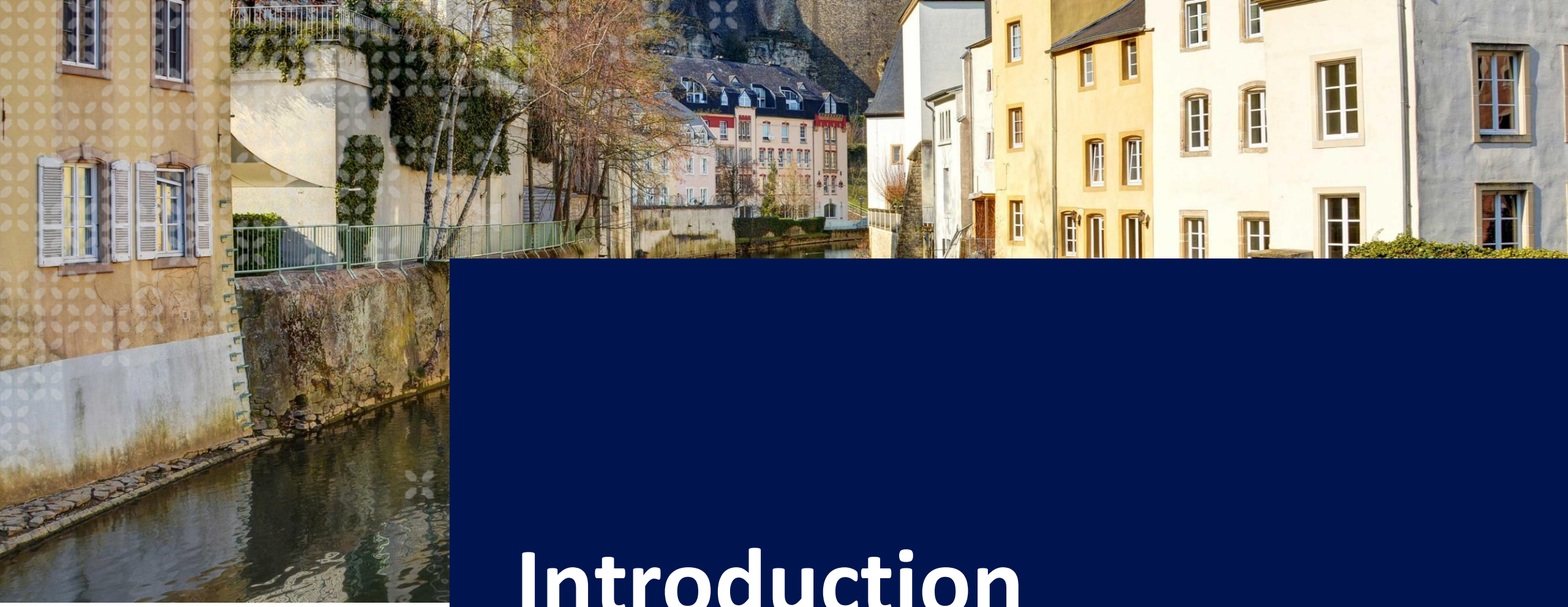
The trajectory to the Luxembourg House of Cybersecurity OSPO and open Data Space

December 2024

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

Agenda

- Introduction
- Approach in Cybersecurity
- Today’s challenges
- Radically increasing the scope



