

The background features a light blue field with a fine, repeating pattern of small circles and lines. Overlaid on this are several large, white geometric shapes: a large circle on the right and several angular, polygonal shapes on the left. A red dotted line traces a path through the composition, starting from the bottom left, moving upwards and to the right, then curving around the top right, and finally descending towards the bottom right, passing behind the text.

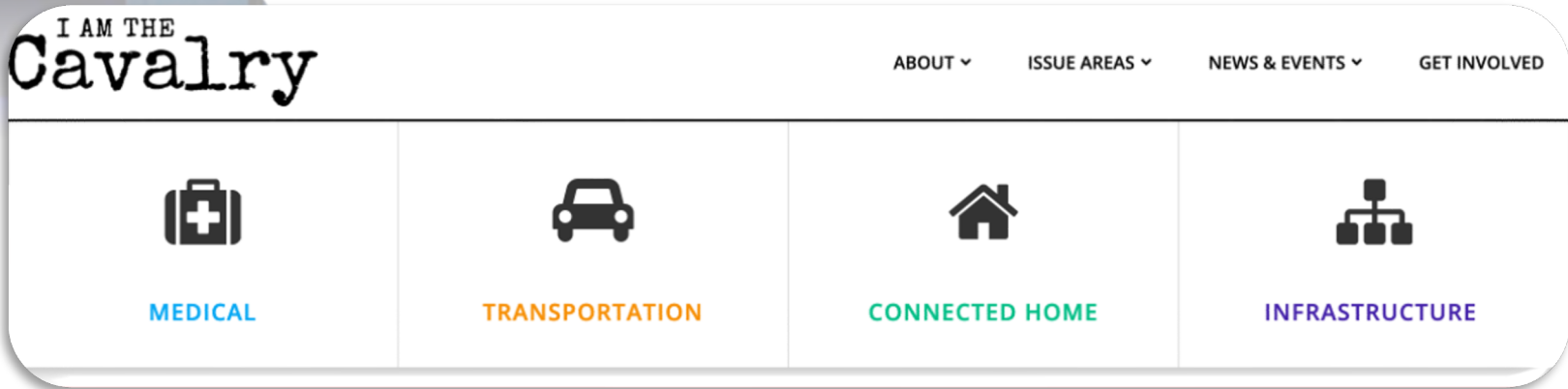
CYBERSECURITY is a team's sport

by Luxembourg House of Cybersecurity

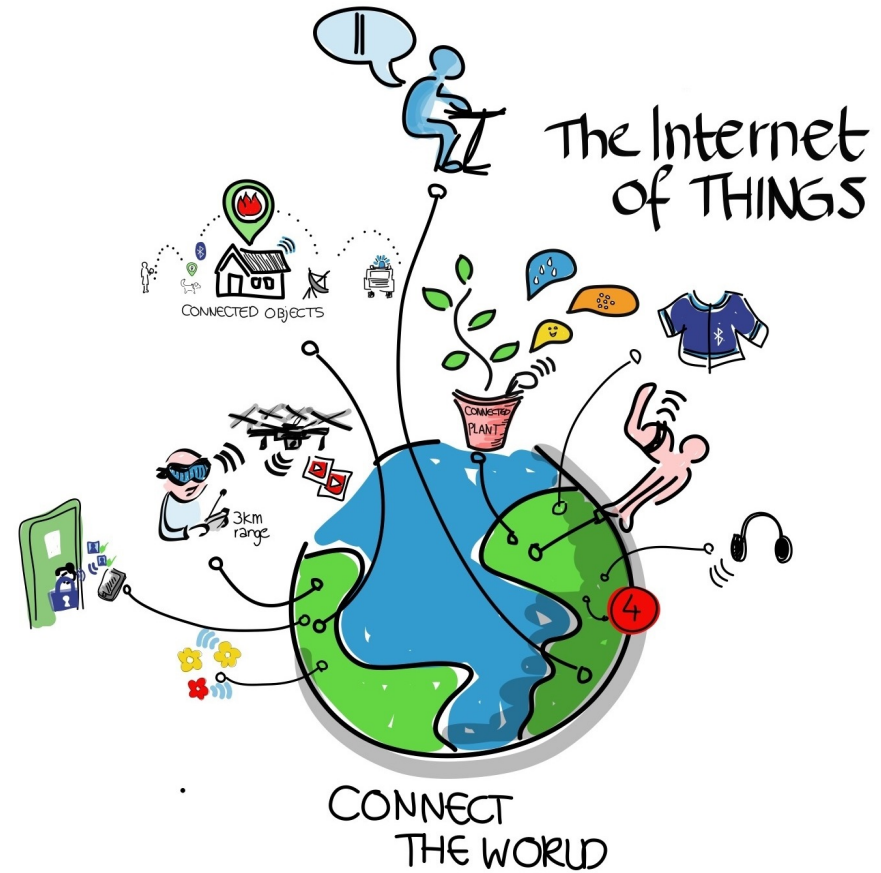
The story of Marie Moe



The story of Marie Moe



Welcome to, the



I AM THE
Cavalry

ABOUT ▾

ISSUE AREAS ▾

NEWS & EVENTS ▾

GET INVOLVED



MEDICAL



