



---

UNIVERSITÉ DU  
LUXEMBOURG



UNIVERSITÉ DU  
LUXEMBOURG

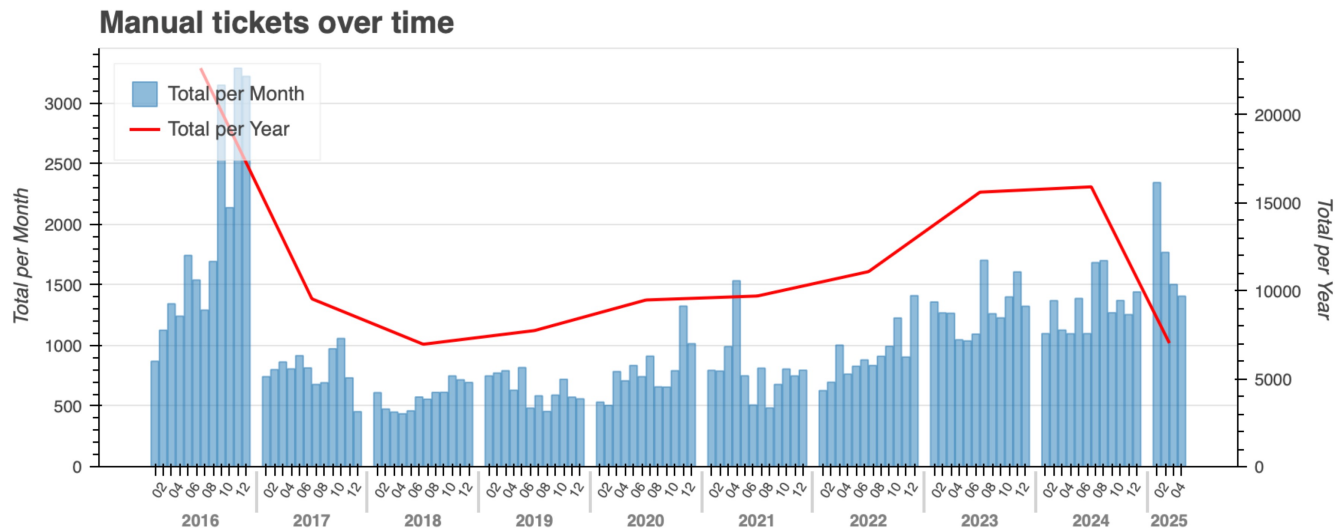
# ***Cybersecurity Landscape & IoT (in-)security***

Master in Technopreneurship

# Threat landscape

2024/2025

# Luxembourg Incidents



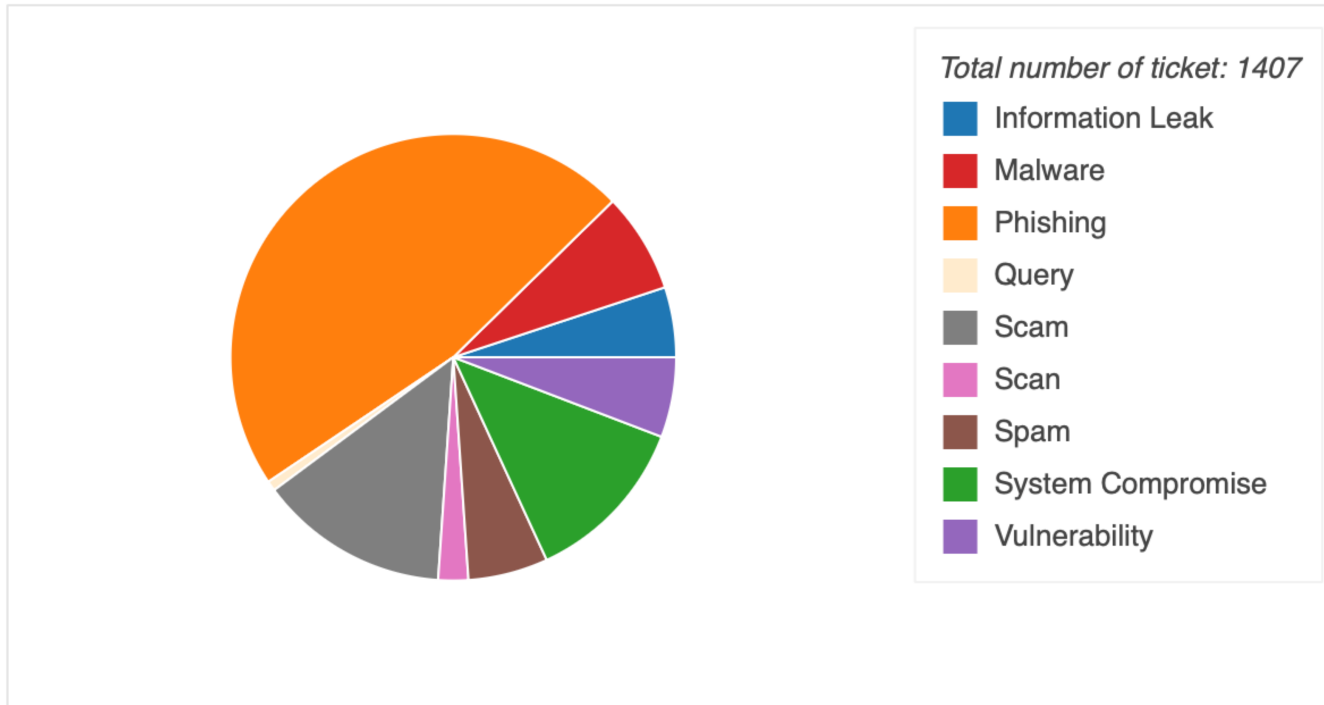
<https://circl.lu/opendata/statistics/>



# Luxembourg

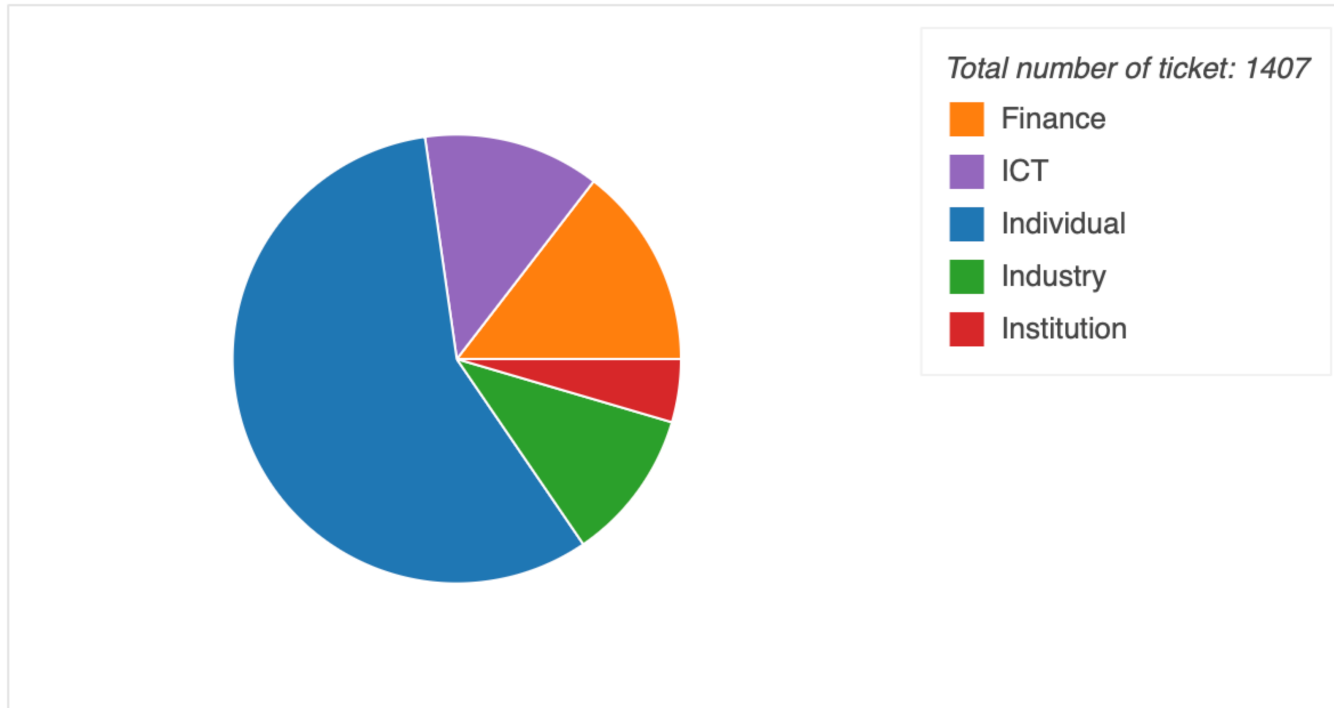
## Incidents Types

### Ticket Classification (2025-04)



# Luxembourg Sectors

## Ticket Sector (2025-04)



<https://circl.lu/opendata/statistics/>

# Threats Observatory Overview



## LATEST THREAT INSIGHTS IN LUXEMBOURG

**Sonicwall CVE-2022-  
22274**  
**9.8 (CRITICAL)**

Most recently exploited CVE  
(from Vulnerability Lookup)

**Technology**  
**(40.83 %)**

Most targeted sector  
(country %, provided by  
Fortiguard)

**44519**

Number of phishing emails  
reported in Luxembourg since  
Jan. 1st 2025  
(provided by SpamBee)

<https://observatory.nc3.lu/>

# Luxembourg Vulnerabilities



## Top 10 most exploited CVEs

What are the CVEs that have been the most exploited over the last month?

### Our analysis

Through several feeds and sources, we have collected data on exposed vulnerabilities that are currently known to be exploited in the wild. The table below covers exploits over the last 30 days.

