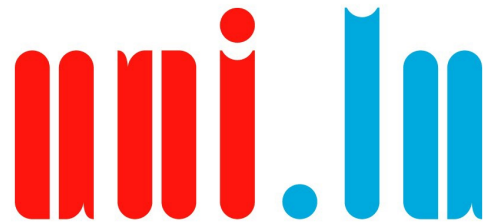




UNIVERSITÉ DU  
LUXEMBOURG



UNIVERSITÉ DU  
LUXEMBOURG









# *New Technology, old risks, IoT (in-)security*





Master in Technopreneurship

# Threat landscape

2022/2023

# Luxembourg CyberWeather (Q3 2022)

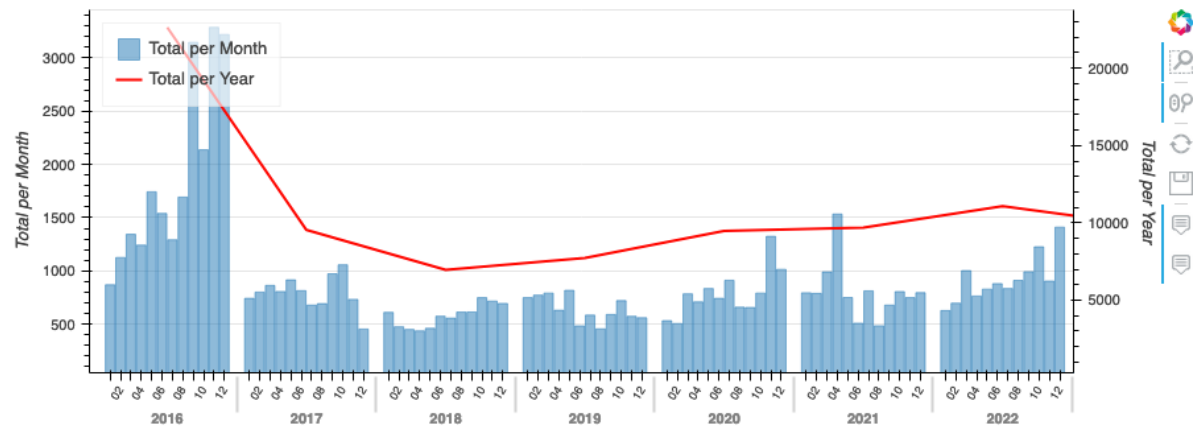
Category	Status
Malware	
Availability	
Phishing and scams	
Intrusions	
Vulnerabilities	
IoT	
eID	
APT	

Symbol used	Explanation
0 - 15% of teams indicating this type of incident	
16 - 50% of teams indicating this type of incident	
51 - 85% of teams indicating this type of incident	
86 - 100% of teams indicating this type of incident	

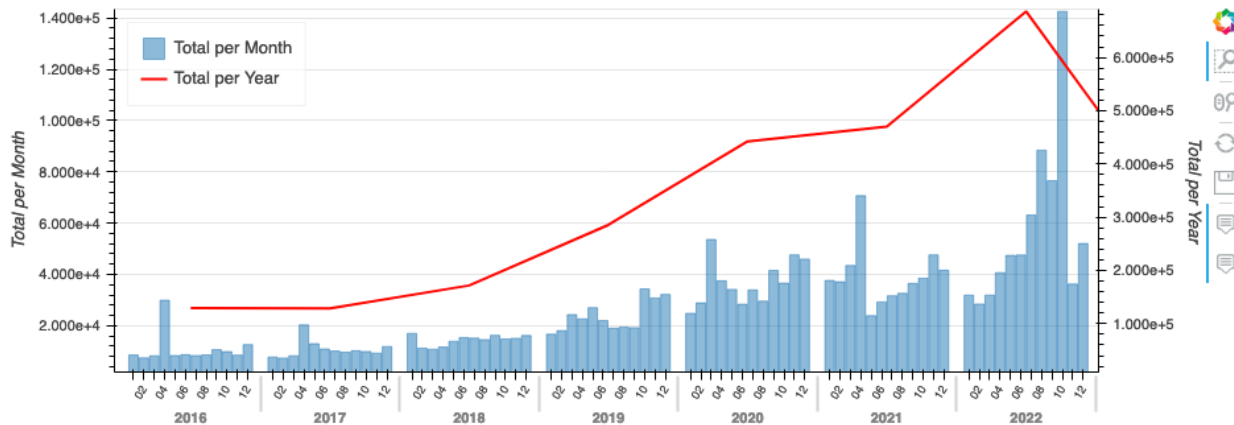
<https://www.govcert.lu/en/cyberweather/>

