Deloitte.

Cyber intelligence exchange in business environment : a battle for trust and data

Experiences of a cyber threat information exchange research project and the need for public private collaboration

BISC BELGIAN INTELLIGENCE STUDIES CENTRE

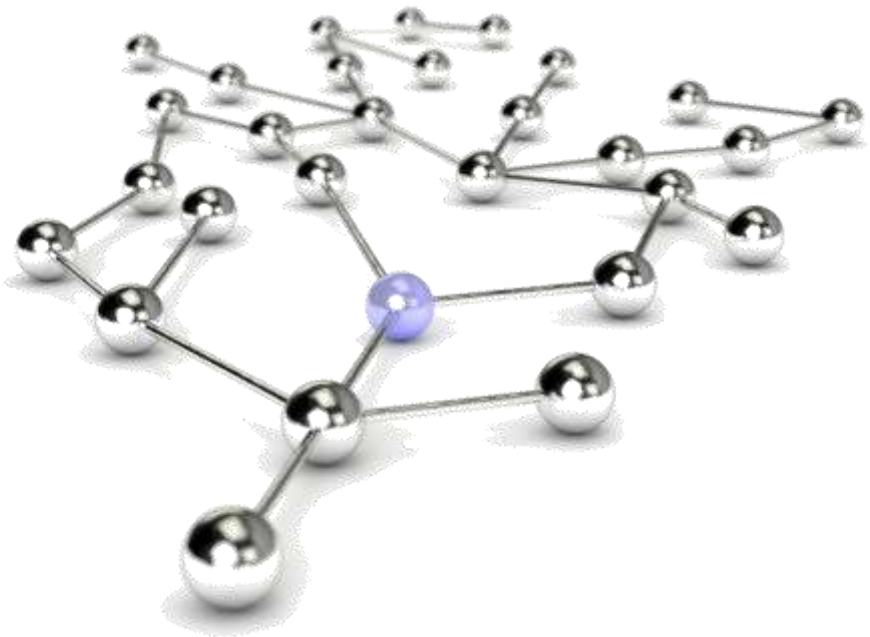
Building Belgium's Cyber intelligence knowledge capabilities
Brussels, December 2nd 2014

Luc Beirens
in a nutshell

- Joined Deloitte June 1st 2014 – Director cyber security services

- 32 years in law enforcement – 27 years in ICT
- 23 years in computer forensics and cybercrime combating
- Former head of Belgian Federal Computer Crime Unit (2001-2014)
- Former chair of EU Cybercrime task force (2010 -2013)

Contents



CTIS Initiative Problem Statement - The Challenge

The digital revolution is driving innovation and growth, yet also exposing us to new and emerging threats.

New organisational goals and new ways of working are driving innovation and growth, but these expose us to new and emerging threats.

Prevention and detection must be optimized by exchange of information on cyber attacks. This is effective since actors will re-use their criminal infrastructure and mode of operation.

Introduction

Problem statement

Cyber Threat Information is **critical to proactively deal with targeted attacks**

Need for understanding **intent, tactics, and the campaigns of threat actors**.

However…

1. **Lack of efficient tools / channels to share this knowledge**
2. **Commercial vendors not always consider sharing such information as it is not in their business interest**
3. **Impacted organisations are reluctant to share information on their Indicators of Compromise**
4. **Information sharing takes place in unstructured format (text) and with incomplete content which doesn't allow for automated response**
5. **Cyber Threat Information is only valid if used within a very specific time frame**
6. **Handling and escalation of information on a case-by-case (incident) basis is very time and resources consuming**

Stocktaking : what existed ?

On national level (with international extensions)

- BELNIS => government only
- B-Ccentre => no operational exchange
- CERT community (EU level & world wide)
- Law enforcement (Europol, Interpol, …)
- FS ISAC (Information Sharing & Analysis Community)
- No Cyber coalition (at that moment 2013)

Except for financial sector :

- No real exchange platform for firms
- No public private exchange platform
- No intersector exchange platform

Cyber threat intelligence sharing research project
CTISRP

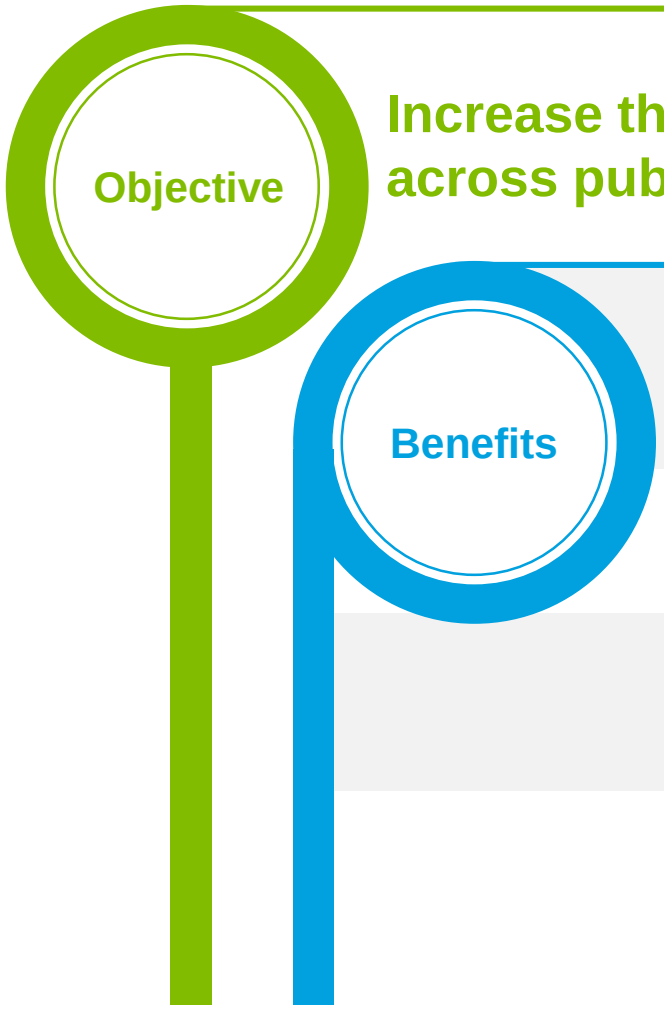
- Started Sept 2013
- 13 Members from different sectors
- Limited number of willing organizations
- One year project : checking feasibility
- Continues only if members agree
- Deloitte as facilitator