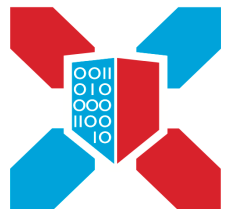
TRANSPORTATION



CONNECTED HOME

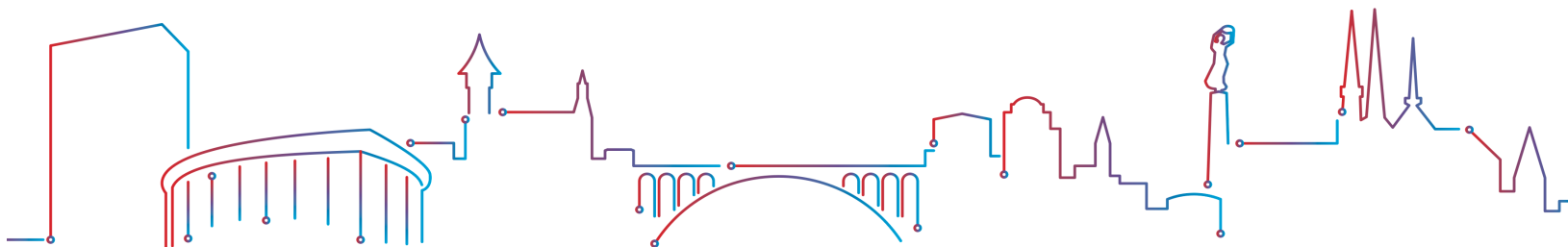


INFRASTRUCTURE

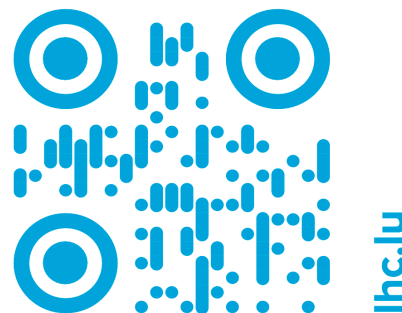


Luxembourg House
of Cybersecurity

THE GATEWAY TO CYBER RESILIENCE



**Luxembourg,
a pioneer in the open
cybersecurity data economy**



lhc.lu

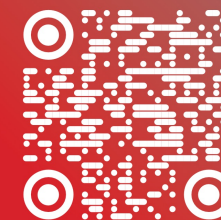
**CYBERSECURITY
LUXEMBOURG**

310+ ACTIVE ACTORS
IN CYBERSECURITY

90+ WITH CYBERSECURITY
AS A CORE BUSINESS

70+ STARTUPS

More about
the ecosystem



The Ecosystem

Ecosystem Overview

366

Entities are part of
the ecosystem



Private Companies

314



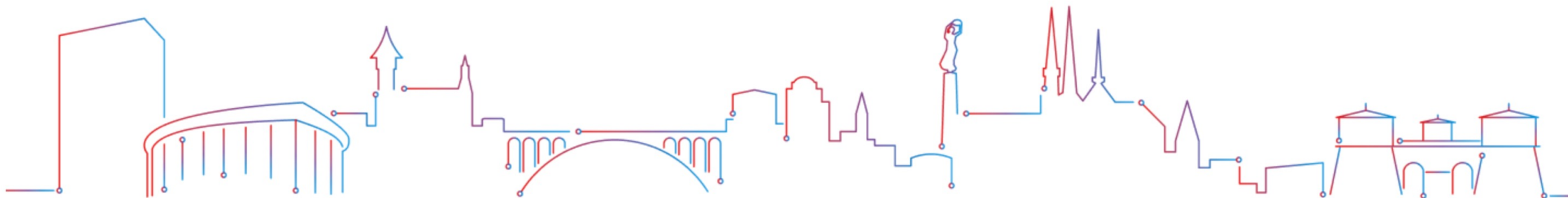
Public Entities

40



Clubs, Associations &
Initiatives

12



314

Companies are part of
the ecosystem

[Access the full list →](#)