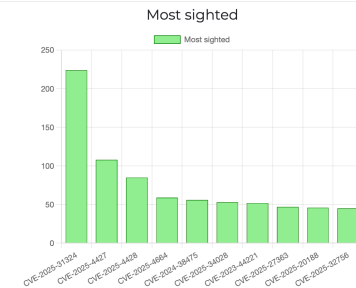
Vendor(s)	CVE	Score	N° of exploitations
✓ Huawei Technologies Co., Ltd.	CVE-2017-77215	8.8 - HIGH	27
✓ SolarWinds	CVE-2024-28995	8.6 - HIGH	27
✓ billion, zyxel	CVE-2017-18368	9.8 - CRITICAL	27
✓ Cisco	CVE-2019-1653	7.5 - HIGH	27
✓ metabase	CVE-2023-38646	9.8 - CRITICAL	27
✓ Apache Software Foundation	CVE-2021-42013	9.8 - CRITICAL	27
✓ dlink	CVE-2015-2051	8.8 - HIGH	27
✓ phpunit_project, oracle	CVE-2017-9841	9.8 - CRITICAL	27
✓ belkin	CVE-2019-12780	9.8 - CRITICAL	27
✓ netgear	CVE-2016-6277	8.8 - HIGH	27

## Top 10 most sighted CVEs

What are the most discussed CVEs over the past month?

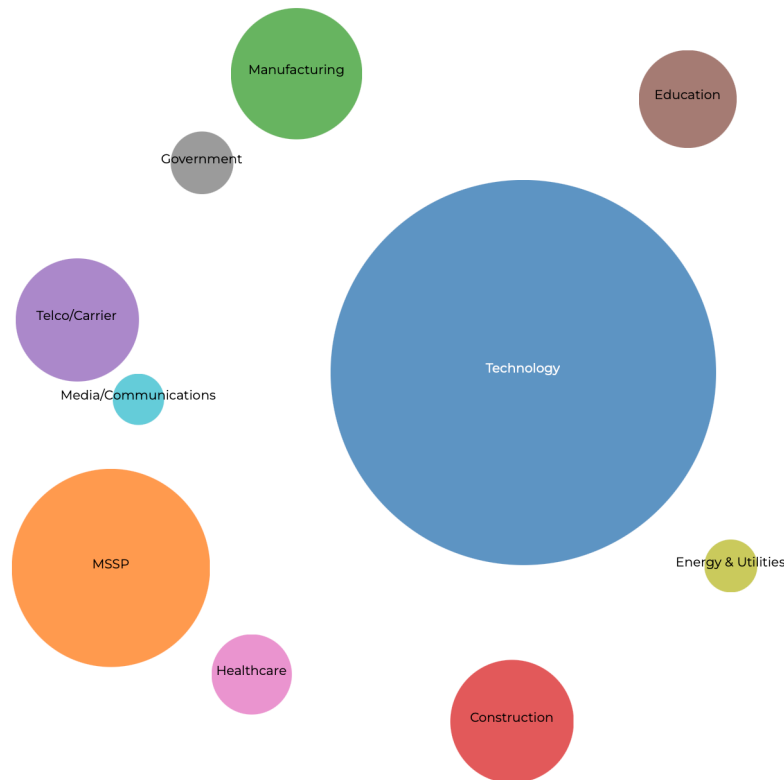
### Our analysis

Through several feeds and sources, we have collected data on vulnerabilities that have been sighted, discussed, updated or mentioned over the last month. You can find out more details on each CVE by clicking the bars in the graph.



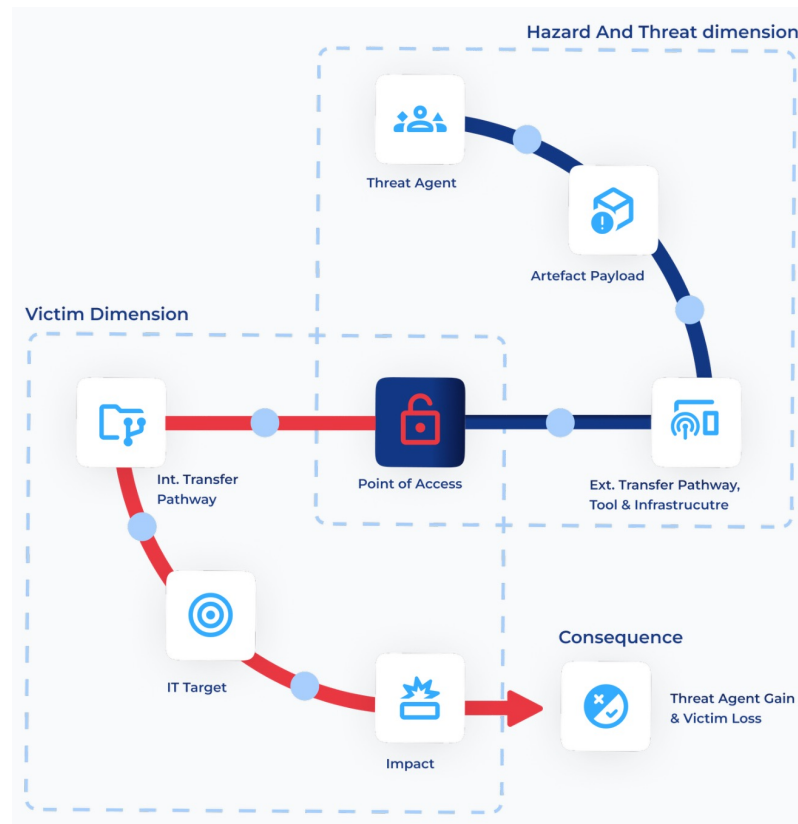
<https://observatory.nc3.lu/threat-observatory/>

# Luxembourg Sectors



<https://observatory.nc3.lu/threat-observatory/>

# Methodology



<https://observatory.nc3.lu/our-methodology/>

# Europe

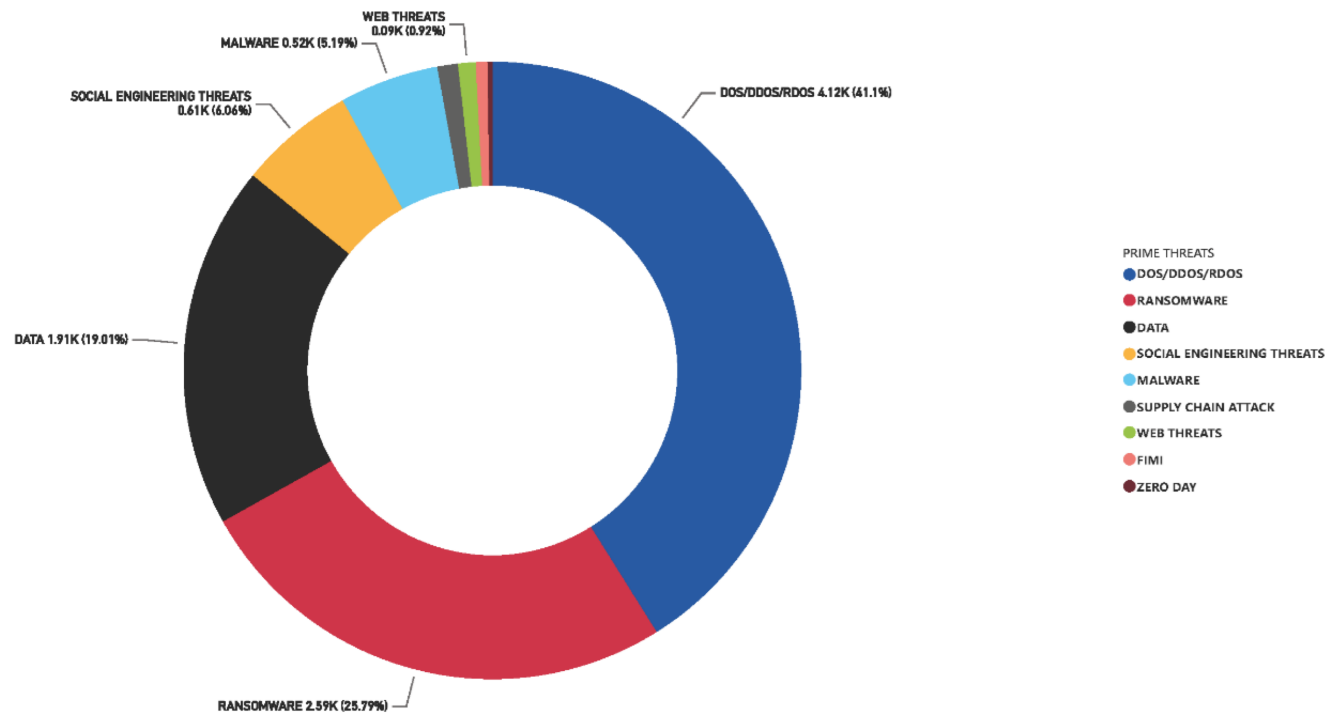
## Top threats, majors trends



<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

# Europe Incidents

Breakdown of analysed incidents by threat type (July 2023 till June 2024)