Participating sectors

International public organization	CERT organizations	Energy
Banking	Deloitte	Insurance
Military	Retail	Manufacturing

Introduction

Objective and benefits of the Research Project



Increase the level of protection against targeted attacks across public sector and private industry

- **Better protection against targeted cyber attacks**
- **Creation of a trusted Community**
- **Exchange of information through a Proof of Concept platform**
- **A vision towards operational Cyber Threat Information**

Introduction

Project streams

Infrastructure & Security	Establish and maintain a proper sharing infrastructure Ensure that the platform and its data are secure.
Define & standardise the platform's operational processes Ensure that most value is extracted in an easily repeatable manner	**Operational Processes**
Community & Governance	Establish governance structures to ensure trust and participation within the Community
Coordinate streams, activities Guarantee delivery of expected outcomes	**Project Management**

Role of Deloitte
Facilitator

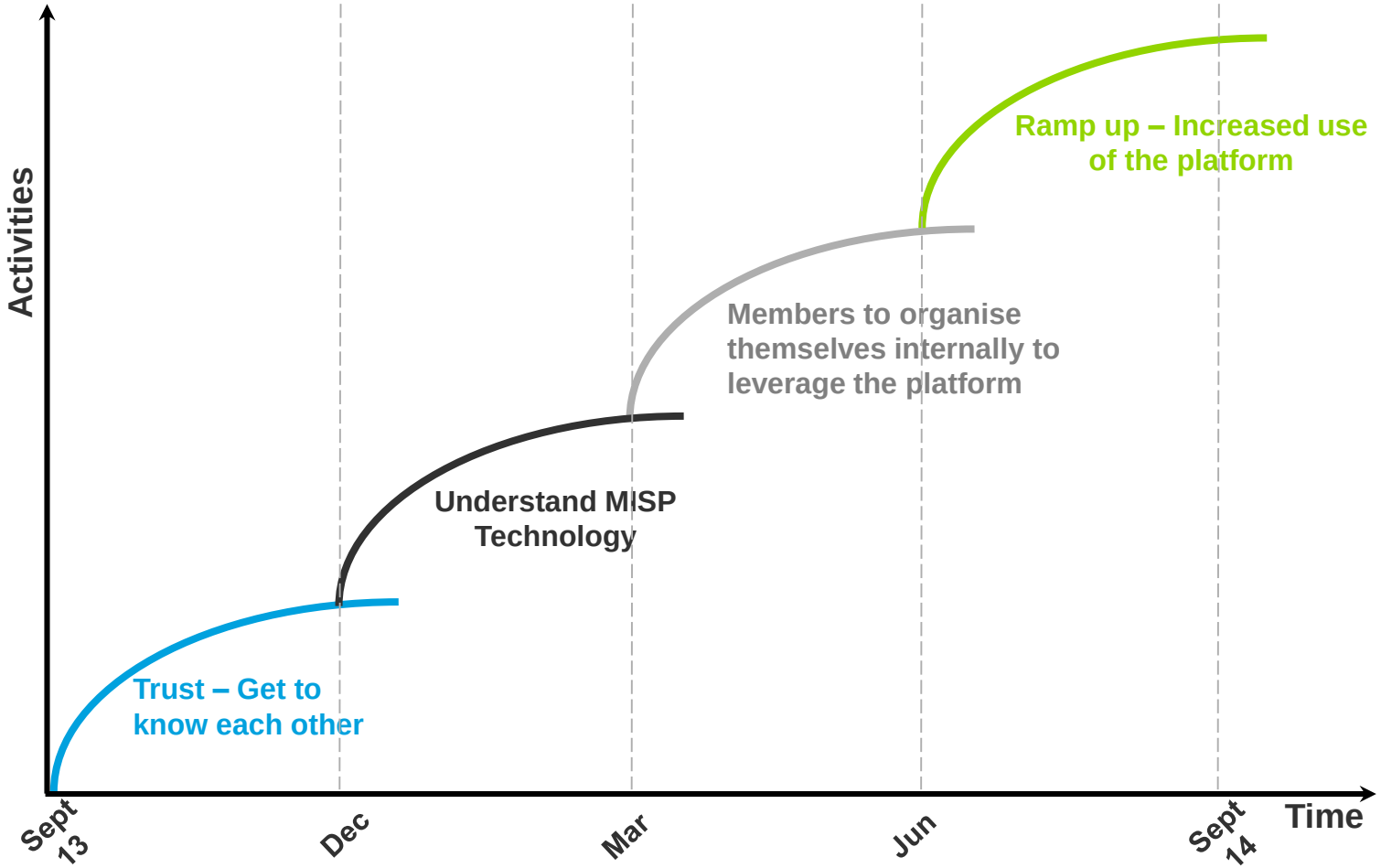
- Not cyber threat intelligence provider in this project

- Participating member of the project

- Facilitating role most important
  - Scout and **motivate** ”willing” organizations
  - **Facilitate** meetings
  - Provide **project management** & administrative support
  - Run **platform** for information exchange