# Luxembourg Operational statistics

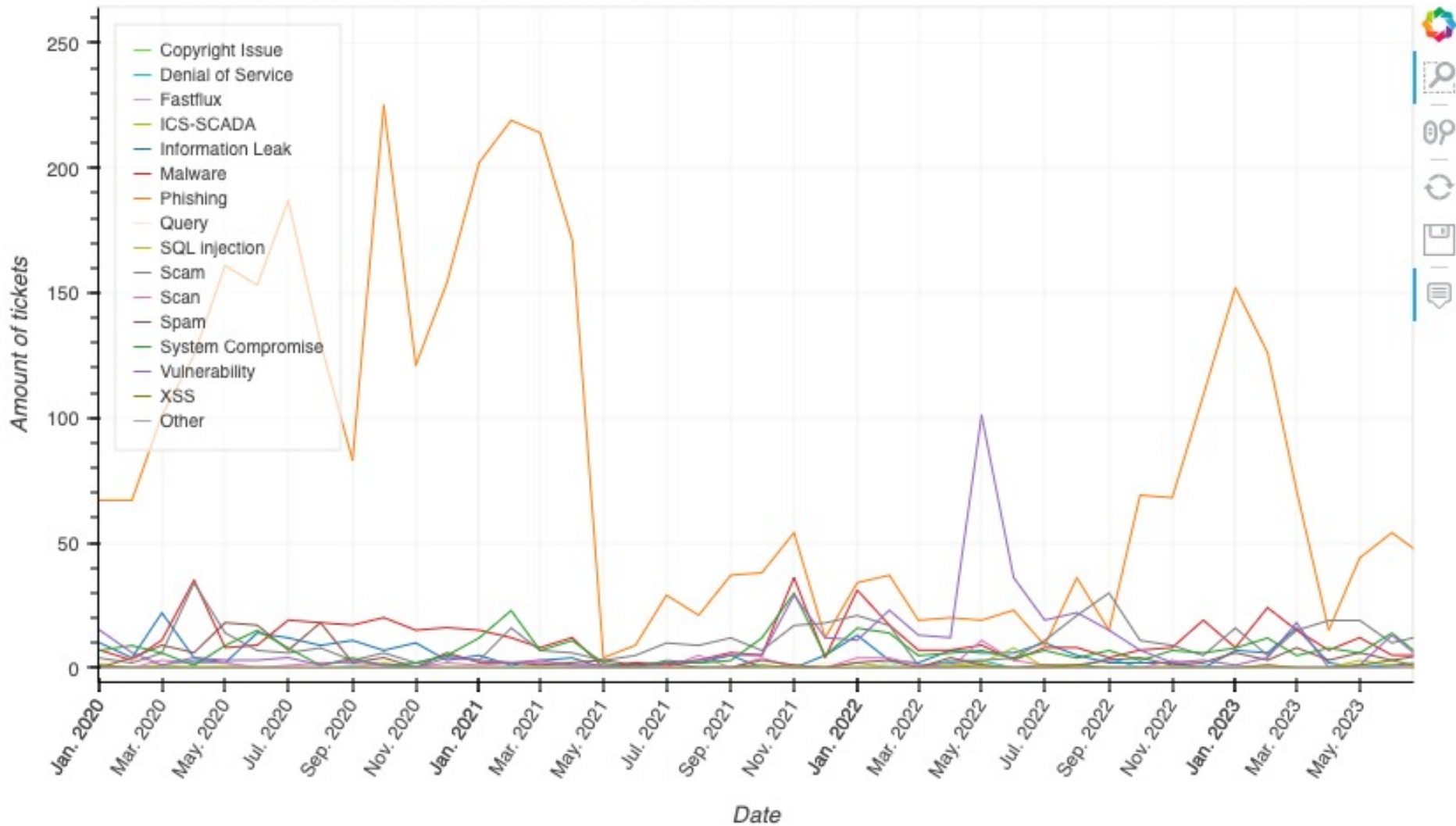
## Manual tickets over time



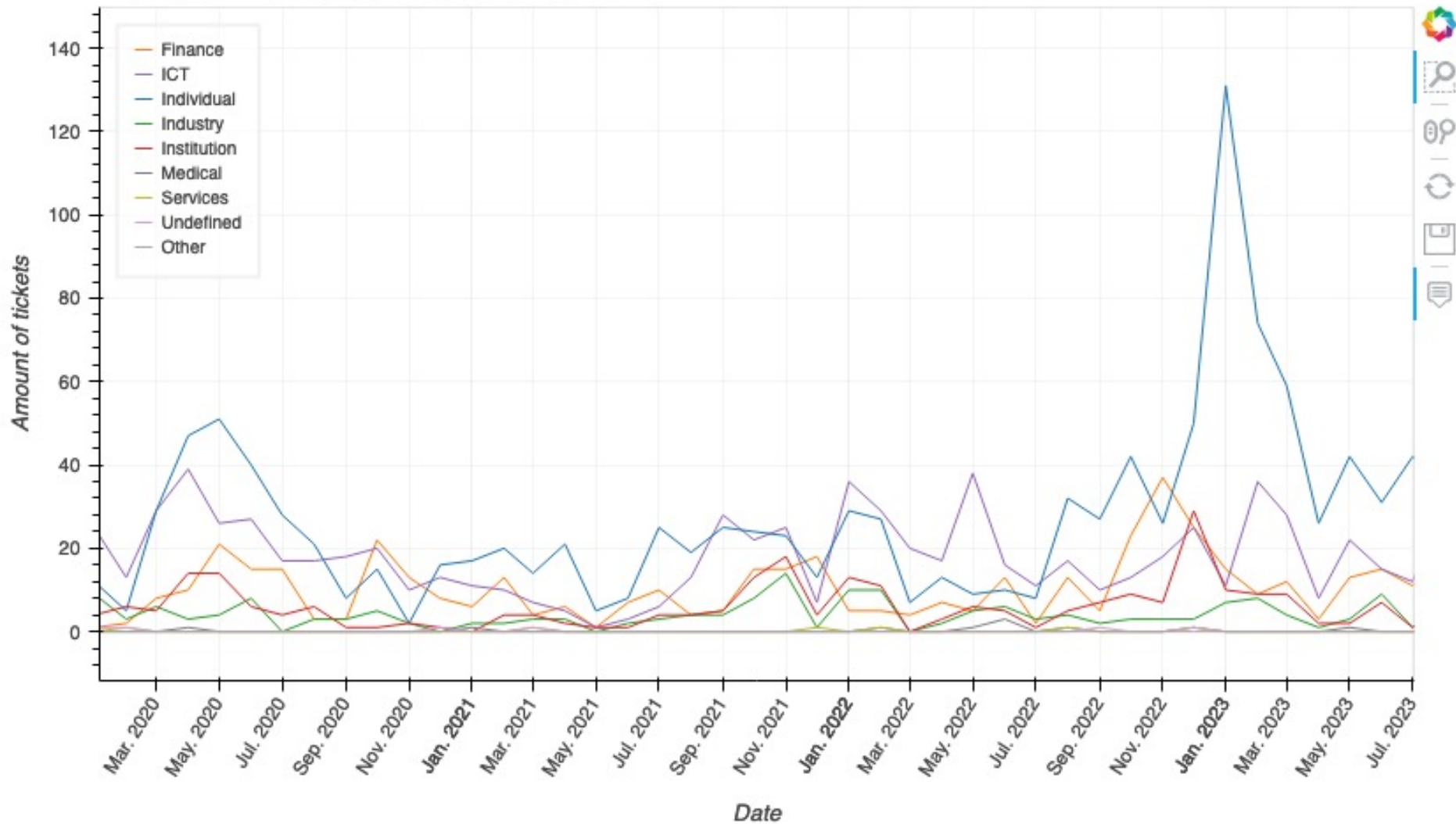