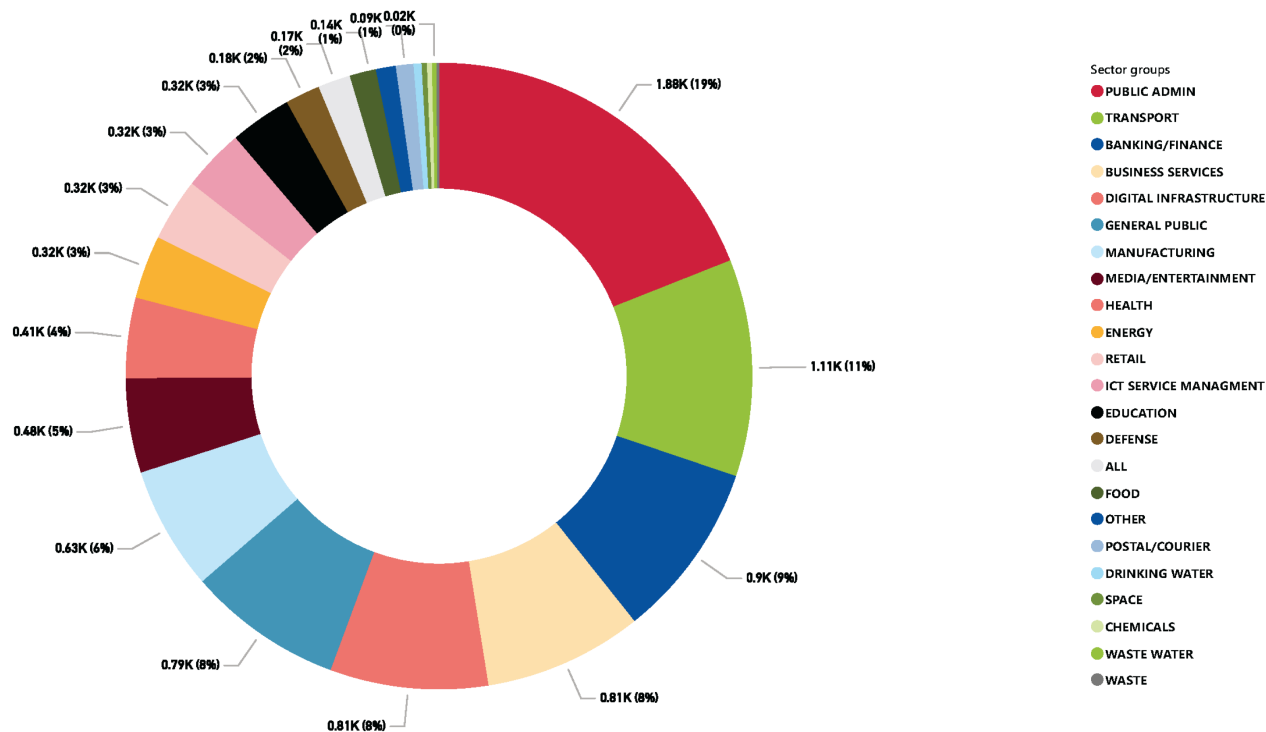
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>





# Europe Sectors

Targeted sectors per number of incidents (July 2023 - June 2024)

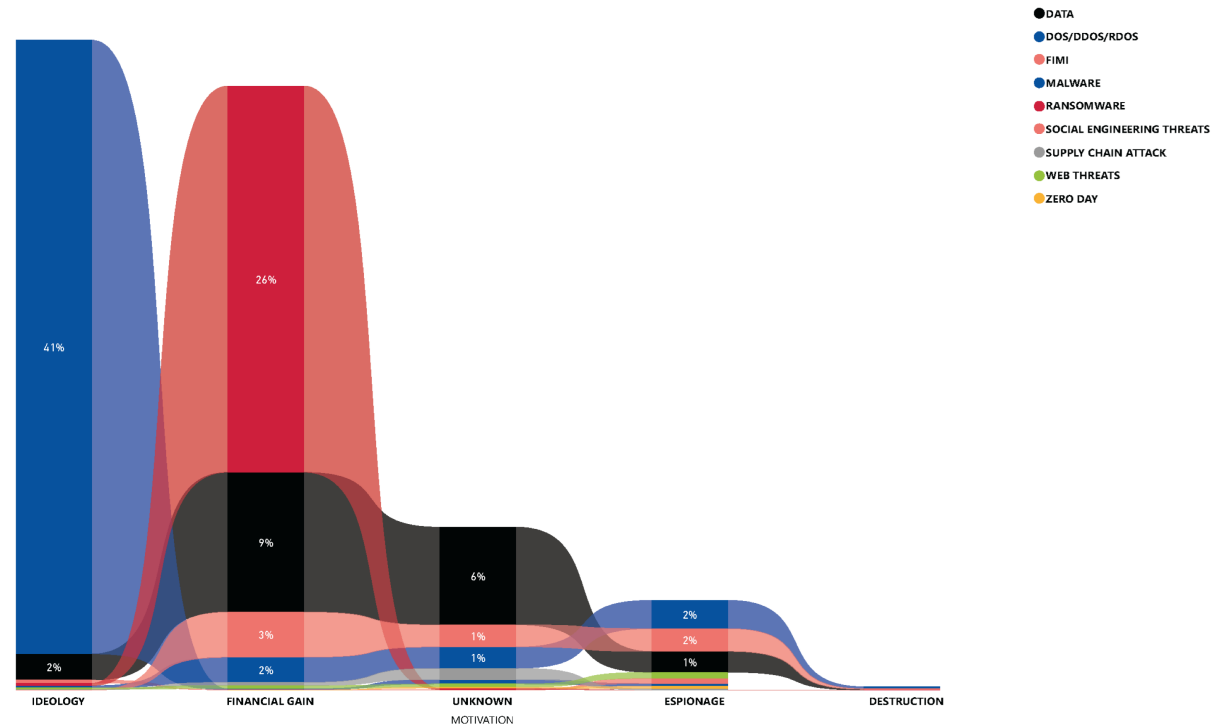


<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

# Europe

## Threat Actor Motivations

Motivation of threat actors per threat category



# International Threat Landscape



**2025 Data Breach  
Investigation Report**



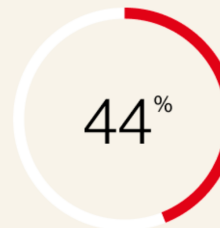
of breaches were linked to third-party involvement, twice as much as last year, and driven in part by vulnerability exploitation and business interruptions



increase in attackers exploiting vulnerabilities to gain initial access and cause security breaches compared to last year's report



of perimeter-device vulnerabilities were fully remediated by organizations in the past year, while almost half remained unresolved



of all breaches analyzed showed ransomware was present, marking a notable rise from last year's report

<https://www.verizon.com/business/resources/reports/dbir/>

## International Threat Landscape

“Pay up or else.”

**\$115,000**

Ransomware attacks can take a costly toll on organizations. The median amount paid to ransomware groups was \$115,000.



But there's good news, too. The majority of victim organizations – 64% – did not pay the ransoms.

**verizon**  
business

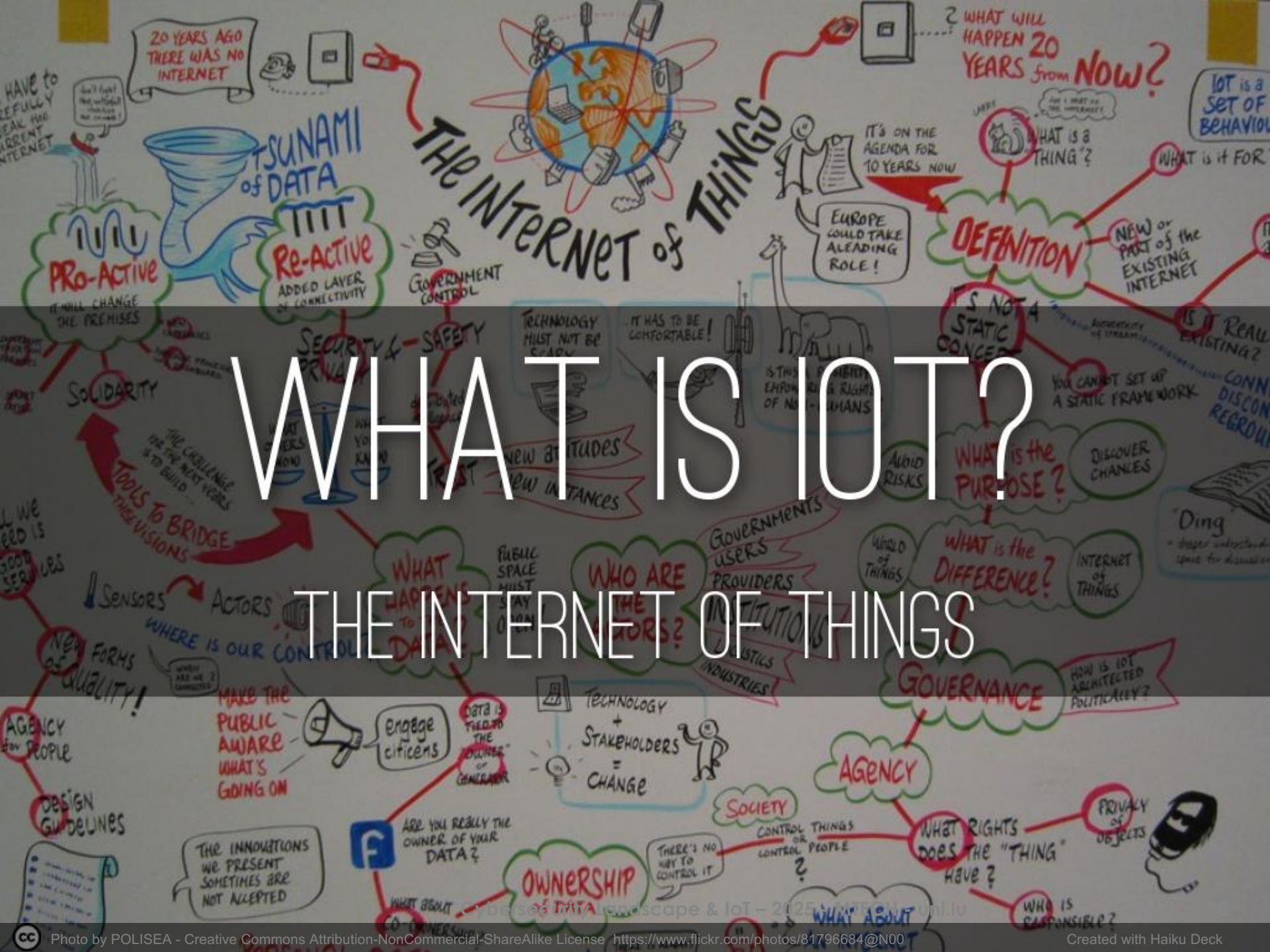
2025 Data Breach  
Investigation Report

<https://www.verizon.com/business/resources/reports/dbir/>

IoT

# WHAT IS IOT?

## THE INTERNET OF THINGS







# TAKE THESE SENSORS, MICRO-CONTROLLERS...



PUT THEM INTO "NORMAL" OBJECTS  
(LIKE UMBRELLAS, DOLLS, FRIDGES, CARS...)







TO MAKE THEM SMART!  
BUT WHAT ABOUT SECURITY?