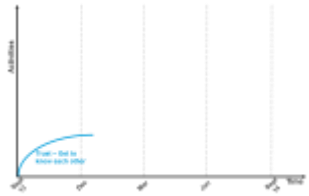
Research Results

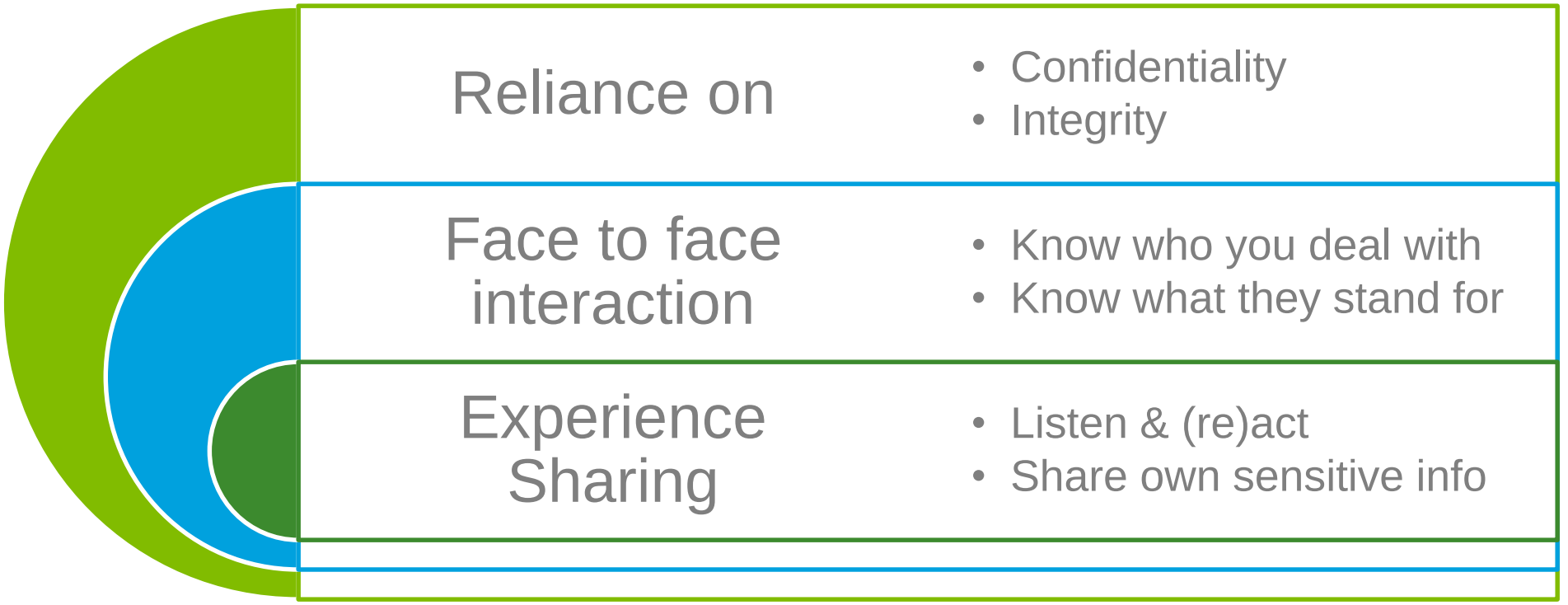
Evolution of the CTI Research Project



Research results

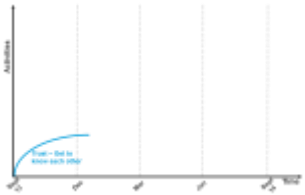
TRUST is key success factor





Research Results - Key lessons learned

Trust



Physical meetings : key for trust

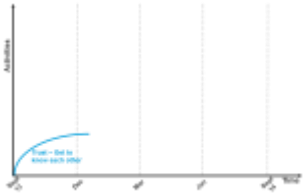
TRUST BUILDING

Not NDA but sharing guidelines

Regular calls : key for project

Research Results - Key lessons learned

Trust : attitude towards others / project



No participant in the Project should claim ownership of any of the data, except for the data that have been provided by its own organization.

OWNERSHIP

USE OF INFO

The information is only for your individual use and should under no circumstances be shared with any other party than the Community Members.

TRADEMARKS

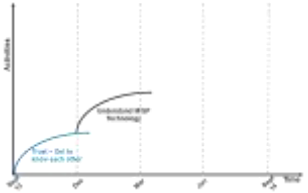
Neither Community Member should use the other Community Members' trademarks, service marks, logos, and/or branding in external publicity material.

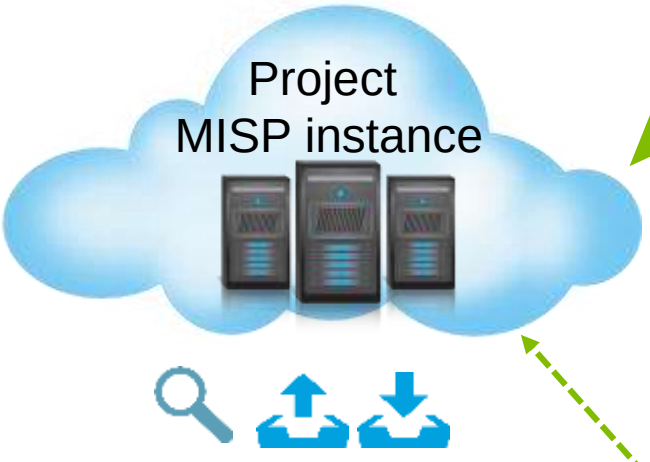
TERMINATION

In case the Project will be discontinued or in case the Project will end and it is decided that it will not be incorporated in a permanent structure for certain reasons, participants should agree to destroy all data received.

Research Results - Key lessons learned

Understand, use and install MISP





Deloitte hosted an instance to facilitate the secure exchange of CTI within the community

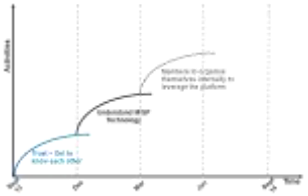
Documentation was provided on how to use MISP, leverage data and upload data

- Quick start guide
- Operational guidelines
- Admin guide
- MISP export/sync guide
- MISP private instance setup guide
- Use case template