## Automatic tickets over time



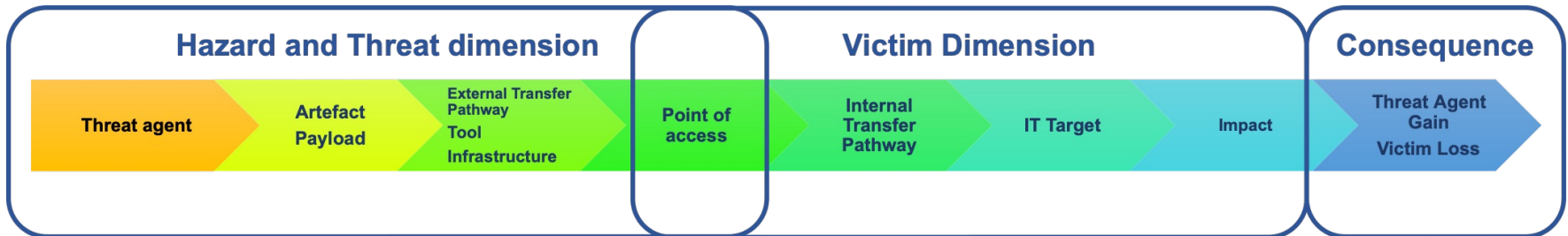
## Manual Ticket Classification over time





