From MISP to RISP a keynote on the benefits of collaboration in cybersecurity

François Thill, Director cybersecurity,
Ministry of the Economy.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

Agenda

- Collaboration
- MISP a success story
- Informed governance and RISP

Collaboration

- To collaborate, you must be at least 2
- You must be able to understand each other
- You should have a mutual interest

Alone

- Like a farmer without weather forecast
- You might try to read natural indicators, but still cannot exchange with peers, as there is no common language, no taxonomy

That’s not collaboration

Collaboration

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Immature governmental entity (former times)

- Only has few information as nobody trusts him
- The information he has might be classified and are de facto unusable
- He might even have a very outdated repressive state of mind

That’s not collaboration either

Collaboration

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

The Leitmotiv of our national cyber strategy:

- **Cybersecurity is a collaborative task**, involving governments, companies and individuals.
- For a country building its economic strengths on ICT, **cyber security is an essential asset to its economic attractiveness**.

Collaboration

Examples of effective collaboration:

- Experts groups
- Crisis management, coordination within government
- CERT.lu
- Cooperation in the European context between regulators (NIS, GDPR)
- **MISP** … the basis for mass collaboration and threat intel generation

Malware Information Sharing Platform

- A platform provided in **open source**
- That can be **interconnected**
- With nearly a thousand instances over the world
- Where technical experts agreed upon contextual **taxonomies**
- Where mostly technical experts exchange with their **peers**
- Where the information provider decides about the **outreach**

CIRCL runs 7 MISP platforms

- The private sector MISP connects
  - 1164 entities
  - 2414 users
- The private sector MISP gives access to
  - 22.308 events
  - Described with 5 million attributes

MISP

MISP provides more than purely technical information:

- Events
- Campaigns
- Threat actors

MISP is a valuable source for threat intel, it provides a kind of “cyber weather”

Informed governance

From technical to organizational security

(From MISP to RISP)

From threat intel to risk management in order to **involve the management** and implement **informed governance**

Informed governance

Why is this important?

- **Interdependences** between systems are growing and complex; cyber security is **no more an individual challenge**, there is too much at stake.
- Risk management decisions should be **reliable**, **comparable** and **repeatable.**
- **Risk management decisions** should be taken upon as **FACTUAL INFORMATION** as possible.

- **Collaboration** is a **MUST, common taxonomies are required**
- **Coordinated guidance** is needed.

Risk management - **governance choices**:

- Primary assets (scope)?
- Risk scenarios (granularity)?
- Qualification of impacts?
- Qualification of threats?
- Qualification of vulnerabilities?
- Risk treatment decisions?
- Effectiveness of risk treatment measures?
- Risk acceptance matrix?

Informed governance

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Primary assets (scope)
- Risk scenarios (granularity)
- Qualification of impacts
- Qualification of threats
- Qualification of vulnerabilities
- Risk treatment decisions
- Effectiveness of risk treatment measures
- Risk acceptance matrix

How to choose relevant **risk scenarios**?

- The most frequent incidents in SME can be described by **42 scenarios** (CASES Diagnostic)
- **CERTs** and **SOCs** often know the scenarios that led to incidents.
- **Regulators** already have or will have this information (breach and incident notification)
- **ENISA** and other's threat landscapes
- **Specialised security companies** have a lot of experience
- Creation of **sectorial ISAC**

SHARE this most valuable information for the sake of all

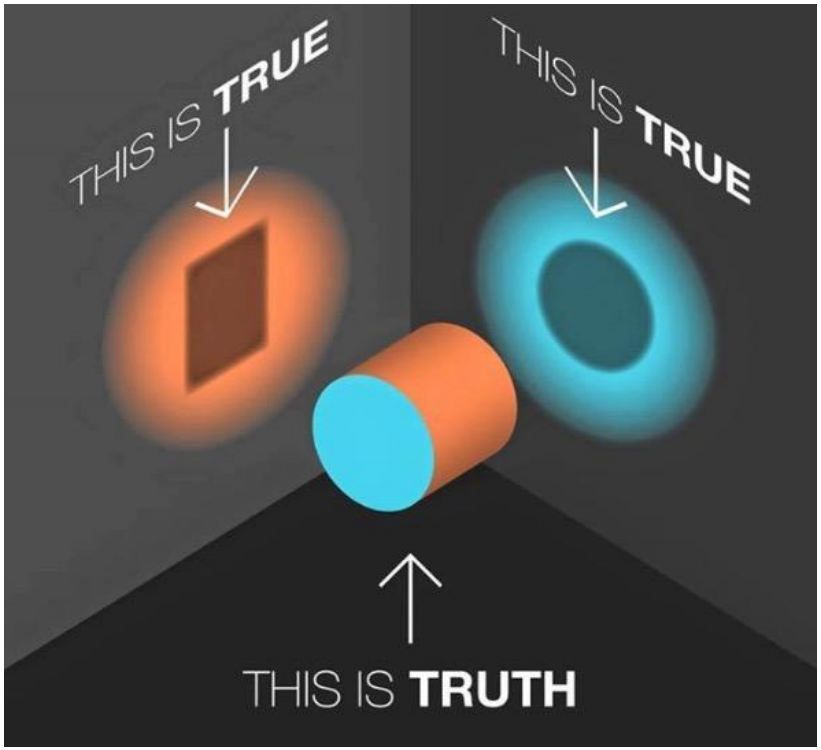
Informed governance

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Primary assets (scope)
- Risk scenarios (granularity)
- Qualification of impacts
- Qualification of threats
- Qualification of vulnerabilities
- Risk treatment decisions
- Effectiveness of risk treatment measures
- Risk acceptance matrix

How to choose qualification of **impact(s)?**

- For yourselves
- For data subjects
- For your customers



Maggie Hos-McGrane

Informed governance

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

How to **qualify threats**, **vulnerabilities** and **effectiveness** of treatments?

- Projects like MISP*, AIL**, D4***, BGPRanking**** generate intel
- **ENISA** and other threat landscapes
- **SOCs** and **specialised security companies** have a lot of experience

*: MISP - https://www.circl.lu/services/misp-malware-information-sharing-platform/
** AIL: https://www.circl.lu/services/ail-training-materials/
*** D4: https://d4-project.org/
****: BGPRanking: https://www.circl.lu/projects/bgpranking/

Informed governance

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Informed governance based upon collaboration provides

- Primary assets (scope)?
- Risk scenarios (granularity)
- Qualification of impacts?
- Qualification of threats
- Qualification of vulnerabilities
- Risk treatment decisions?
- Effectiveness of risk treatment measures
- Risk acceptance matrix?

Collection of frequent incidents provided by SA & ISAC & RISP

Information provided by Situational Awareness, ISAC and RISP

Informed governance in regulation

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- **International collaboration of regulators**
  - GDPR: CNPD – EDPB
  - NIS: ILR – European collaboration group
- **Transversal collaboration of regulators**
- **Regulators giving guidance**

Informed governance in regulation

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Informed governance based upon collaboration and involvement of regulators

- Primary assets (scope)
- Risk scenarios (granularity)
- Qualification of impacts
- Qualification of threats
- Qualification of vulnerabilities
- Risk treatment decisions?
- Effectiveness of risk treatment measures
- Risk acceptance matrix

Regulator

By the community

LUXEMBOURG

LET'S MAKE IT HAPPEN

LET'S MAKE IT HAPPEN