# MAJOR RISKS OF IOT

- account hijack
- data/privacy abuse
- interception/surveillance
- rogue/“zombie” devices
- supply chain/SDLC compromise
- massive botnets (e.g. DDoS)
- physical attacks
- human casualty

A person stands on the edge of a dark, craggy rock formation. The background is a vast, hazy landscape of rolling hills or mountains under a warm, orange-hued sky, suggesting a sunset or sunrise. The overall mood is contemplative and expansive.

# SOME EXAMPLES





# MIRAI BOTNET

"SMART" CAMERAS



MIRAI SUENAGA

SMART DOLL

DESIGNED BY DANNY CHOO

# CAYLA THE DOLL

## SMART TOY



# BIOTRONIK CARDIOMESSENGER II SMART PACEMAKER



A woman with long red hair, Marie Moe, is speaking on a stage. She is wearing a black jacket over a patterned top. The background is a blue screen with a circuit-like pattern. The text 'HACKING YOURSELF: MARIE MOE AND PACEMAKER SECURITY' and the URL 'HTTPS://YOUTUBE.BE/W1YWpVMpPi8' are overlaid on the image.

# HACKING YOURSELF: MARIE MOE AND PACEMAKER SECURITY

## [HTTPS://YOUTUBE.BE/W1YWpVMpPi8](https://youtube.be/W1YWpVMpPi8)



# RECOMMENDATIONS (USER)

- strong password security
- software/firmware updates
- network segmentation and filtering

- physical security
- check contracts, terms and conditions

- ! if you don't need it don't use it !



**ACCOUNT  
HIJACKING**  
The Digital First Aid Kit



**SECURE  
COMMUNICATION**  
The Digital First Aid Kit



**DDOS  
MITIGATION**  
The Digital First Aid Kit



**MALWARE**  
The Digital First Aid Kit



**LOST & STOLEN  
DEVICES**  
The Digital First Aid Kit

A custom-built electronic device housed in a clear acrylic enclosure. The device features a black printed circuit board (PCB) with various components, including a microcontroller, resistors, and a small display. A black battery pack is connected to the board. A black cable is plugged into a port on the side. The enclosure is secured with clear acrylic panels and metal fasteners. The text "AND LAST BUT NOT LEAST" and "!! IF YOU DON'T NEED IT DON'T USE IT !!" is overlaid on the image.

AND LAST BUT NOT LEAST  
!! IF YOU DON'T NEED IT DON'T USE IT !!



# RECOMMENDATIONS (PROVIDER)

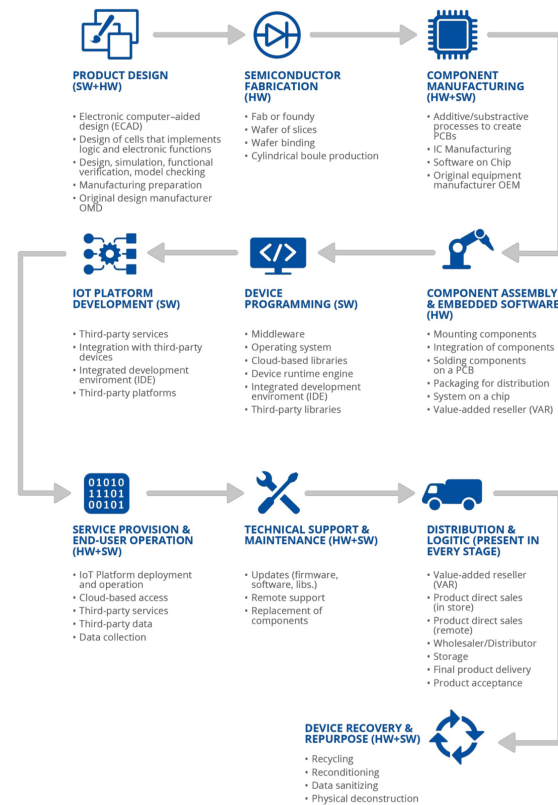


EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

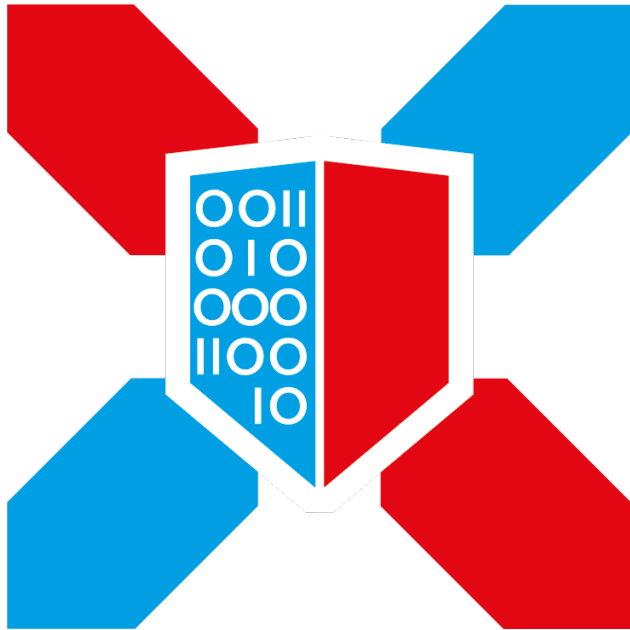
- security by design
- sound data collection/mgmt
- supply chain integrity
- check third party software
- comprehensive testing
- security by default
- sound patch policy and process
- comprehensive documentation



# ENISA reference



<https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>



# CYBERSECURITY LUXEMBOURG

The Luxembourg Cybersecurity Ecosystem

*20 years of creating a culture of security  
for economic and social prosperity*