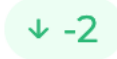



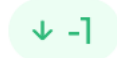









## Manual Ticket by Sector over time



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





	Threat Actors Name	Attributed Events 	Trend 
>	APT-C-35	0 	
>	APT-C-36	2 	
>	APT-C-61	0 	
>	APT28	3 	
>	APT29	0 	
>	APT35	0 	
>	APT36	0 	







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

### Type of Impact

Various outcomes of cyber threats identified.

#### Our analysis

The information detected by the monitoring system regarding the type of consequences for the victim is mainly related to scam and ransom demands. The high number of scams is strictly related to the classification of phishing records as scam events. Therefore, the attribution rate of this class remains rather low.



Type of Impact	Attributed Events ⓘ	Trend ⓘ
Espionage	0 ↓ -3	
Ransom	30 ↓ -14	
Scam	256 ↑ 141	
Customer Data	1 ↑ 1	
Data loss, OS / file corruption	0 ↓ -2	
War conflict	8 ↓ -3	

### Type of Victim

Diverse sectors targeted by cyber threats during the period.

#### Our analysis

During this quarter there was a reduction in the number of events detailing the type of victim affected.

Infrastructure	Attributed Events ⓘ	Trend ⓘ
Airlines	0 ↓ -4	
Bank	12 ↓ -44	
Communication	0 ↓ -3	
Defense	1 ↓ -3	
Education Institutions	1 ↓ -28	
Energy	0 ↓ -2	
Financial Institutions	0 ↓ -8	