The ability to synchronise the centralized MISP instance to a private instance

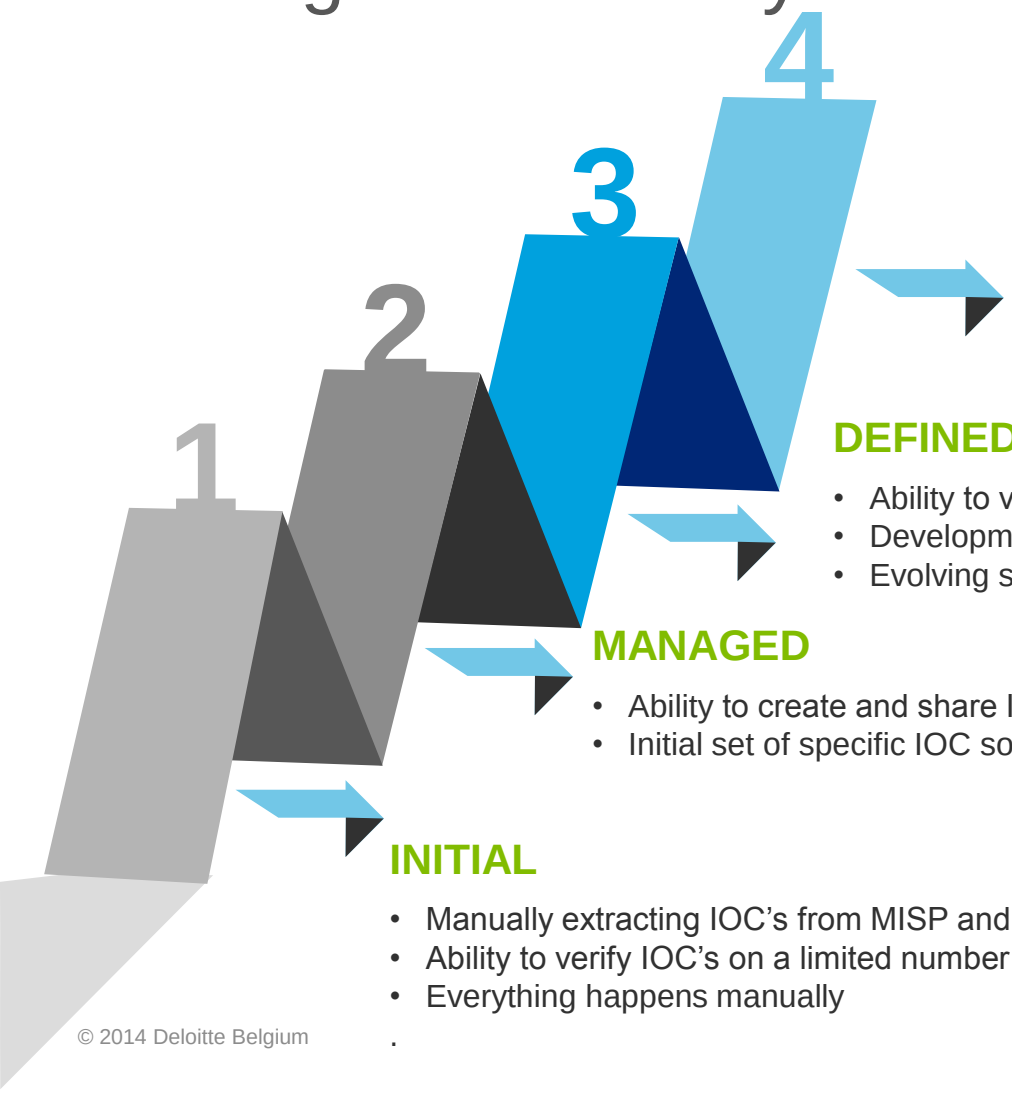
A tested and packaged image of the platform for internal use by community members, allowing members to enter information in the private node and synchronize with the central MISP node

Research Results - Key lessons learned



How to organise internally

Raising CTI Maturity levels



OPTIMIZING

- Upload and download of IOC's in an automated fashion
- Broad coverage that are monitored using IOC's
- Creating and sharing IOC's is an integral part of the incident response playbook
- Automation is key

DEFINED

- Ability to verify IOC's on a broader set of systems
- Development of infrastructure and tools to automate tooling
- Evolving set of IOC sources & use cases

MANAGED

- Ability to create and share IOC's
- Initial set of specific IOC sources & use cases

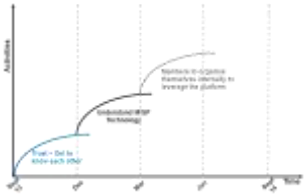
INITIAL

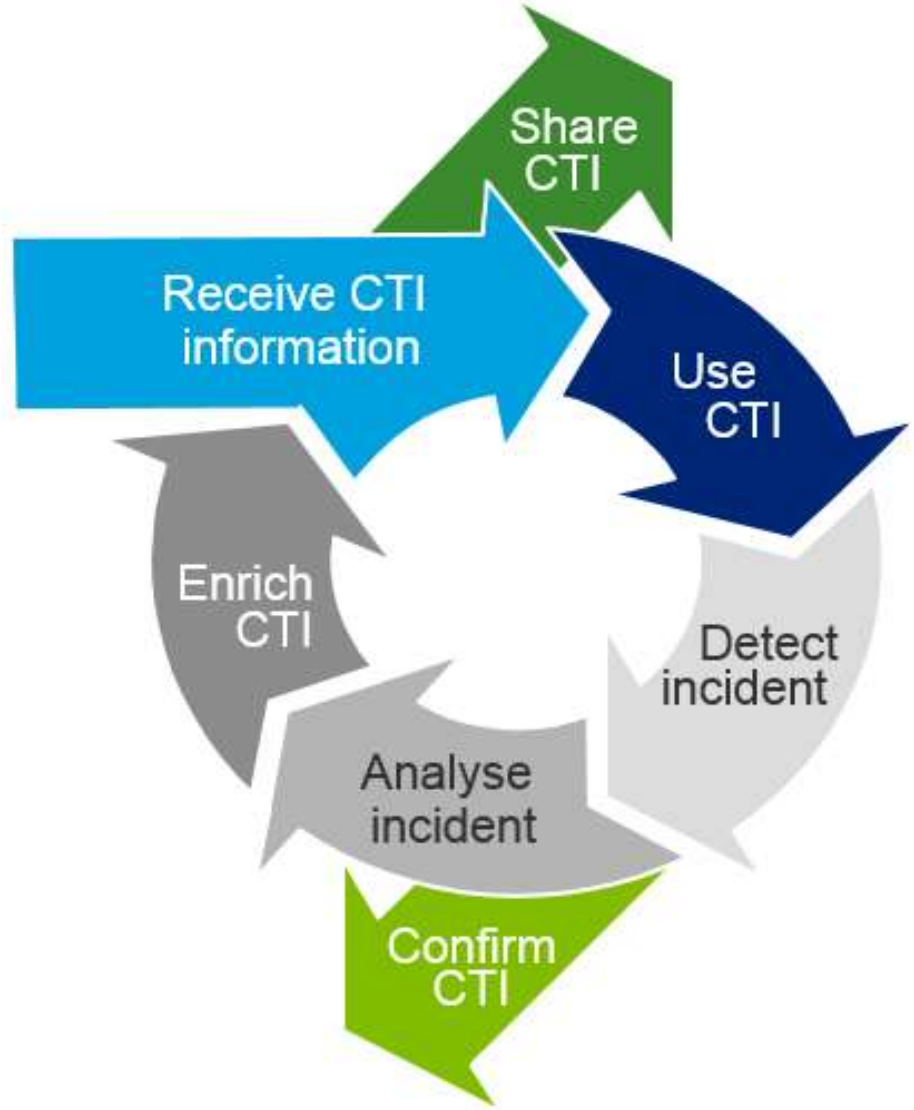
- Manually extracting IOC's from MISP and importing these into internally available tooling
- Ability to verify IOC's on a limited number of systems
- Everything happens manually

.