# WHERE IT ALL STARTED

## “I LOVE YOU” VIRUS (2000)



# TOWARDS A CULTURE OF SECURITY

## OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS (2002)

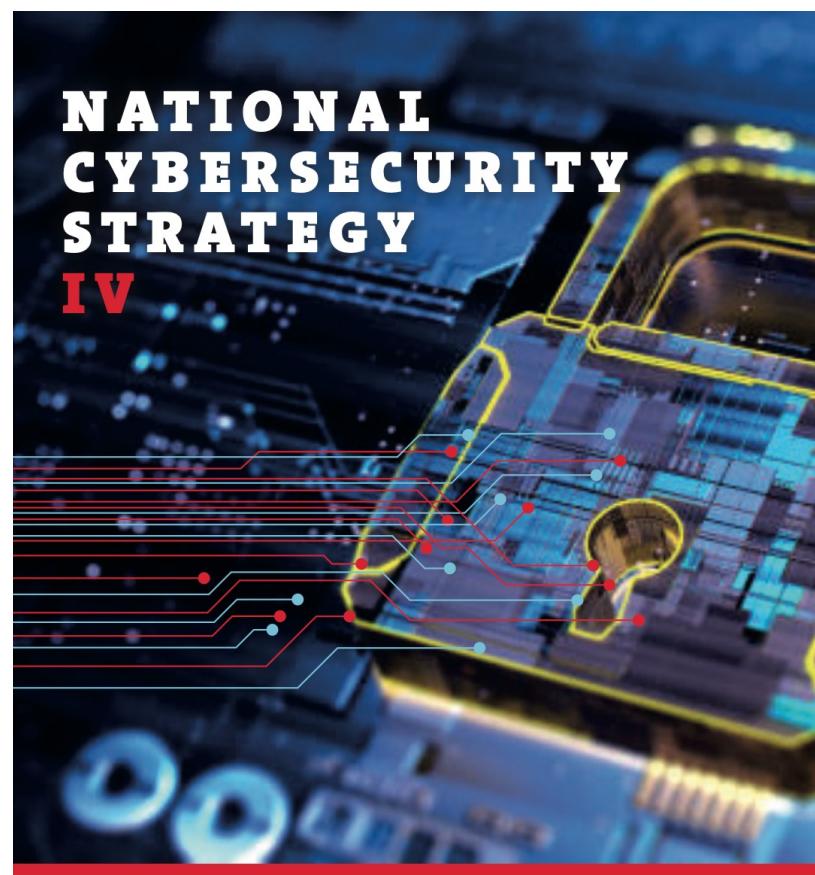


# TODAY

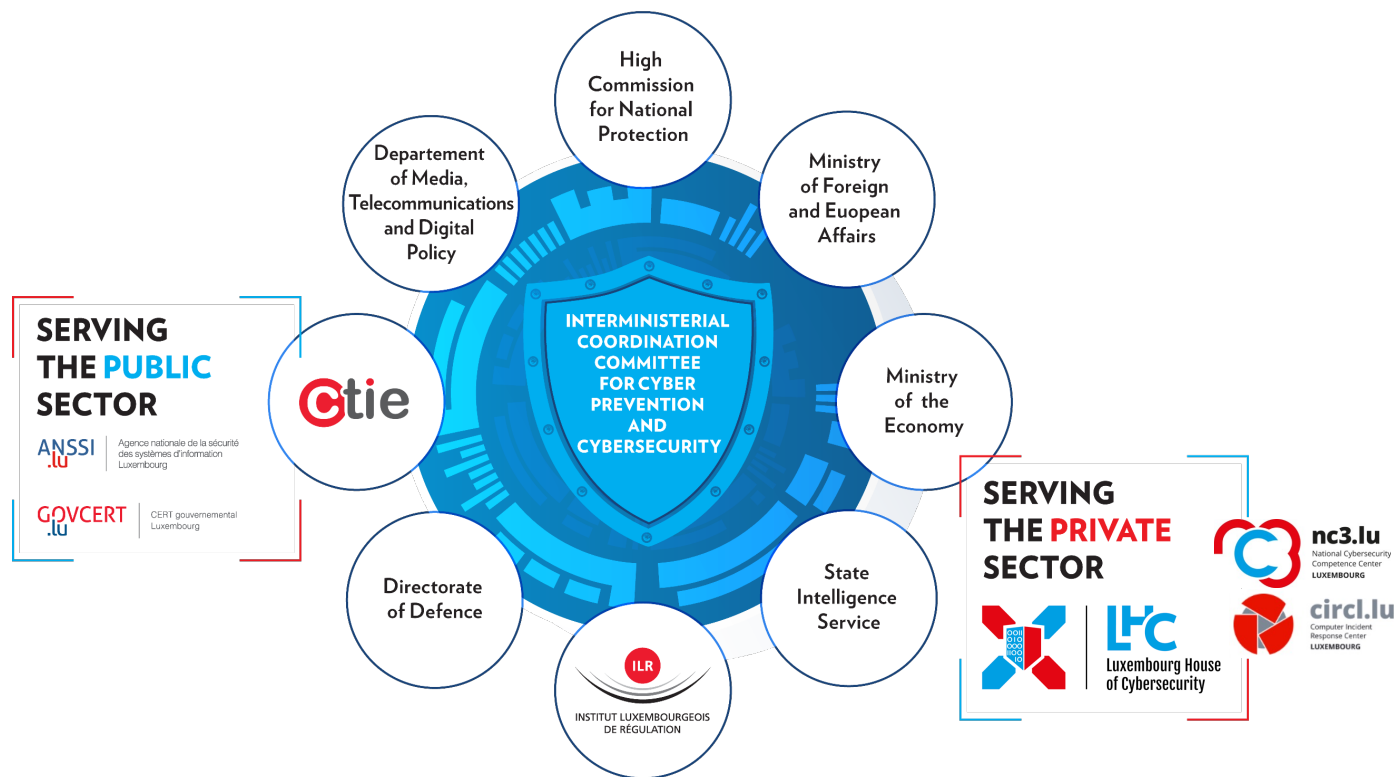


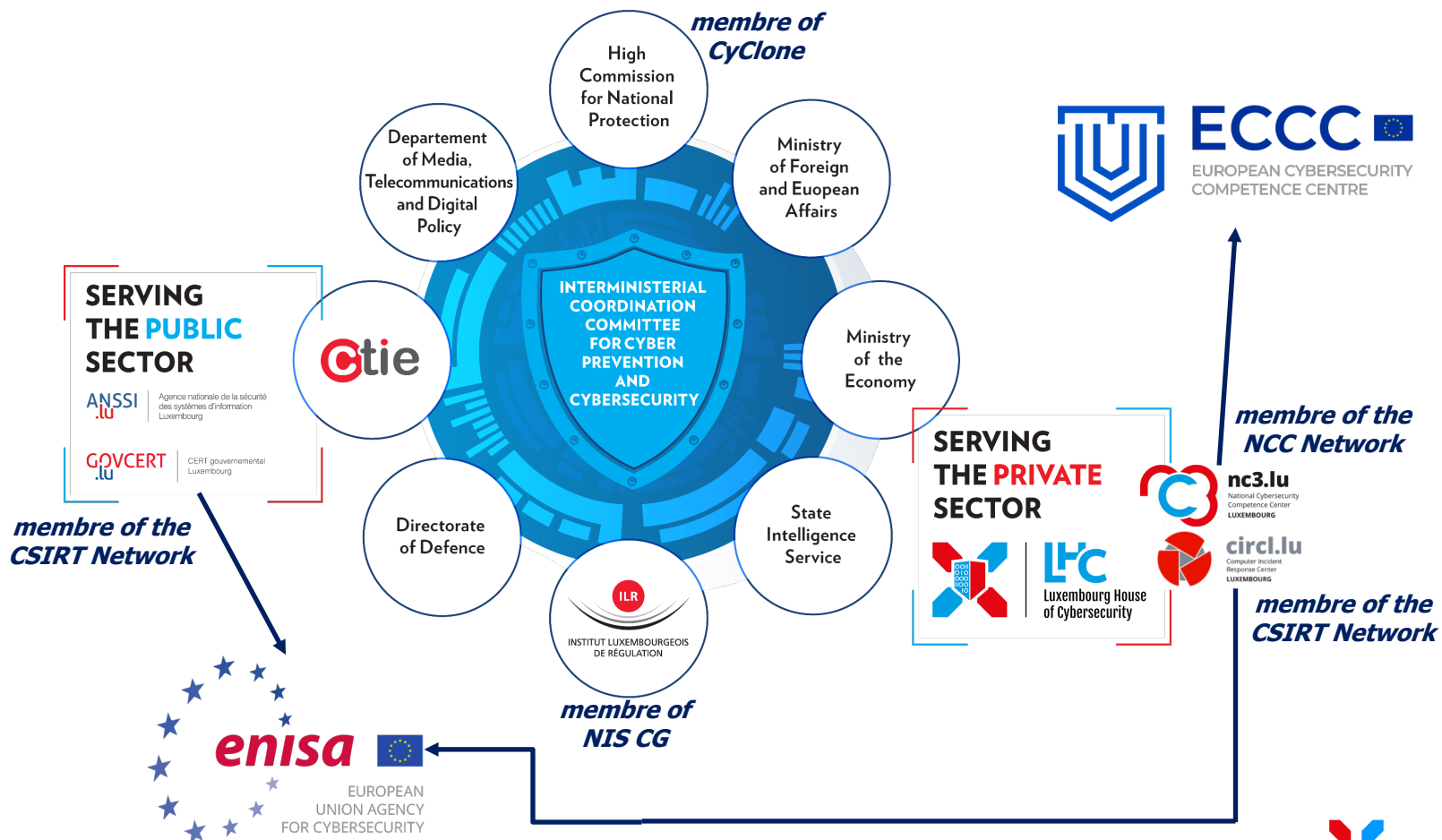
## 2021-2025

- 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



National Cybersecurity Strategy IV





# AUTHORITIES & REGULATORS

- **CER** Critical Entities Resilience  
(loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale – **to update**)
- **GDPR** General Data Protection Regulation  
(loi du 1er août 2018 portant mise en place du régime général sur la protection des données)
- **NIS(2) (DORA)** Network and Information Security  
(loi du 28 mai 2019 portant transposition de la directive NIS – **to update**)
- **PSDC** Prestataires de Services de Dématérialisation ou de Conservation  
(loi du 25 juillet 2015 relative à l'archivage électronique)
- **PSF** Professionnels du Secteur Financier de Support  
(loi modifiée du 5 avril 1993 relative au secteur financier)

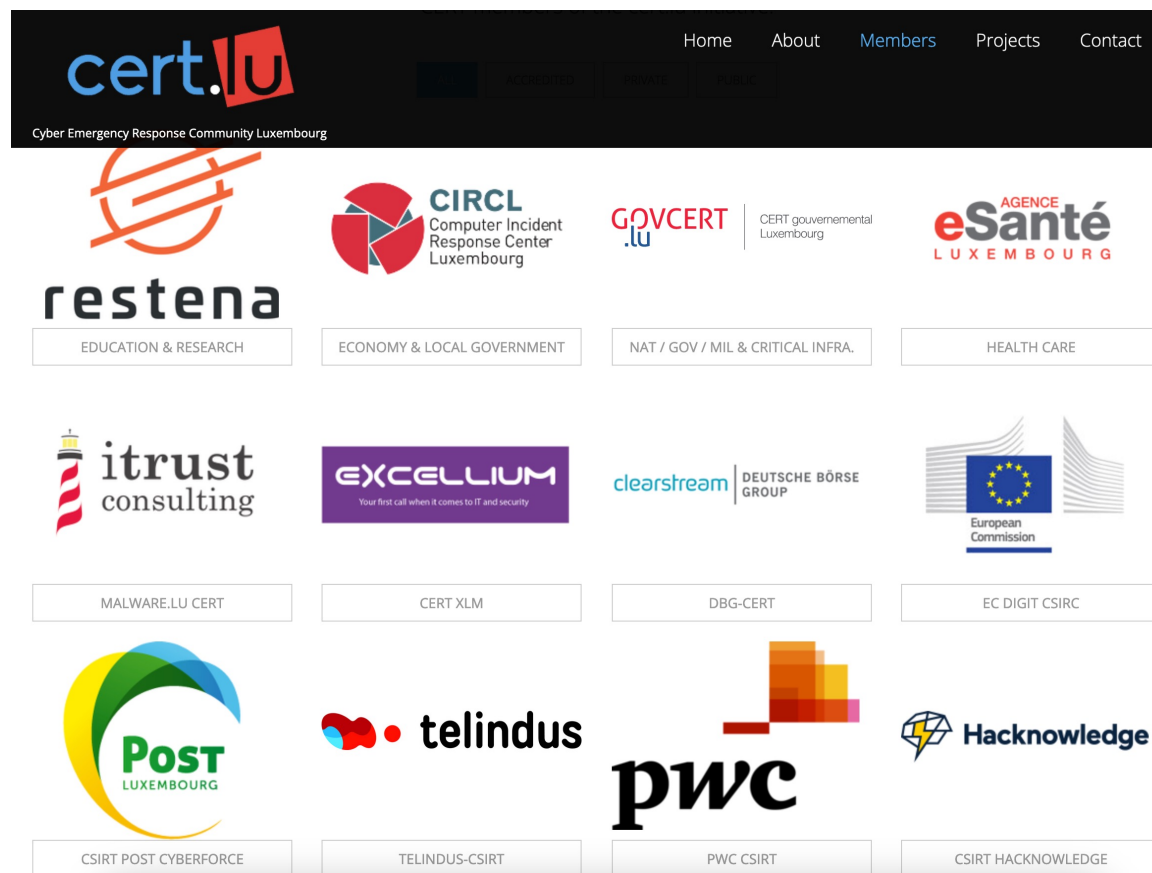


=> more on [cybersecurity.lu](https://cybersecurity.lu)




# PREPAREDNESS & RESPONSE

## PUBLIC-PRIVATE COOPERATION IN ACTION





# PREPAREDNESS & RESPONSE


## PIU CYBER





[Français](#) | [Deutsch](#) | [English](#)


**NUCLEAR  
EMERGENCY**


**VIGILNAT**


**POWER  
CUT**


**CYBER**


**EXTREME  
WEATHER  
CONDITIONS**



**INFLUENZA  
AND  
PANDEMICS**

**EBOLA**

**CBRN**

**FLOODING**

**DRINKING  
WATER**

**LU-CIX**  
DDoS Scrubbing  
Center  
**MASS  
CASUALTIES**



## Education & Research





# Research & Development



LUXEMBOURG  
INSTITUTE OF SCIENCE  
AND TECHNOLOGY



## Competence Hub in Research in Cybersecurity and Cyber Defence



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG  
Ministère des Affaires étrangères  
et européennes, de la Défense, de la  
Coopération et du Commerce extérieur  
Direction de la défense

### Our Funded Chairs

Chair in Capital Markets and Post-Trade

Chair in Cyber Policy

Chair in Digital Procurement

Chair in Entrepreneurship and Innovation

ATOZ Chair in European and International Tax Law

ADA Chair in Financial Law (Inclusive Finance)

Arendt and Elvinger Hoss Prussen Chair in Investment Fund Law

SES Chair in Space, Satellite Communication and Media Law

Chair in Sustainable Finance



## The Ecosystem Dashboard

Welcome to the interactive dashboard of the Luxembourg Cybersecurity Ecosystem. It presents a complete overview of all relevant cybersecurity key figures in the Grand-Duchy.