Show more

# Europe

## Top threats, majors trends

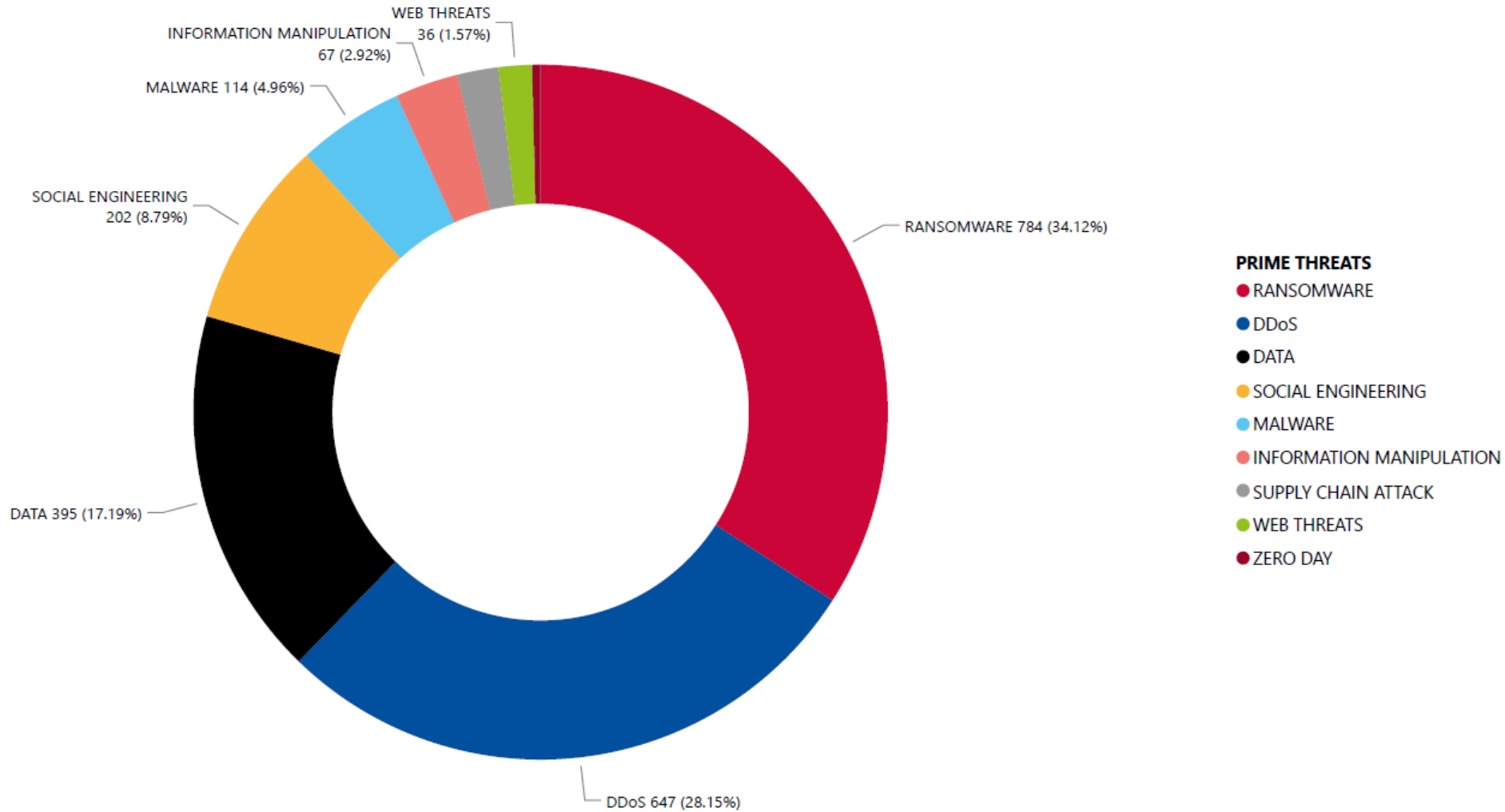


<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>

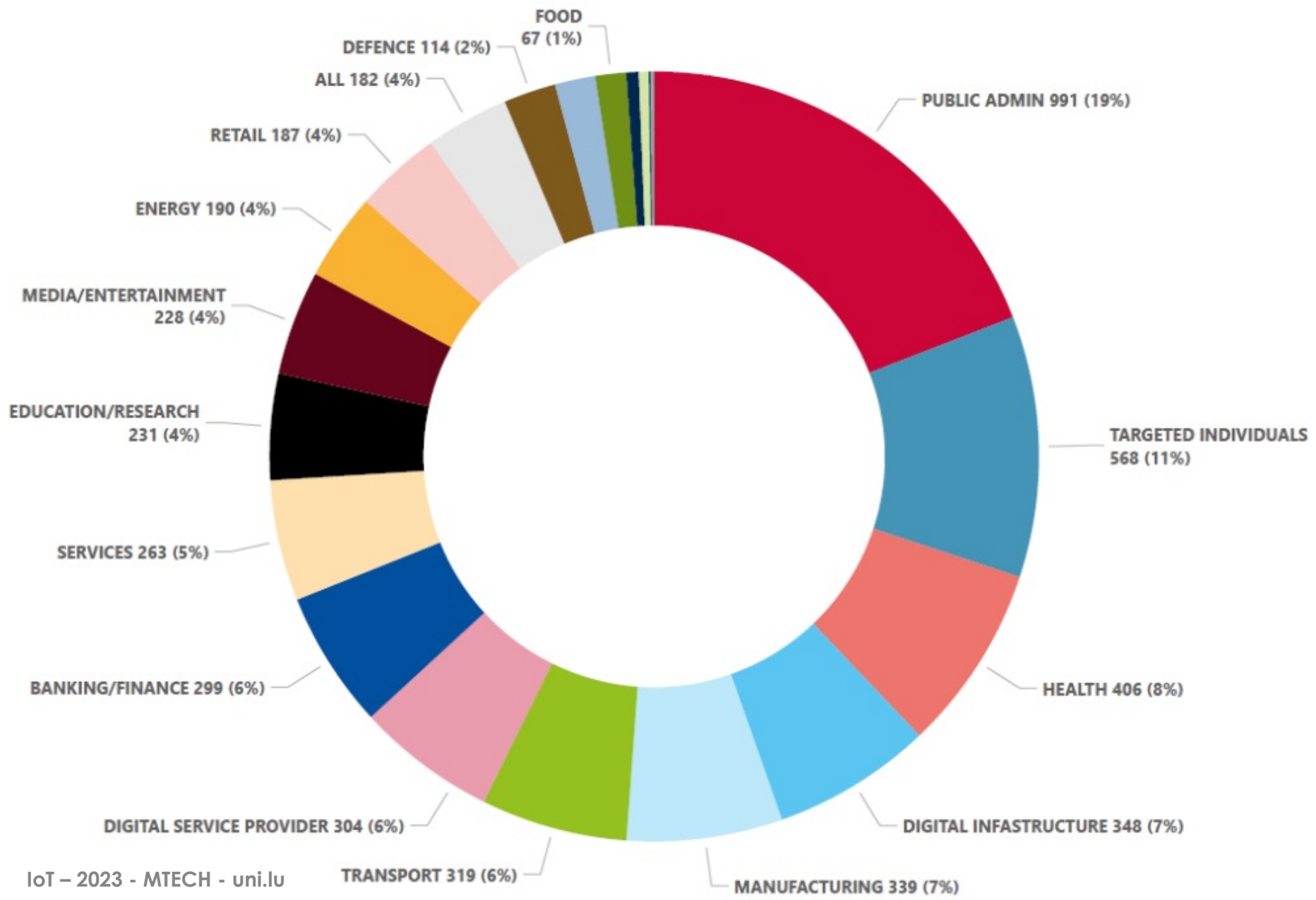
Figure 1: ENISA Threat Landscape 2022 - Prime threats



