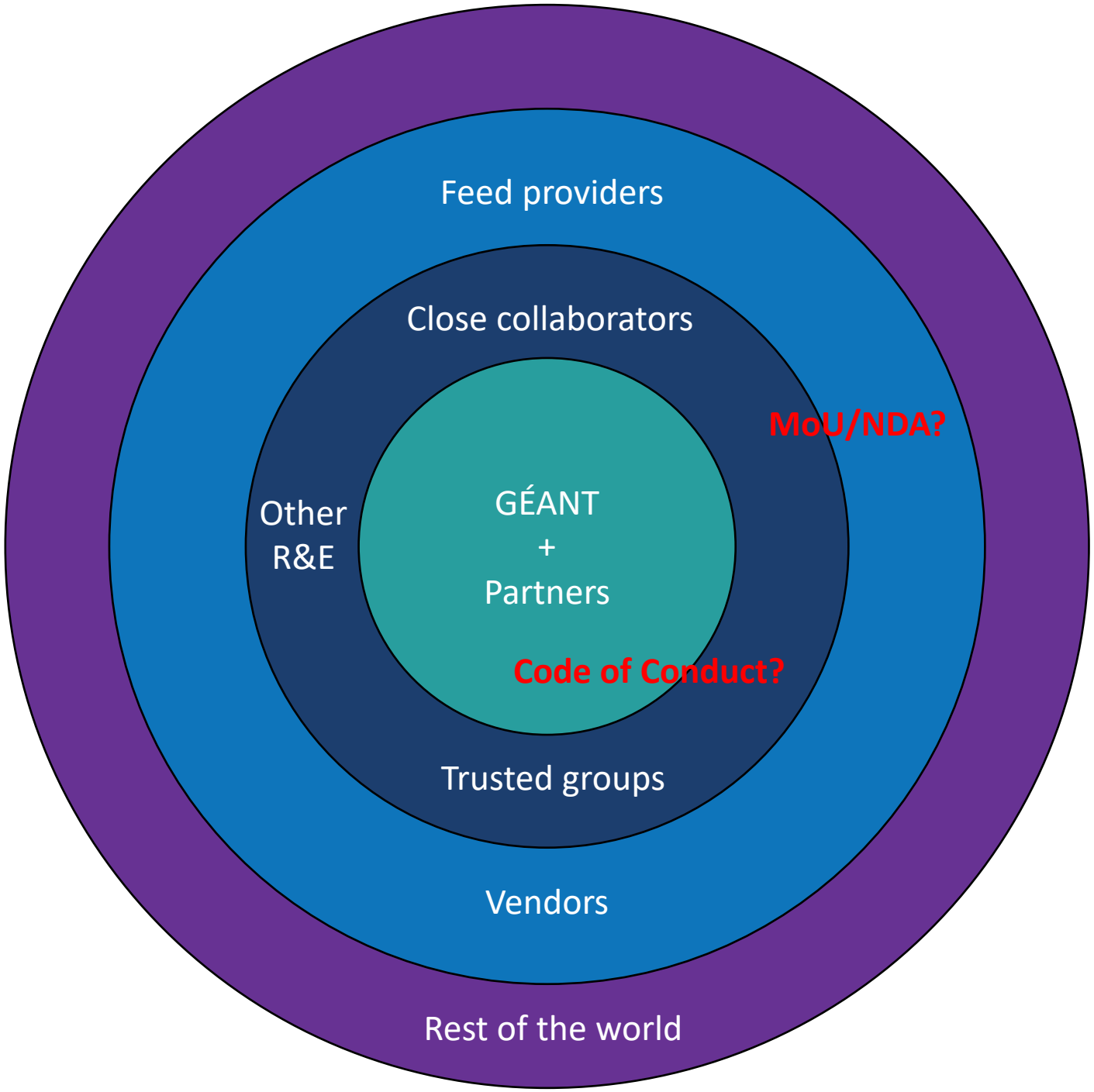
Any personal data under the Agreement will be processed under the responsibility of the data controller of the granting authority in accordance with and for the purposes set out in the Portal Privacy Statement.

For grants where the granting authority is the European Commission, an EU regulatory or executive agency, joint undertaking or other EU body, the processing will be subject to Regulation 2018/1725[15].

15.2 Data processing by the beneficiaries

The beneficiaries must process personal data under the Agreement in compliance with the applicable EU, international and national law on data protection (in particular, Regulation 2016/679[16]).