Created during the last 5
years

32

Main point of contact

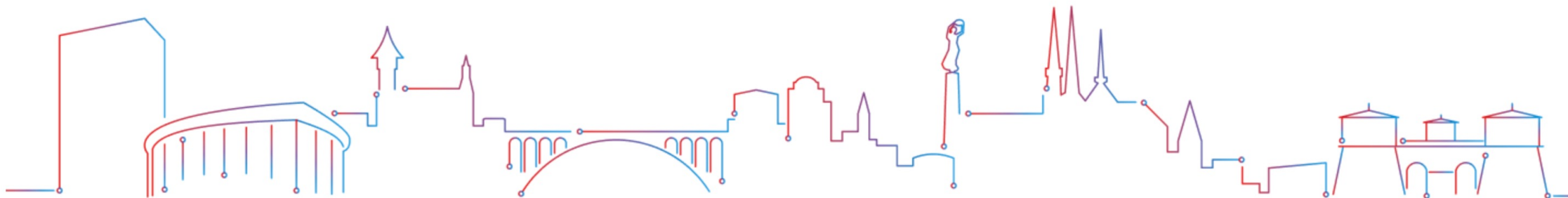
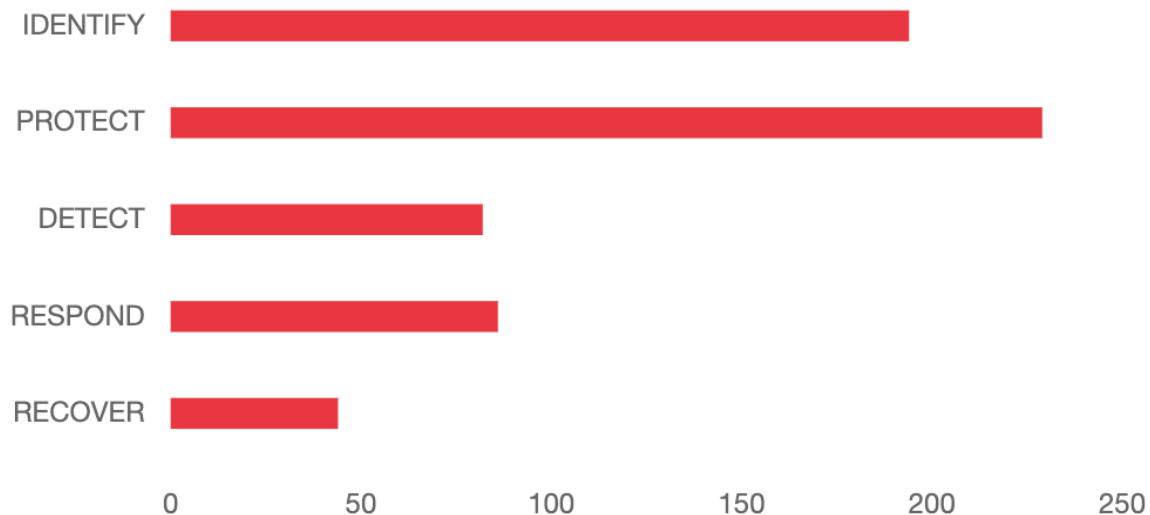


Number of Startups

73

The Ecosystem

Diversified solutions offered by the ecosystem



National cybersecurity Portal



SEARCH

DASHBOARD

LOG IN/REGISTER

IMMEDIATE SUPPORT

The Ecosystem

News & Events

Skills & Jobs

Resources & Support

About

Contact



The national cybersecurity portal, for everyone

All in one place, explore & be a part of this community-driven platform whether you are a seasoned pro or just starting out.

The Ecosystem

How can we help?

<https://cybersecurity.lu>

Latest Alerts

TR-85 - Three vulnerabilities in Cisco ASA software/appliance and FTD software being exploited

See all alerts →



Stay safe online with these Cybersecurity best practices

Cybersecurity essentials



Training on daily work, software, and security

People are often the weakest link in cybersecurity, therefore, knowledge share, awareness-raising is key to fight against the never-ending flow of cybersecurity threats and attacks.