Figure 5: EU breakdown of number of threats by threat group



**Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)**



# Europe (main findings)

- **Ransomware and threats against availability ranked at the top during the reporting period.**
- **Resourceful threat actors have been observed to misuse legitimate tools** primarily to prolong their cyber espionage operations . Their aim was to evade detection for as long as possible and obscure their activities by using widely available software from most systems which makes it more challenging for defenders to identify them. Maximizing their chances of success when it comes to an intrusion by not arousing victim' suspicions
- **Geopolitics continue to have a strong impact on cyber operations.**
- **Several threat actors further professionalised** their As-a-Service programmes. They not only used novel tactics and methods to infiltrate environments but also delved into alternative approaches to pressure and extort victims, all the while advancing their illicit enterprises.
- **By Using Extortion Only Techniques** criminal organisations have been progressively blending extortion methods that almost invariably incorporate some form of data theft. Double extortion has witnessed a notable rise, with certain groups even relying solely on the act of stealing information.
- **Increased operations by law enforcement**, such as the takedown of Hive ransomware group's IT infrastructure or Trickbot.
- **CI0p rose** in the first half of 2023 with the weaponisation of two zero-days.
- **One of the biggest malware threats is still information stealers** such as Agent Tesla, Redline Stealer and FormoBook.
- **There is a steady decline in classic mobile malware**, with adware remaining in numbers of occurrences the most prevalent threat to mobile devices while in terms of impact spyware can be seen as the most prevalent threat to mobile devices.