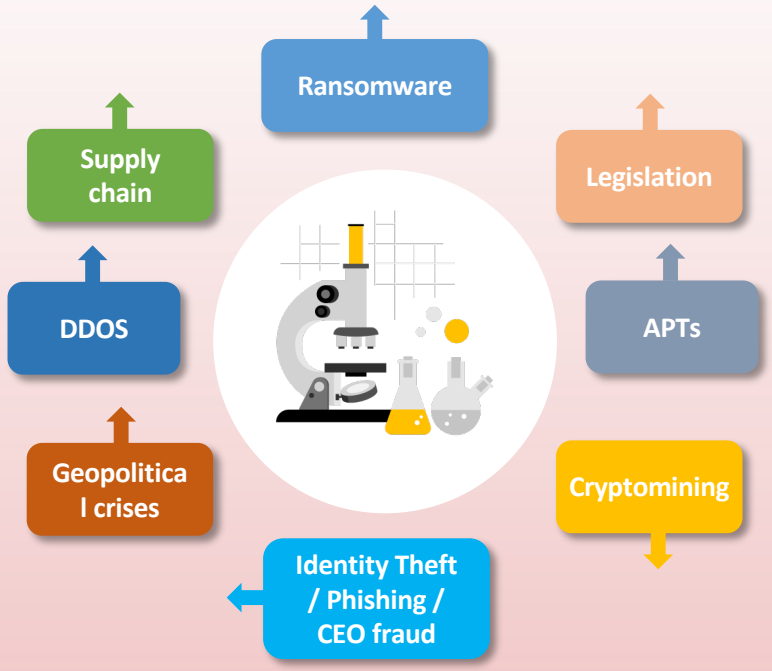
Agreements?


Feed providers
Close collaborators
MoU/NDA?
Other
R&E
GÉANT
+
Partners
Code of Conduct?
Trusted groups
Vendors
Rest of the world

The European 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

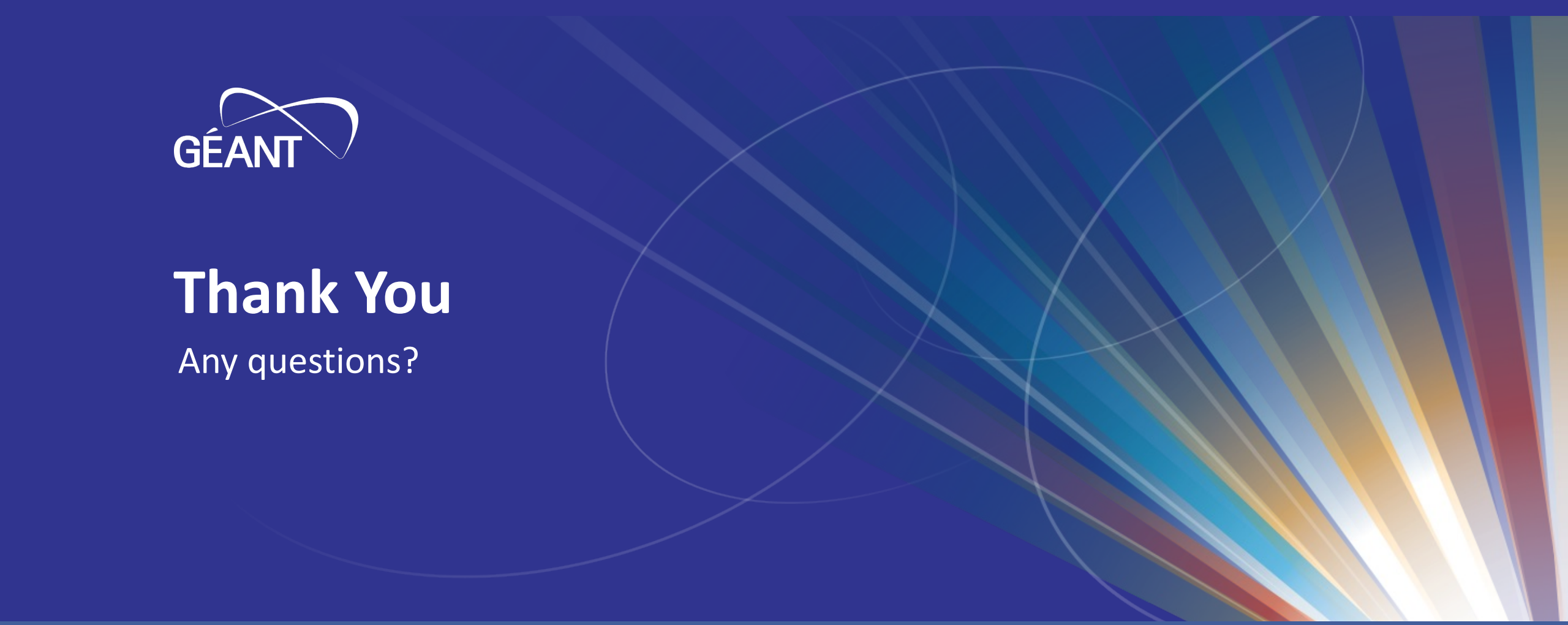
Trusted Collaboration

Data
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



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).