[Read more →](#)



Procedures, rules and user charter

Existence and adherence to clear safety policies and rules are essential for the continuity of an organization's activities.



[Read more →](#)



DDoS Attack

A distributed denial-of-service (DDoS) attack is a cyberattack to disrupt the normal traffic of a targeted server, service or network by overwhelming the target IT infrastructure with a flood of Internet traffic.



[Read more →](#)



Compromised Data

Your data is compromised if your data is accessed, copied, modified, damaged, destroyed, deleted, distributed or transmitted by a third party in any way.



[Read more →](#)



Wireless network



Password

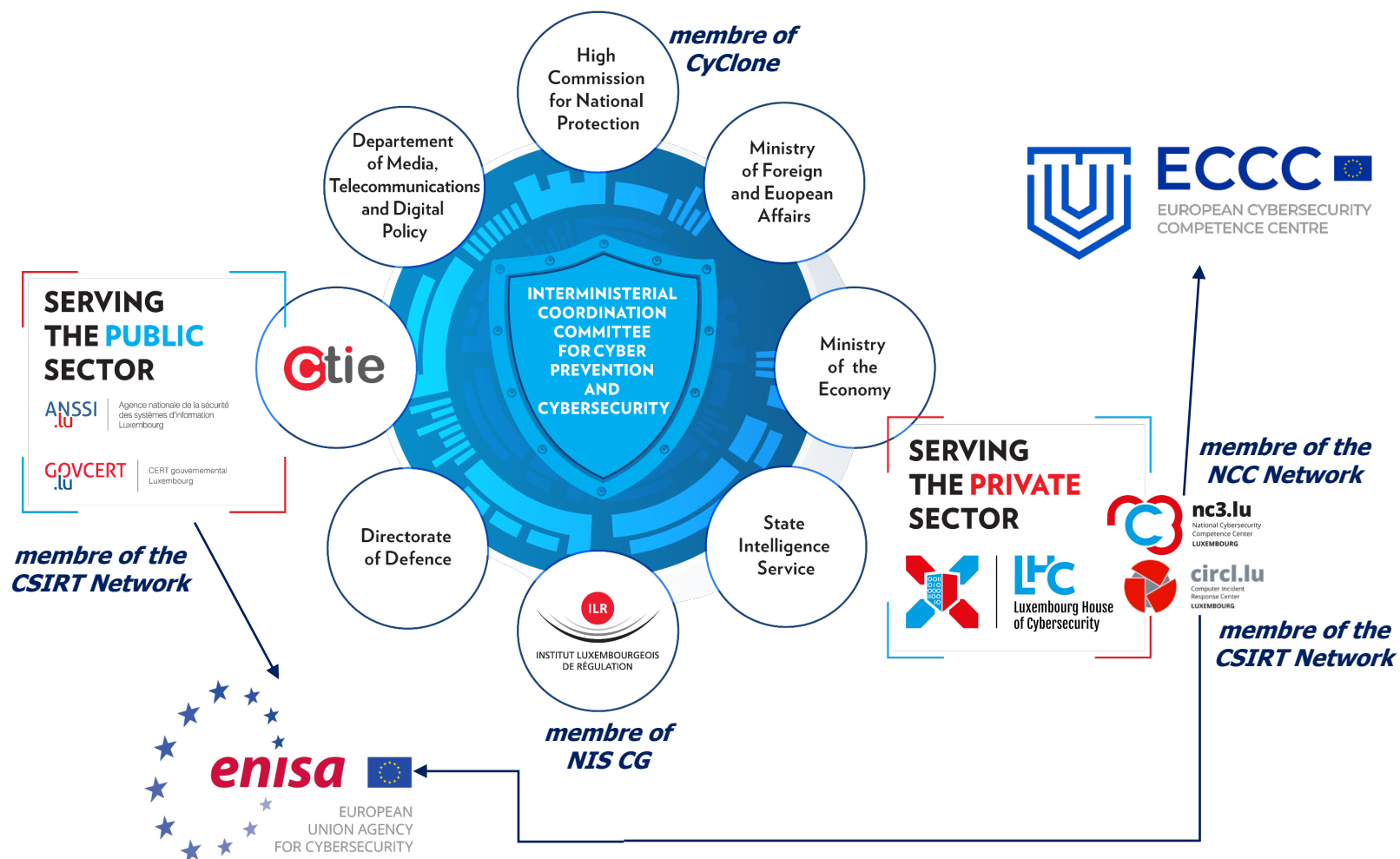