[Ecosystem Overview](#)

[Public Sector](#)

[Private Sector](#)

### Ecosystem Overview

**369**

Entities are part of  
the ecosystem



Private Companies

**316**



Public Entities

**40**



Clubs, Associations &  
Initiatives

**13**

## Public Sector

40

Institutions are part of the ecosystem

[Access the full list →](#)



Access the latest and upcoming International, European and National Legal Frameworks

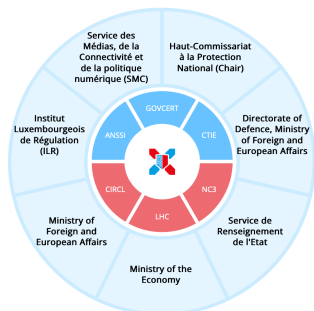
National contact point



[Access the full list →](#)

### A closer look to the national actors

#### National Strategy & Governance



Comité Interministériel en matière de cyber-prévention et de cybersécurité (CIC-CPCS)

[Access the full list →](#)

#### Preparedness & Response



#### Research & Development



#### Education & Training

##### Formal Education



[Access the full list →](#)

##### Initial and Ongoing Training, Re-skilling and Upskilling



[Access the full list →](#)

##### Awareness Raising Activities



[Access the full list →](#)

## Private Sector

316

Companies are part of the ecosystem

[Access the full list →](#)



Created during the last 5 years

30

Main point of contact



Number of Startups

74

### A closer look to the private sector

Companies Start-ups

#### Cybersecurity as core business

Companies have Cybersecurity as their core business

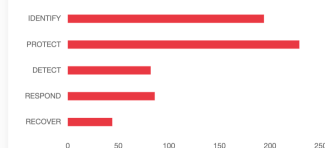
90



ALL COMPANIES COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more →](#)

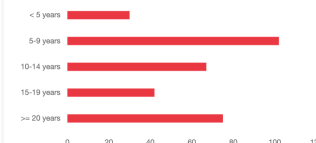
#### Diversified solutions offered by the ecosystem



ALL COMPANIES COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more details on the solutions offered →](#)

#### 50% of companies have been created in the last 5 years



### Join the ecosystem today!

Become an active member of the ecosystem and gain great visibility! Throughout the year, a wide set of actions is organised by the ecosystem for the ecosystem.

[See more information →](#)

# Private Sector

316

Companies are part of the ecosystem

[Access the full list →](#)

Main point of contact



Created during the last 5 years

30



Number of Startups

74

## A closer look to the private sector

[Companies](#)

[Start-ups](#)

### Cybersecurity as core business

Companies have Cybersecurity as their core business

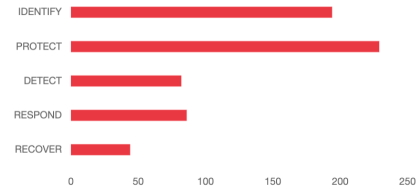
90



● ALL COMPANIES ● COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more →](#)

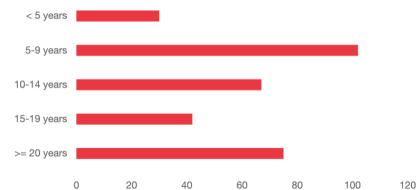
### Diversified solutions offered by the ecosystem



● ALL COMPANIES ● COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more details on the solutions offered →](#)

### 50% of companies have been created in the last 5 years



## Join the ecosystem today!

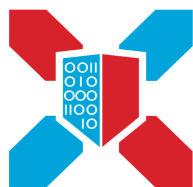
Become an active member of the ecosystem and gain great visibility! Throughout the year, a wide set of actions is organised by the ecosystem for the ecosystem.

[See more information →](#)

# Protecting & Strengthening the Economy

at national and European levels

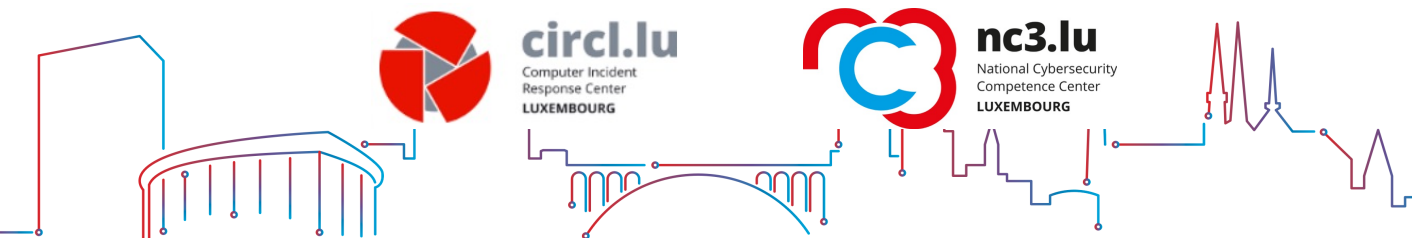




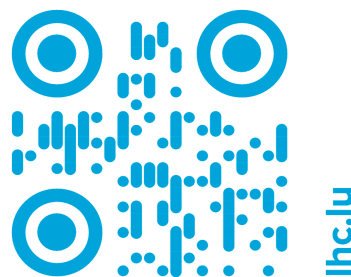
**LHC**  
Luxembourg House  
of Cybersecurity

## THE GATEWAY TO CYBER RESILIENCE

*est. 2010*



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



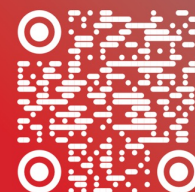
**310+** ACTIVE ACTORS  
IN CYBERSECURITY

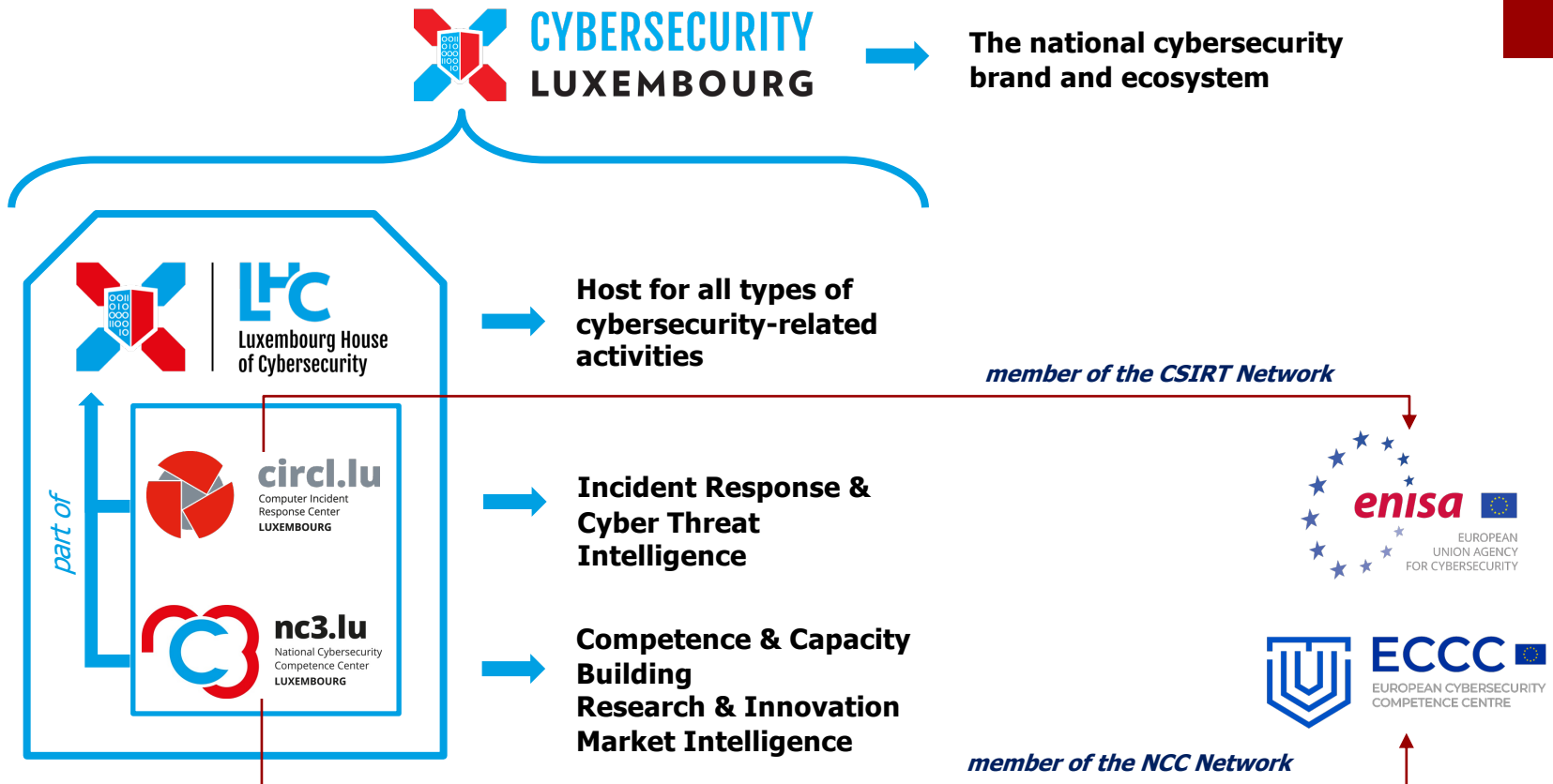
**90+** WITH CYBERSECURITY  
AS A CORE BUSINESS