Research Results - Key lessons learned

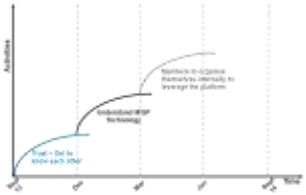
How to organise internally

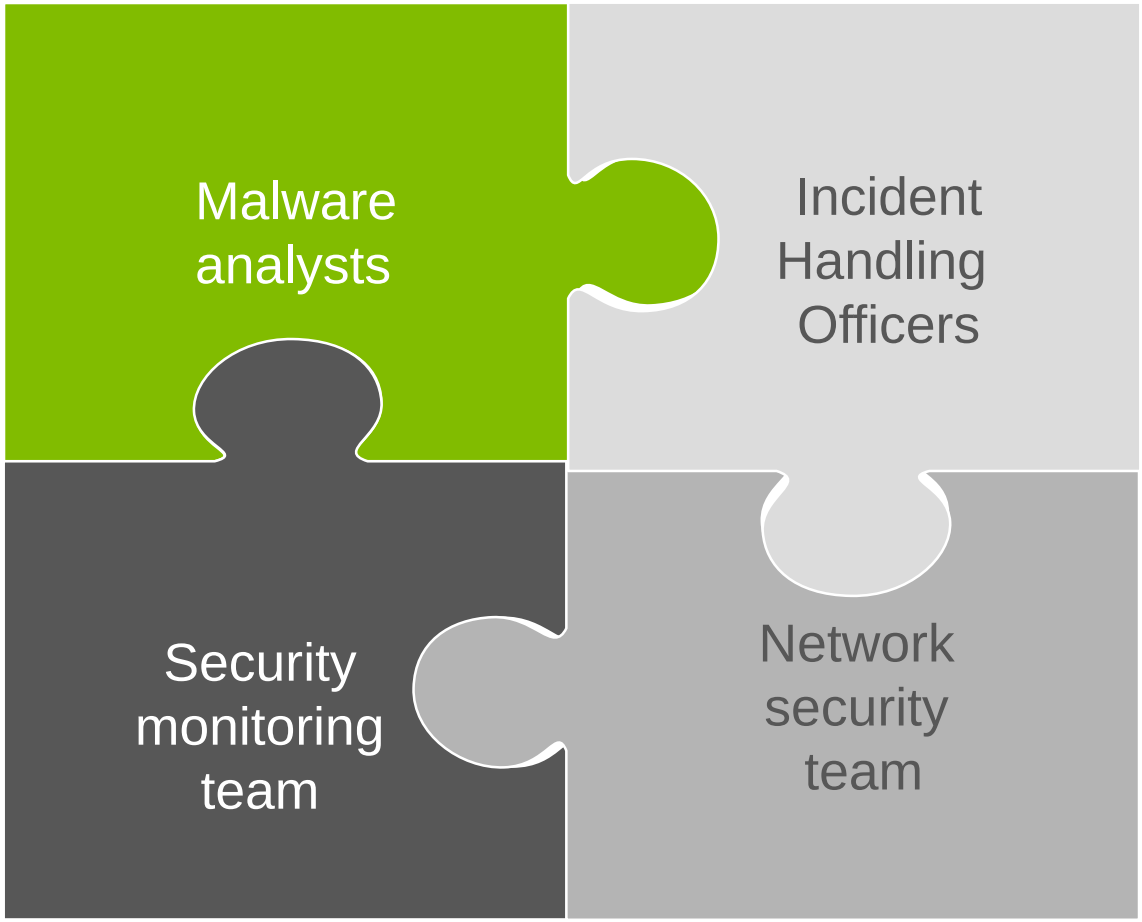




Research Results - Key lessons learned

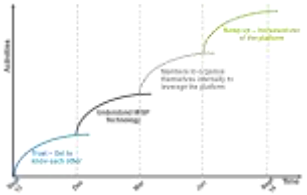
How to organise internally

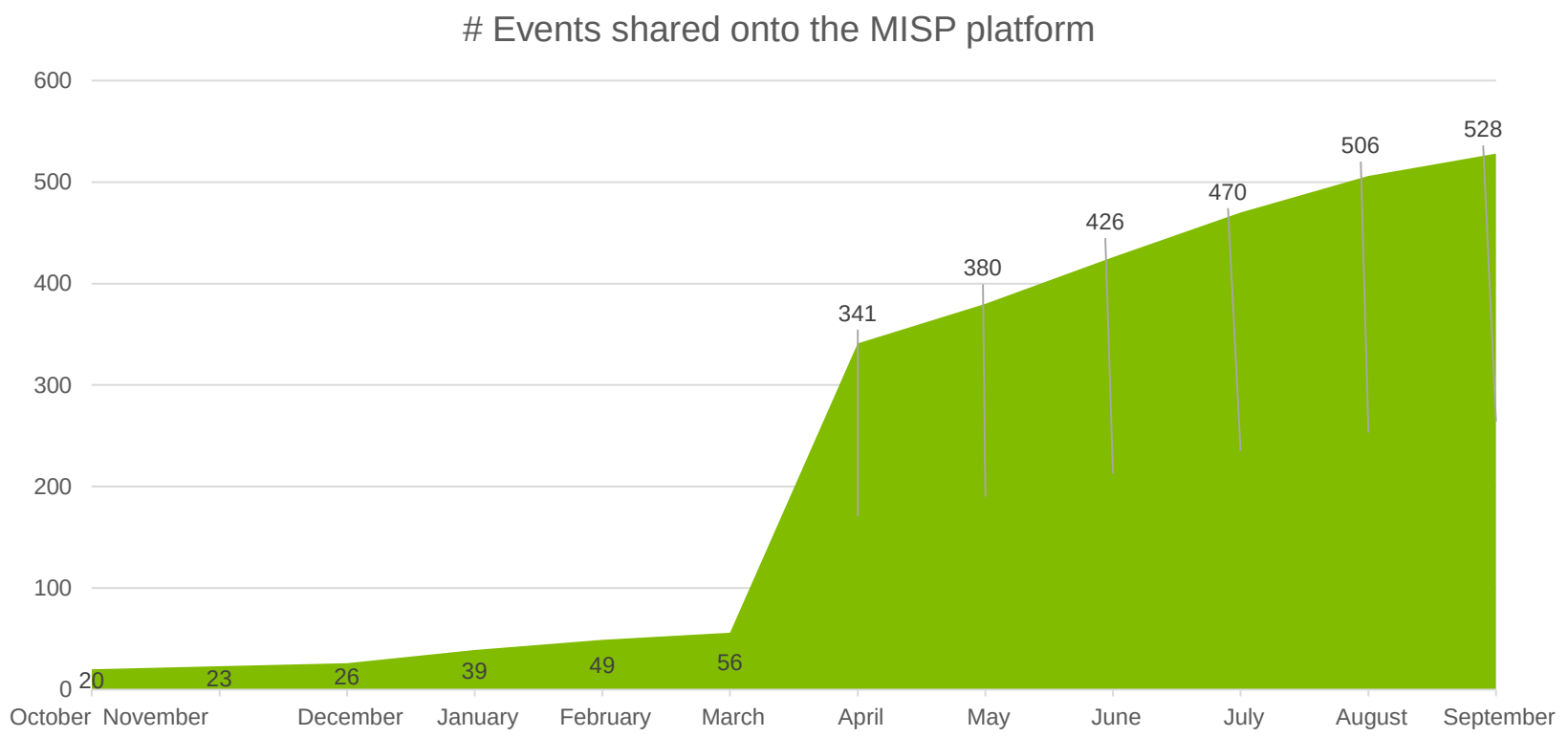




Research Results - Key lessons learned

Ramp-up





Important for success

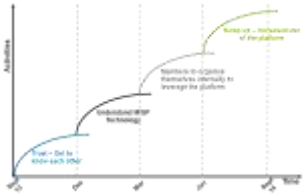
NOT VOLUME OF DATA

but

QUALITY OF INFORMATION

Don’t expect high data volume – start small

Research Results
Conclusions