Infected computer



Suspicious e-mail

National Governance



National Strategy

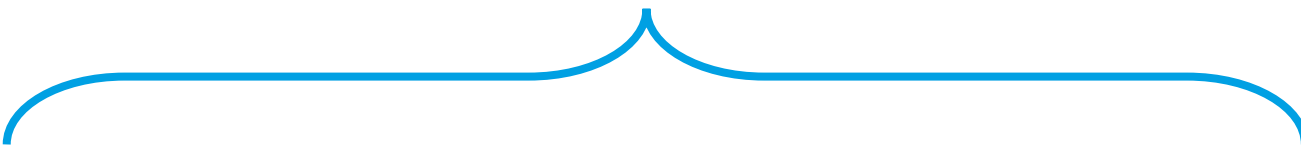
2021-2025

- Objectives
 1. Building trust in the digital world and protection of human rights online
 2. Strengthening the security and resilience of digital infrastructures in Luxembourg
 3. Development of a reliable, sustainable and secure digital economy
- Governance Framework
- Preparedness & Response
- Education and Awareness
- Research & Development





The national cybersecurity brand and ecosystem



Host for all types of cybersecurity-related activities

member of the CSIRT Network

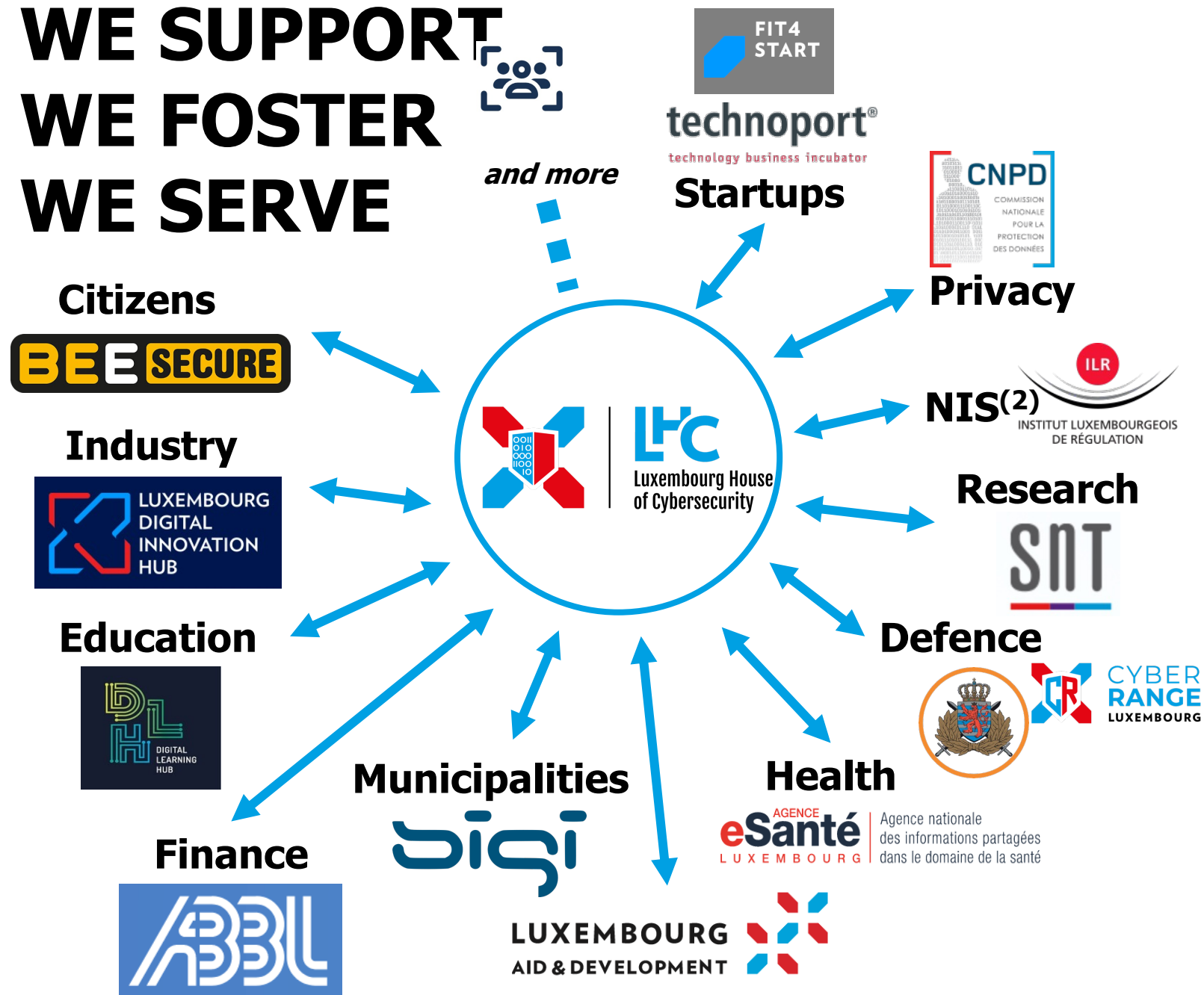
Incident Response & Cyber Threat Intelligence