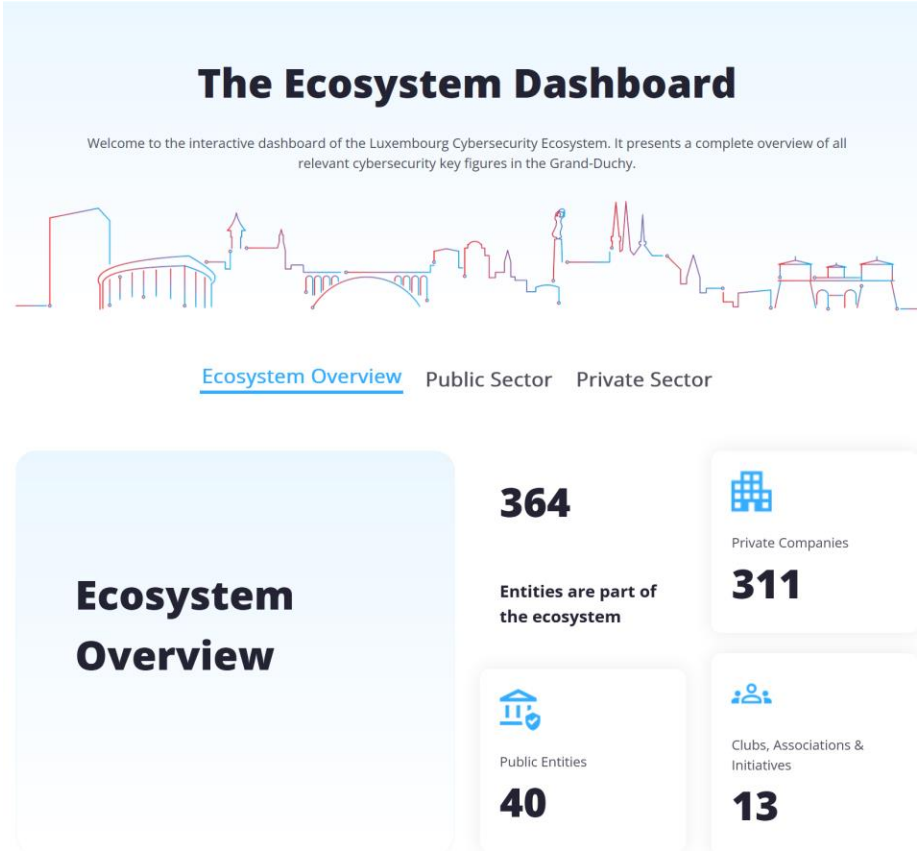
Introduction

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

A mature cybersecurity ecosystem

The Luxembourg cybersecurity ecosystem

- https:///www.cybersecurity.lu
  - 40 public sector actors
  - 311 private sector actors (70 start-ups)
  - 12 CERT federated in https://cert.lu



The trajectory of the ecosystem

The trigger event

- “I love you” virus in 2000

The starting point

- Year 2001 with 25.000 €

The guiding document

- OECD Towards a Culture of Security (25 July 2002)

Multi-country approach “CASES”

- Initiated by BE, followed by LU, DE, IT, CH

The challenge

Over all these years, the challenge stayed the same

- Awareness raising and training
- Capacity building
- National and international collaboration

We still face the same limiting factors

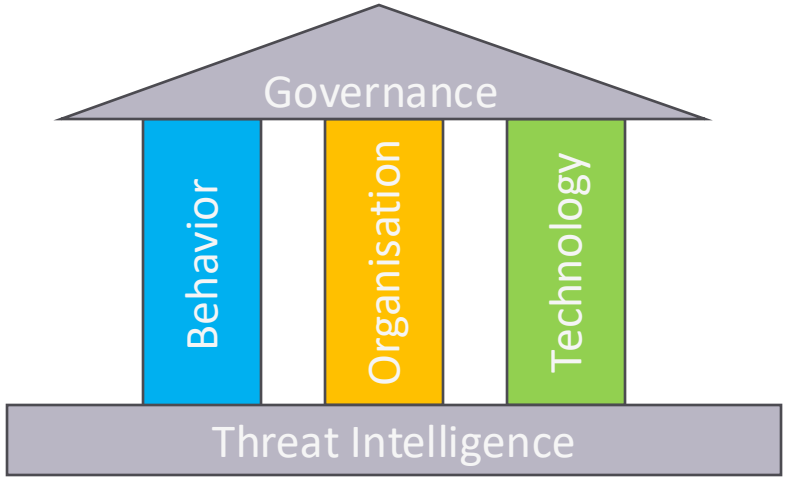
- Lack of skills
- Costs and complexity of cybersecurity solutions
- “secrecy” around incidents, vulnerabilities and threats
- Waste of talents due to unwillingness or incapacity to share threat intelligence resulting in parallel investigation of same threats

Approach in Cybersecurity

The three pillars of cybersecurity are linked

Since 2001, we are facing the same challenges in

- Gathering threat intelligence,
- translating threat intelligence into awareness raising messages,
- translating threat intelligence into risk management information,
- feeding threat intelligence into protection mechanisms,
- finding tools and services that are affordable and manageable.