At the end of the first year of CTIRP, **the key achievements** of the Community are:

- Central and secure ability to **share information**
- Established **trust** in a unique blend of public and private, cross-sector Community members.
- **Sharing of best practices, concerns, discussion items** by members themselves
- **Documented outcomes** usable for internal awareness on CTI

We are committed **to continuing this research project** to further grow the community CTI capabilities and **further capitalize on the trust** built within this Community.

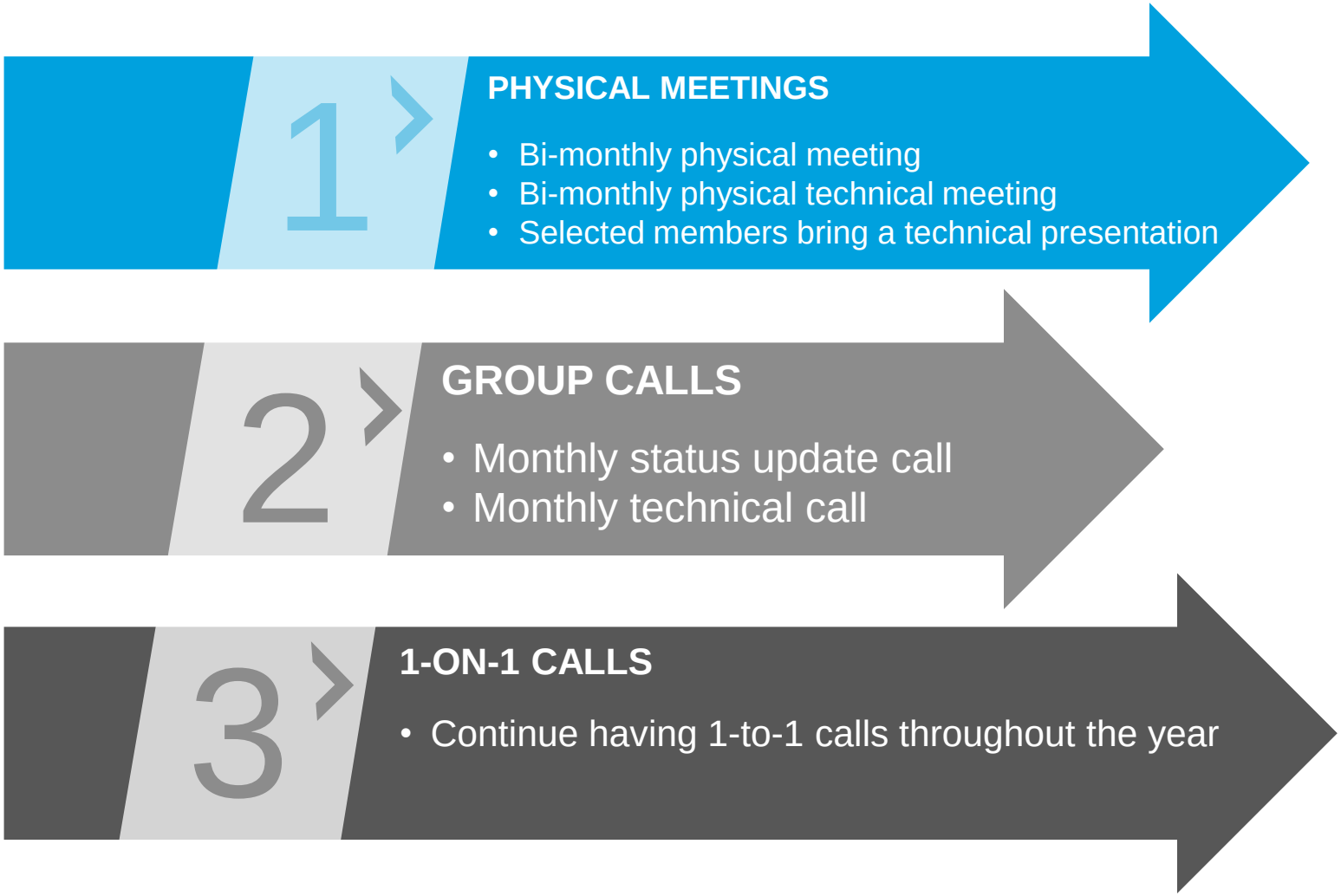
Deloitte.