# Europe (main findings cont'd)

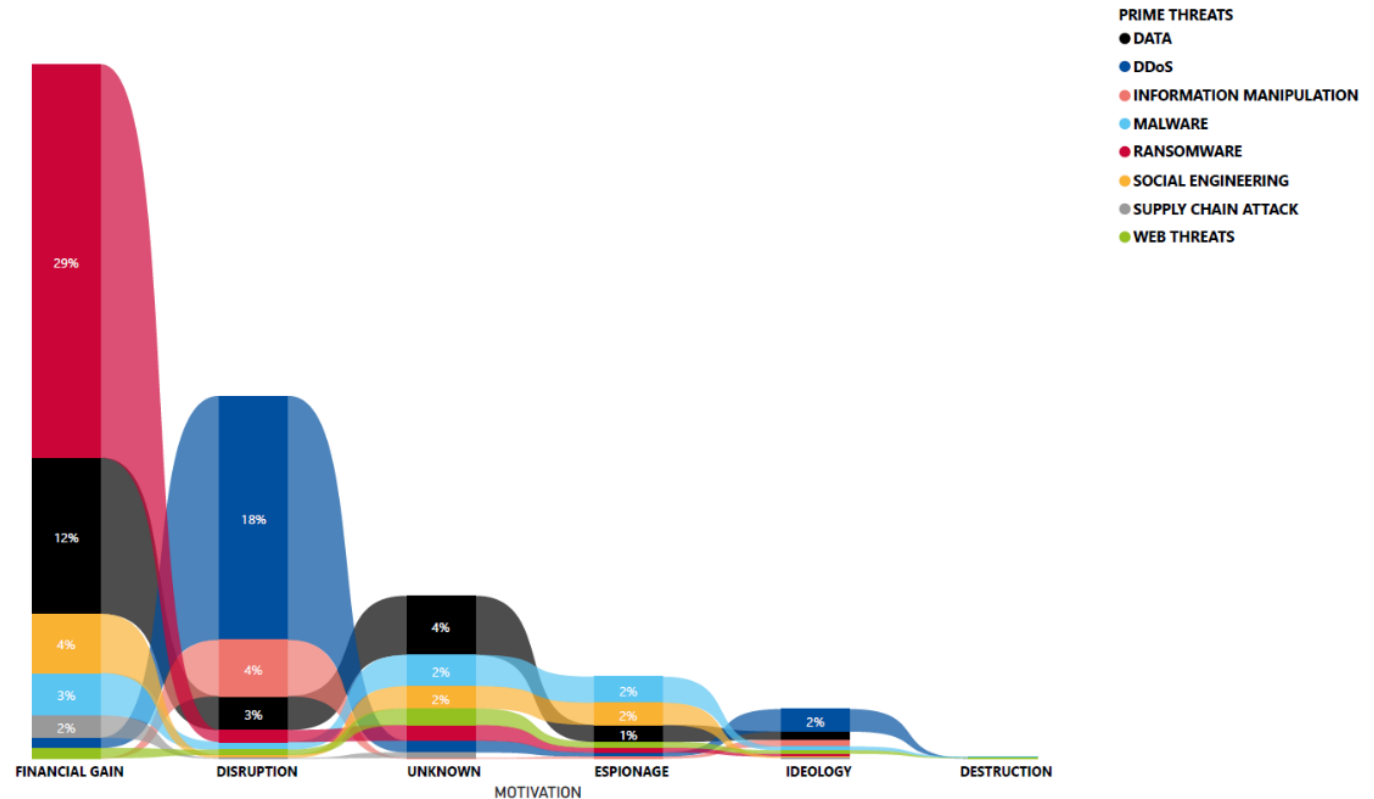
- **Hacktivists are increasingly claiming that they target OT environments** but public reporting indicate they often **overestimate** or do not **substantiate** their claims.
- **Phishing is once again the most common vector** for initial access. But a new model of social engineering is also emerging, an approach that consists of **deceiving victims in the physical world**.
- **Business e-mail compromise (BEC, VEC) remains** one of the attacker's favourite means for obtaining financial gain.
- **The move from Microsoft macros to ISO , Onenote and LNK files is continuing**, a shift towards the use of LNK and ISO/ZIP files as well as Onenote files in response to Microsoft's macro changes.
- **Data compromise increased in 2023**. There was a rise in data compromises leading up to 2021, and although this trend remained relatively stable in 2022, it began to increase once more in 2023.
- **There has been a Surge in AI Chatbots impacting the cybersecurity threat landscape**. The disruptive impact and the exponential adoption of generative artificial intelligence chatbots such as OpenAI ChatGPT, Microsoft Bing and Google Bard are changing the way in which we work, live and play, all built around data sharing and analysis.
- **DDoS attacks are getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of** being used in support of additional means in the context of a conflict.
- **Internet shutdowns are at an all-time high**. Internet availability threats are keeping up their momentum, especially in the post-covid era, due to the increasing reliance of human activities and society on Internet technologies.
- **Information manipulation is a key element of Russia's war of aggression against Ukraine**. Information manipulation has been an essential and well-established component of Russia's security strategies<sup>16 17</sup>. The number of analysed events for the reporting period has also grown significantly.
- **'Cheap fakes' and AI-enabled manipulation of information** continues to be a cause for concern. In the past months, the debate on the use of AI to manipulate information has heated up both within and beyond the circle of industry professionals.
- **Threat groups have an increased interest in supply chain attacks and exhibit an increasing capability by using employees as entry points**. Threat actors will continue to target employees with elevated privileges, such as developers or system administrators





# Europe (threat actors)

Figure 10: Motivation of threat actors per threat category



IoT



A top-down view of a collection of electronic components. In the center, a black battery pack holds three AA batteries. To the right, an Arduino Uno micro-controller board is visible. Above it are two blue servo motors with orange and red wires. To the left, there are several push buttons and a breadboard. The background is filled with various other components like sensors, LEDs, and connectors.

# TAKE THESE SENSORS, MICRO-CONTROLLERS...



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



A close-up photograph of a white humanoid robot, Pepper, with large, expressive blue eyes and a small black dot for a nose. The robot is holding a tablet computer. A semi-transparent dark grey banner is overlaid across the middle of the image, containing white text. The background is a warm, wooden wall.

# 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 is standing on the edge of a large, dark rock formation that juts out over a vast, hazy valley. The scene is bathed in the warm, golden light of a sunset or sunrise, with the sun low on the horizon behind the person. The background shows rolling hills and mountains under a soft, orange glow. The overall mood is contemplative and serene.