**Competence & Capacity Building
Research & Innovation
Market Intelligence**



member of the NCC Network

WE SUPPORT WE FOSTER WE SERVE



WE HOST



National Cybersecurity Competence Centre

- Competence and Capabilities Building
- Ecosystem and Industrialisation
- Research, Data and Innovation
- NCC-LU



FIT4CYBERSECURITY - is a self-assessment tool designed for a non-expert audience to estimate in a general way the degree of maturity of its security posture and obtain some basic recommendations.

This tool can be complemented by:

FIT4CONTRACT, to support business owners in verifying if contracts for the procurement of ICT services cover the essential information security aspects.

FIT4PRIVACY, to provide business owners with a good initial overview of their maturity in the field of privacy and data protection (as required by the GDPR).



TESTING PLATFORM - holds the tools and services that will help organisations to perform basic tests on their most commonly exposed infrastructures, starting with email and web servers.



TOP - aims to support its users with evidence-based information on cybersecurity emerging threats, in order to facilitate their decision-making processes regarding the prevention strategies to be undertaken.



TRUST BOX - is the ideal toolset to raise cybersecurity awareness and empower all users with better cyber hygiene.




MONARC - is a tool and a method allowing an optimised, precise and repeatable risk assessment.

Computer Incident Response Center Luxembourg




- CSIRT (Incident Coordination and Incident Handling)
- Cyber Threat Intel and support tools
- CSIRT NIS






CIRCL TYPOSQUATTING
Typosquatting finder

TYPOSQUATTING FINDER is a free and public service to quickly find typosquatted domains to assess if an adversary uses any existing fake domains. You can enter a domain to discover potentially typo-squatted domains. An advanced option allows you to select the algorithms used.




CIRCL LOOKYLOO

LOOKYLOO is a web interface that captures a webpage and then displays a tree of the domains that call each other. Lookyloo can be used to test unknown or potential malicious links safely.



CIRCL PANDORA

PANDORA is an analysis framework to discover if a file is suspicious and conveniently show the results. You can safely use this free online service to review files or documents received by a third party.




CIRCL URL ABUSE

URL ABUSE is a public CIRCL service to review the security of an URL (Internet link). Users regularly encounter links while browsing the Internet or receiving emails. When there are some doubts regarding an URL (e.g. potential phishing attacks or malicious links), users can submit an URL for review, and a take-down process of the fraudulent content is initiated.


More public services are listed on <https://www.circl.lu/services/>

CIRCL ALSO OFFERS ACCESS TO PRIVATE SERVICES OR CLOSED COMMUNITIES:



CIRCL MISP
Threat Sharing

MISP - Open Source Threat Intelligence and Sharing Platform (formerly known as Malware Information Sharing Platform) access is available on request. MISP gives an overview of the current trends of attacks and threat indicators, it is a sharing platform that enables teams to collaborate and provides API access to ingest the information for detection and remediation into the security tools by the organisations.



CIRCL AIL
Analysis of Information Leaks

AIL LEAK DETECTION AIL Project is an open source framework to collect, crawl, dig and analyse unstructured data, like information leaks publicly available on the Internet or Darknet. Organisations in Luxembourg can benefit from the service by being notified based on contextual keyword lists.

Thank you for your attention

Pascal Steichen



LHC

**Luxembourg House
of Cybersecurity**