Moving into the second year of the project

Extensions on the objectives

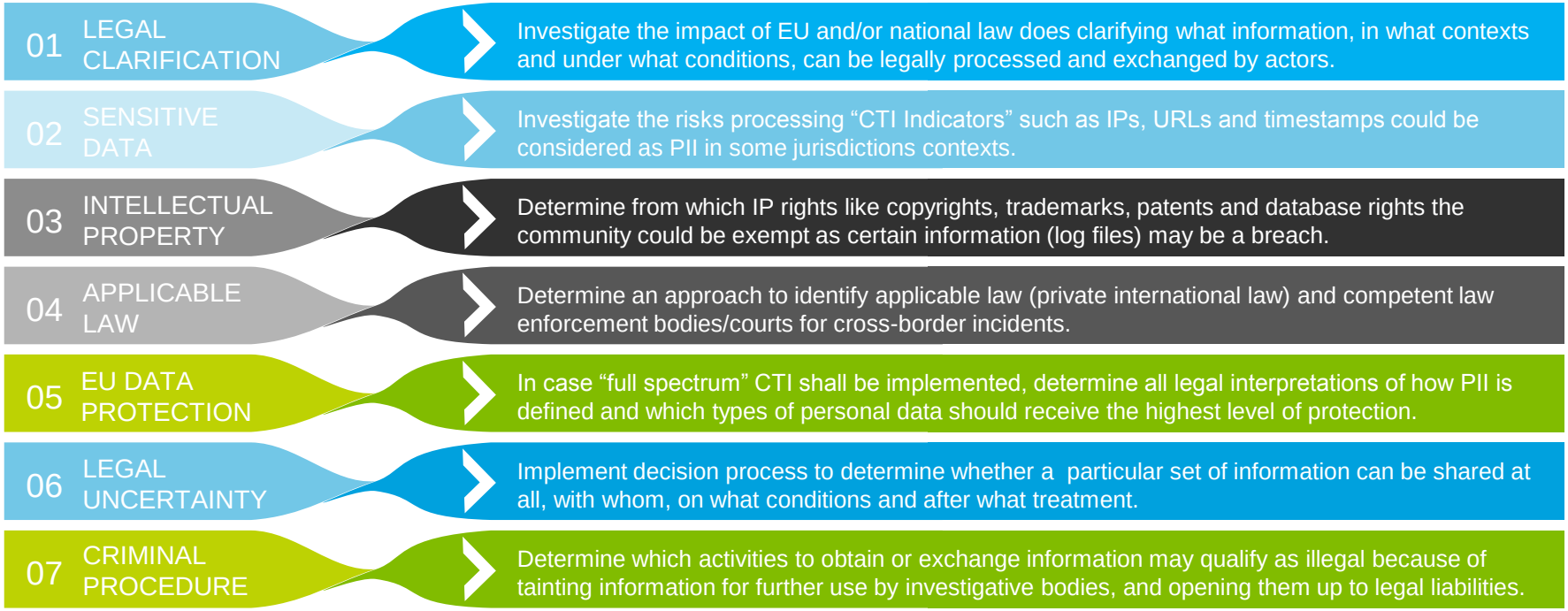
Moving Forward: Research project extension

Enlarge community and optimize communications



Moving Forward: Research project extension

Analyse legal aspects



Moving Forward: Research project extension

CTI scope extension

Moving Forward: Research project extension

MISP

Integration of MISP in project members' infrastructure

- Improve automated exchange

Improve operational use

- Integrate with other security devices
- Improve detection

Critical success factors for this project

Basis for continuation

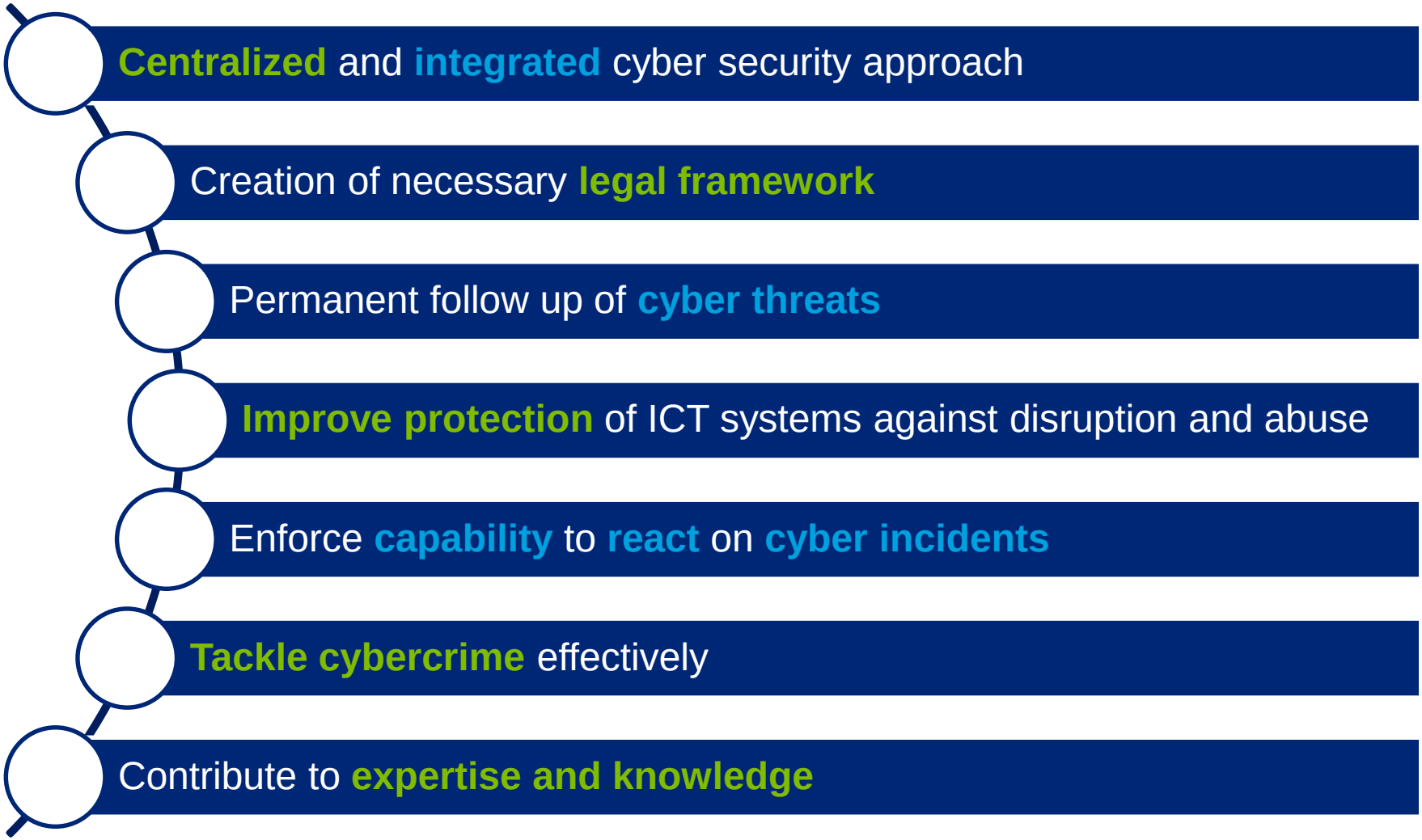
Leveraging Belgium's cyber intelligence capabilities