Definition of the Leitmotiv

In 2014, definition of Leitmotiv in cybersecurity

- Cybersecurity is a **factor of economic attractiveness**
- Cybersecurity is **discriminatory in terms of costs and complexity**
- Cybersecurity is **highly collaborative**

Today’s challenges

The real challenges

- **Industrialisation of threats**
- **Principle of anybody against anybody** (plausible deniability)
- **Monocultures of systems** (“class break” – Bruce Schneier)
- **Oligopoly of threat intelligence providers** (market failure, bias?)
- **80% of the value chain is badly protected** (mostly SME)
- **Regulation risks to eject these from the ecosystem**
- **No economy will survive the next all-out cyber war**
- **…**

Seller’s market

Cybersecurity market is a seller’s market

- We are facing market failures related to threat intelligence.
- We are more and more facing a seller's market where the demand in services is much higher than the offer and where abusive service pricing is appearing.
- The consequence of this development is that cybersecurity companies are having a hard time servicing the needs of the big companies and that 80% of the market, the SME, are fully excluded. This already has large impacts on the economy, only think about our complex supply and vale chains.

Radically increasing our scope

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

Current scope

Open-source tools developed

- 19 large projects: https://code.lhc.lu//projects/ all on github
- 2,5 Petabyte of structured and unstructured data (CIRCL » Open Data at CIRCL)
- Interoperability between datasets (CIRCL » CIRCL Taxonomy)

We are fostering national and international collaboration and promote capitalizing on synergies in threat intelligence, risk management and governance.

The priority is early warning, incident response, informed governance as well as capacity building of similar teams.

Enlarging the scope

Cybersecurity must become an open data economy

- Creation of the **first open cybersecurity data space**
  - Access with “legitimate interest principle” – replication to other data spaces
- **Creation of open-source cloud-based (OpenNebula) tools** for
  - Data collection, Data analysis
  - Collaboration (SOC and CSIRT)
  - End-point protection, Intrusion detection, SOC tools
  - AI tools for chatbots for SME, Taxonomy mappers for Indicators Of Compromise and MISP, AIL geolocalisation
  - AI tools for MITRE Att&ck risk management scenario builders
- Creation of a data marketplace (data exchange for authenticated users)
- Creation of a resource centre – **the cybersecurity OSPO (data, taxonomies, documentation and code)**
- **Creation of a AI factory for cybersecurity (EuroHPC JU call)**
- **Creation of a national multi-tenant SOC (NIS2 and CSoA)** to feed the data space and AI7

Enlarging the scope

We want to create the basis to democratise cybersecurity in terms of complexity and costs through massive and open collaboration by providing data and the basic tools for further innovation and development of applications and services to address the obvious market failures.

- Cross-borer GBER calls for SME with state-aid intensity of up to 80%
  - Cybersecurity tools developed by SME for SME
  - Including AI-based unattended cybersecurity tools for SME (AI factories)
- AI Factory for cybersecurity at Luxembourg House of Cybersecurity
- Creating solutions on top of the Luxembourg OSPO code and data (DEP)
- Multiple like-minded countries propose joint-actions to the ECCC
  - Co-financing by the ECCC up to 50% and up to additional 30% by countries

Proof of commitment

- **Luxembourg national cybersecurity strategy IV (2021-2025)(*)**
- **Luxembourg Digital Decade trajectory for cloud, AI and data(**)**
- **AI factory in cybersecurity (EuroHPC JU call)**
- AI strategy (Mai 2025)
- Strategy on data (Mai 2025)
- NIS2 and CSoA multi-tenant National SOC
- Cascading Funding call for SME from ECCC via LHC (LU-CID)
- Joint-actions – ECCC
- DEP cybersecurity calls

(*) https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/strategie-nationale-cybersecurite-4/National-Cybersecurity-Strategy-IV.pdf

(**) https://smc.gouvernement.lu/dam-assets/dossiers/digital-decade/240421-digital-decade-national-strategic-roadmap-for-luxembourg.pdf

Thank you for your attention

François Thill

Director Cybersecurity and Digital technologies

Ministry of the Economy

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