**70+** STARTUPS

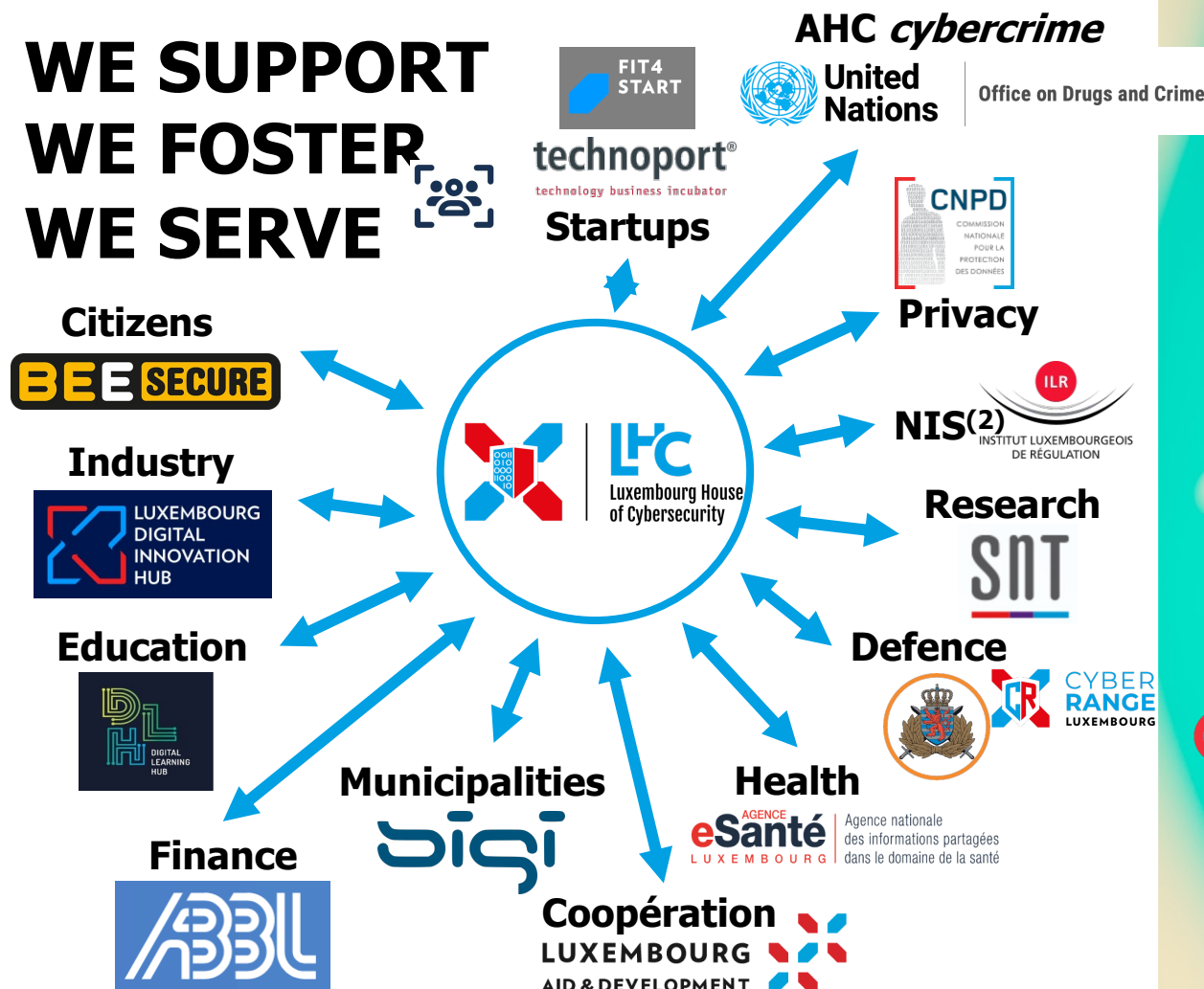
**CYBERSECURITY  
LUXEMBOURG**

More about  
the ecosystem





# WE SUPPORT WE FOSTER WE SERVE



## The first Luxembourg CYbersecurity Accelerator

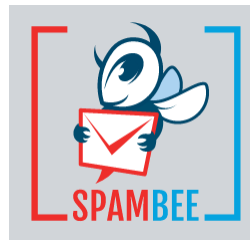
 **Cybersecurity** as a diversification asset contributing to the vitality of the Luxembourg economy

 Operated by  |   
Luxembourg House  
of Cybersecurity

in partnership  
with   
technology business incubator

# 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).



**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.



**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.



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



# LU-CID

## Luxembourg Cybersecurity Innovation & Development (*Funding Programme*)

✕ Promote and **support Innovation** in Cybersecurity contributing to the competitiveness of the Luxembourg economy  
(**state aid up to 60.000 €**)

✕ Operated by  **nc3.lu**  
National Cybersecurity  
Competence Center  
LUXEMBOURG

in partnership  
with



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



Co-funded by the  
European Union

# SME-Package Cybersecurity

Self-assessment via <https://fit4cybersecurity.nc3.lu/>

✕ State **support** to **implement** cybersecurity solutions to strengthen the cyber posture and protect against attacks (**state aid** up to **25.000 €**)

✕ Operated by  **nc3.lu**  
National Cybersecurity  
Competence Center  
LUXEMBOURG

in partnership  
with



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

# 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 key-word lists.



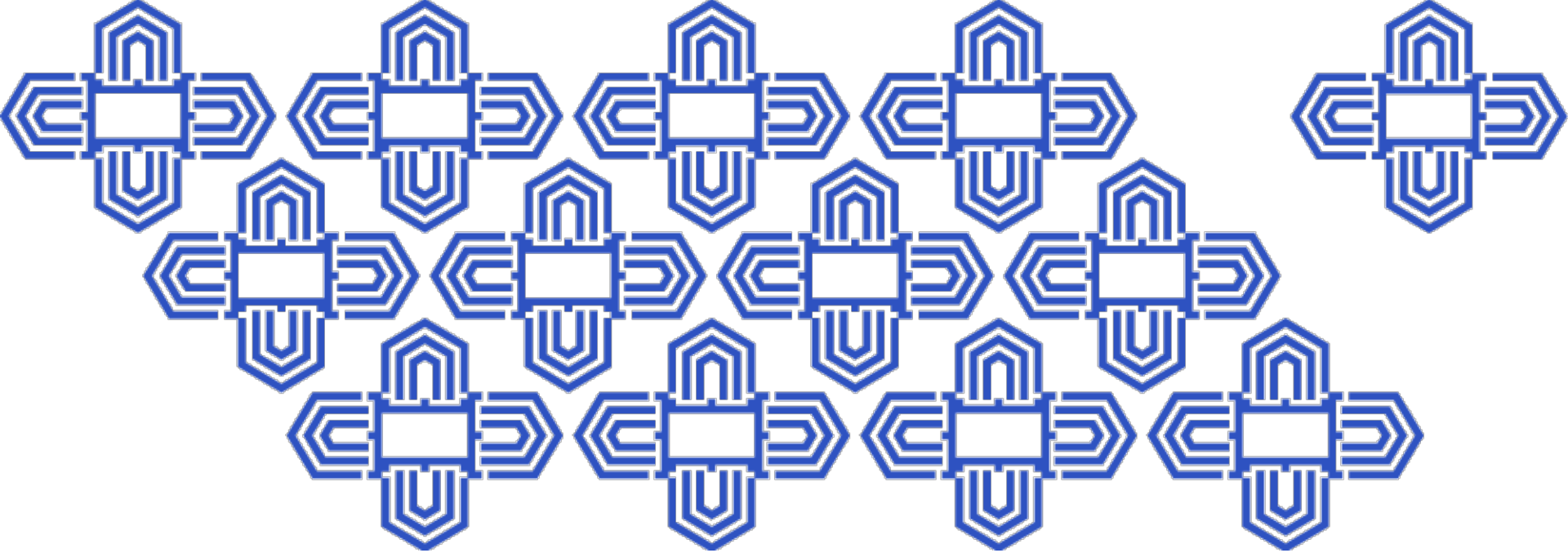
# Digital Security Risk Management for Economic and Social Prosperity

OECD Recommendation and Companion Document



2015

“Digital security risk should be treated like an economic rather than technical issue, and should be part of the organization’s overall risk management and decision-making”



# Shaping EU's cyber future



**THE EU'S CYBERSECURITY  
STRATEGY FOR THE  
DIGITAL DECADE**





# “Team Cyber” for Europe



NIS Coordination Group

CSIRT Network

CyCLONe (Cyber Crisis  
Liaison Network)

<https://www.enisa.europa.eu/>



The Network (NCCs)