Need for more information exchange with and within public sector

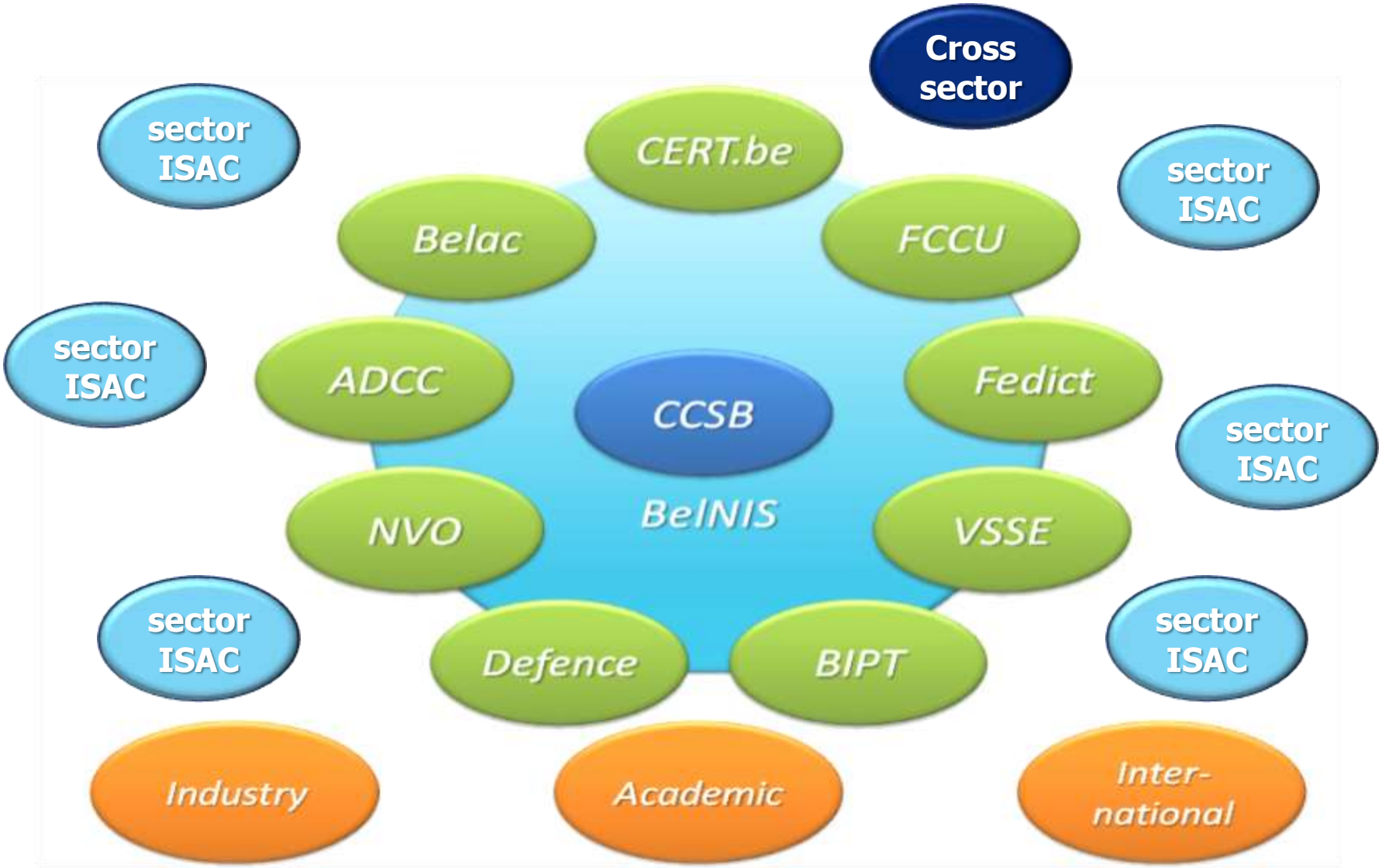
Need for more public private interaction

- Broader public and other organizations also need protection
- Long standing intelligence handling experience of public sector lacks link to private sector
- Government's responsibility to proactively create circumstances for secure critical infrastructures
- Serious cyber incident crisis management Role government – role of private companies

BE National Cyber security strategy
Domains for action



Cyber security center Belgium



How can this project experience help others ?

Experience building trusted community

Community management

Technical guidelines for MISP implementation

Contact details

Luc Beirens
Director

lbeirens@deloitte.com

Deloitte Enterprise Risk Services
Direct: + 32 2 800 22 24
Mobile: + 32 475 36 48 73