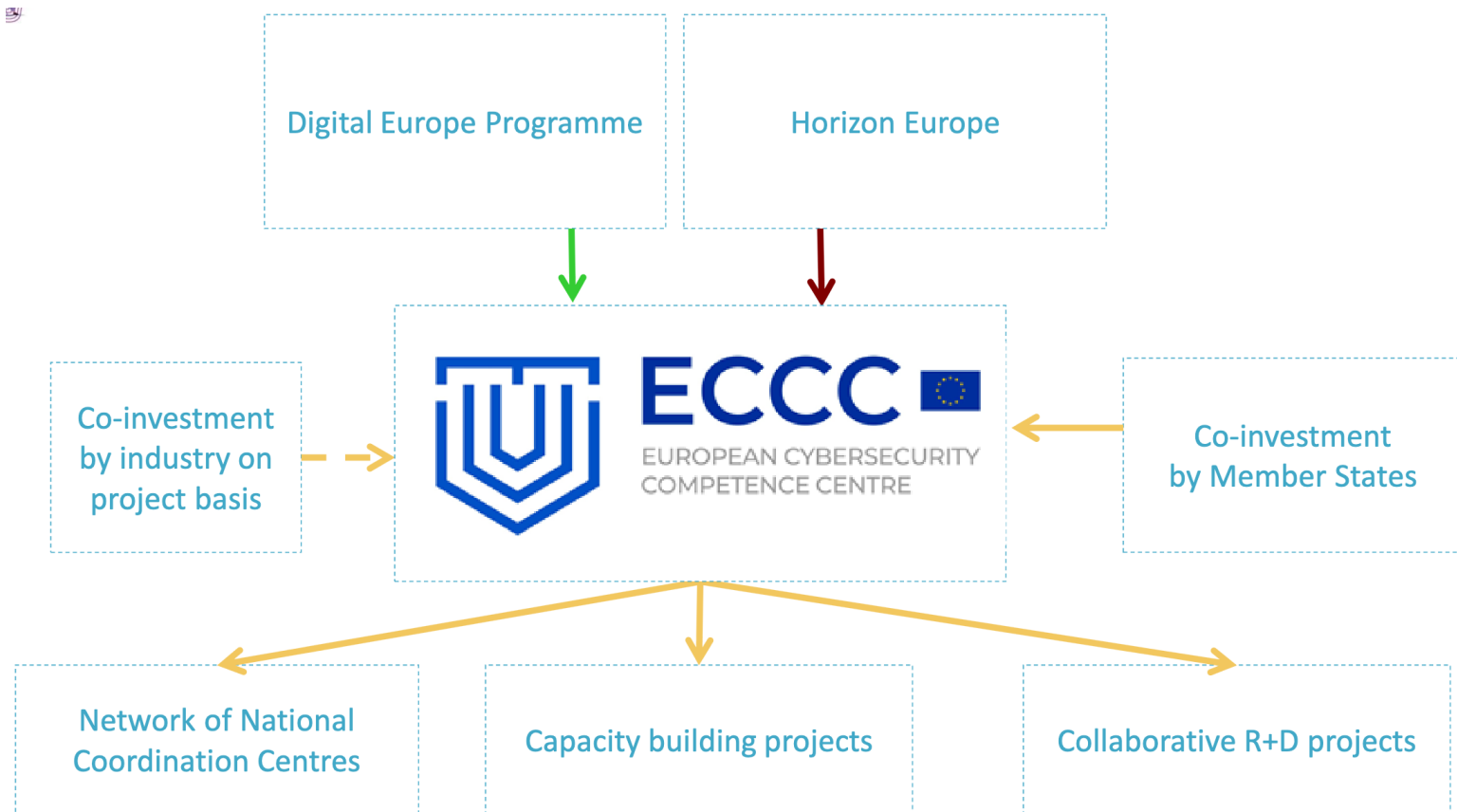
The Community  
(Research, Academia,  
Industry & Civil Society)

<https://cybersecurity-centre.europa.eu/>

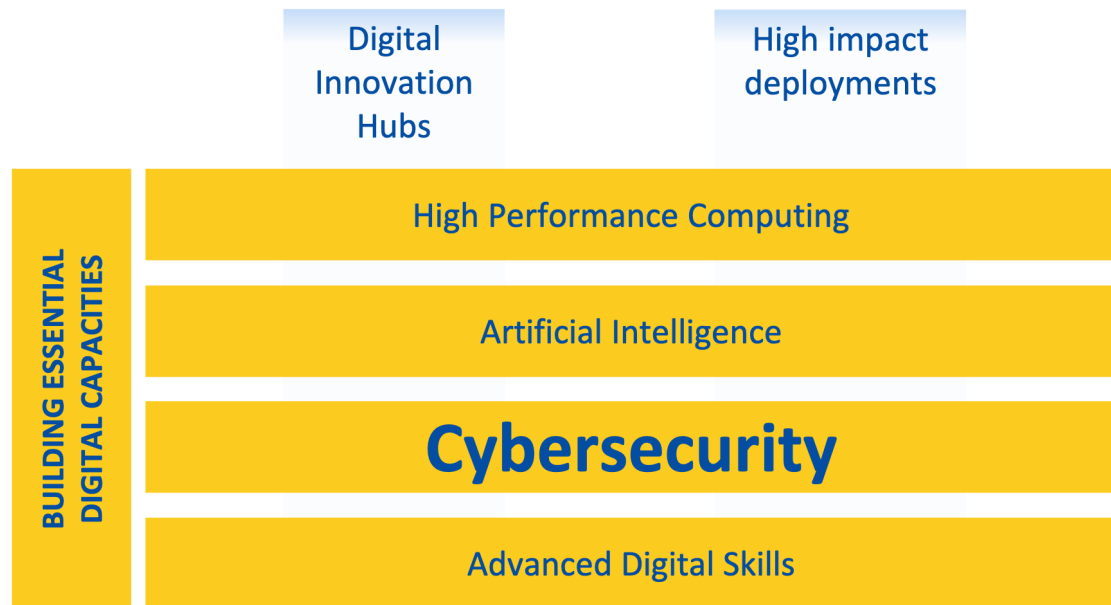
# ECCC mission

- **Encourage** and **coordinate** training activities, to ensure that everyone in Europe has access to the university and **life-long-learning** courses, as well as to motivate young people to go for a **cybersecurity career** and support efforts that address the gender gap; and
- **Increase** the global **competitiveness** of the EU's cybersecurity industry, ensure high cybersecurity standards throughout the EU and turn cybersecurity into a **competitive advantage**.
- **Strengthen** EU's **leadership** and strategic **autonomy** on cybersecurity by developing the EU's capacities and capabilities of the Digital Single Market;
- **Support** and **foster research, innovation** and **technological** developments, for the resilience of systems, including critical infrastructure as well as commonly used hardware and software;

# ECCE Instruments



# DIGITAL EUROPE



# HORIZON EUROPE

## SPECIFIC PROGRAMME: EUROPEAN DEFENCE FUND

*Exclusive focus on  
defence research  
& development*

Research  
actions

Development  
actions

## SPECIFIC PROGRAMME IMPLEMENTING HORIZON EUROPE & EIT\*

*Exclusive focus on civil applications*



### Pillar I EXCELLENT SCIENCE

European Research Council

Marie Skłodowska-Curie

Research Infrastructures



### Pillar II GLOBAL CHALLENGES & EUROPEAN INDUSTRIAL COMPETITIVENESS

Clusters

- Health
- Culture, Creativity & Inclusive Society
- Civil Security for Society
- Digital, Industry & Space
- Climate, Energy & Mobility
- Food, Bioeconomy, Natural Resources, Agriculture & Environment

Joint Research Centre



### Pillar III INNOVATIVE EUROPE

European Innovation  
Council

European Innovation  
Ecosystems

European Institute of  
Innovation & Technology\*

## WIDENING PARTICIPATION AND STRENGTHENING THE EUROPEAN RESEARCH AREA

Widening participation & spreading excellence

Reforming & Enhancing the European R&I system



# HE – synergies with other programmes

## HORIZON EUROPE

### Other Union Programmes, including

Common Agricultural Policy	InvestEU	ESF+	Innovation Fund
External Instrument	LIFE	Digital Europe	Internal Security Fund and Instrument for Border Management
Maritime & Fisheries Fund	EU4Health	Space Programme	
Connecting Europe Facility	ERDF	ERASMUS+	Single Market Programme
Just Transition Mechanism		Creative Europe	Recovery and Resilience Facility

### Enhanced synergies

#### COMPATIBILITY

Harmonisation of funding rules; flexible co-funding schemes; pooling resources at EU level

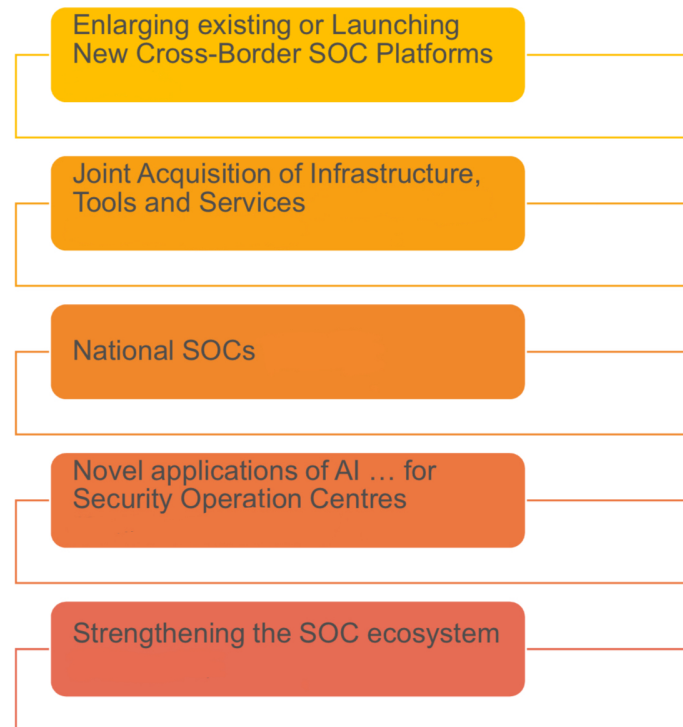
#### COHERENCE & COMPLEMENTARITY

Alignment of strategic priorities in support of a common vision

# Joint Actions – SOC

Building/strengthening  
National cross-border  
SOCs using multiple  
instruments:

Joint Procurement  
Grants



# Strategic Agenda



# Strategic Agenda

By 2027, the ECCC and the Network will have

**1. funded** European **SMEs** in developing and **using** strategic cybersecurity **technologies, services** and **processes** through a coordinated cascade funding mechanism via **NCCs** and national co-financing

**2. supported** and grown the cybersecurity professional **workforce** in both **quantity** and **quality** through the standardisation and certification of cybersecurity **skills** and investments in **education** and **training**

**3. strengthened** the **research, development** and **innovation** expertise and **competitiveness** of the **EU** cybersecurity **community**

# #CyberTogether

*Fostering collaboration and cooperation, to tackle emerging threats and challenges efficiently, as well as to embrace opportunities for a better, safer future.*

Because only together will we tackle the many challenges of our digitised world, and be able to make Europe strong, competitive and cyber secure.

- Cloud and multi-cloud environment
- Supply chain security
- Infrastructure resilience
- Quantum computing
- Advent of AI and autonomous functions
- Skills shortage and competence needs
- Vulnerabilities of small entities (SME)
- Info sharing & threat intel
- Dual use & the geopolitical context
- Commercialisation of R&D



Thank you  
for your attention

Questions ?