# SOME EXAMPLES

The image features three white Axis Mirai botnet cameras against a dark grey background. The central camera is positioned at the top, looking directly forward. The two side cameras are angled downwards and outwards. Each camera has a black lens and a white protective housing. The Axis logo is visible on the side of each camera's housing.

# MIRAI BOTNET

"SMART" CAMERAS



# CAYLA THE DOLL

MIRAI SUENAGA

SMART DOLL

DESIGNED BY DANNY CHOO

## 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. A semi-transparent dark blue banner is overlaid on the image, containing white text.

HACKING YOURSELF: MARIE MOE AND PACEMAKER SECURITY

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

# RECOMMENDATIONS (USER)

- strong password security



**ACCOUNT HIJACKING**  
The Digital First Aid Kit

- software/firmware updates



**SECURE COMMUNICATION**  
The Digital First Aid Kit

- network segmentation and filtering

- physical security



**DDOS MITIGATION**  
The Digital First Aid Kit

- check contracts, terms and conditions



**MALWARE**  
The Digital First Aid Kit

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



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



# 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

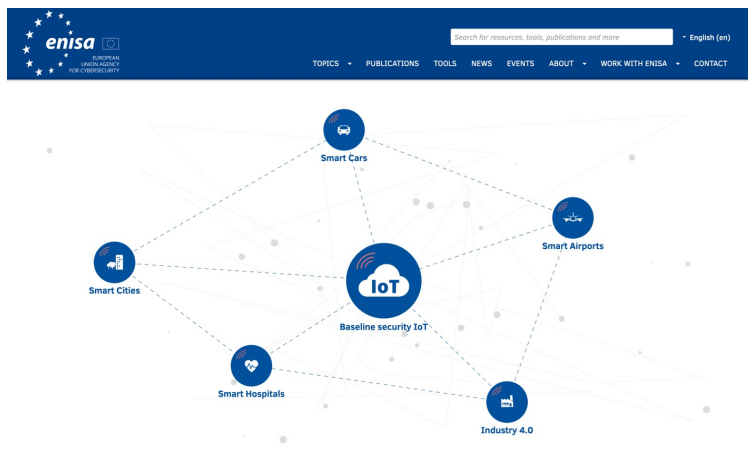
01010  
11101  
00101





# ENISA references

## IoT and Smart Infrastructures Tool



<https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures>

## Threat Landscape for Supply Chain Attacks

**enisa** EUROPEAN UNION AGENCY FOR CYBERSECURITY

Navigation menu

### Threat Landscape for Supply Chain Attacks

This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021. Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

**Download**  
PDF document, 4.79 MB

**Published** July 29, 2021  
**Language** English



# SMART & SECURE

secure-iot.lu

# SMART & SECURE

## NATIONAL AWARENESS CAMPAIGN 2021



**Smart Phone**



**Smart Office**



**Smart Home**



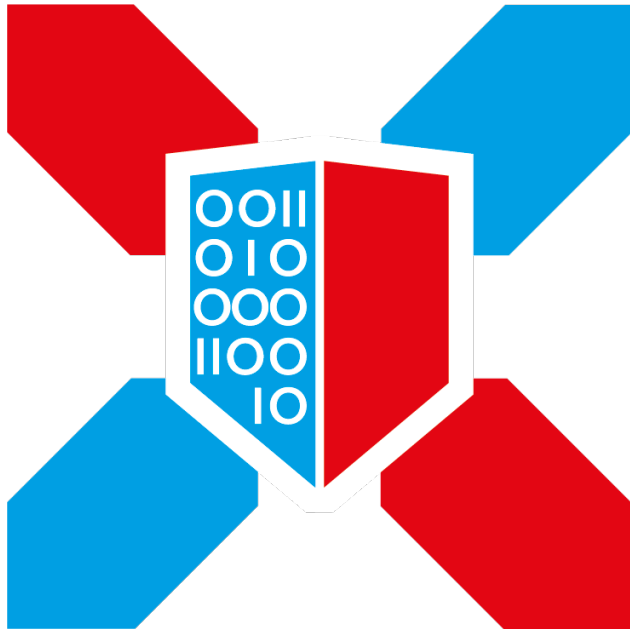
**Smart Wearables**



**Smart Toys**



[WWW.SECURE-IOT.LU](http://WWW.SECURE-IOT.LU)



# 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)

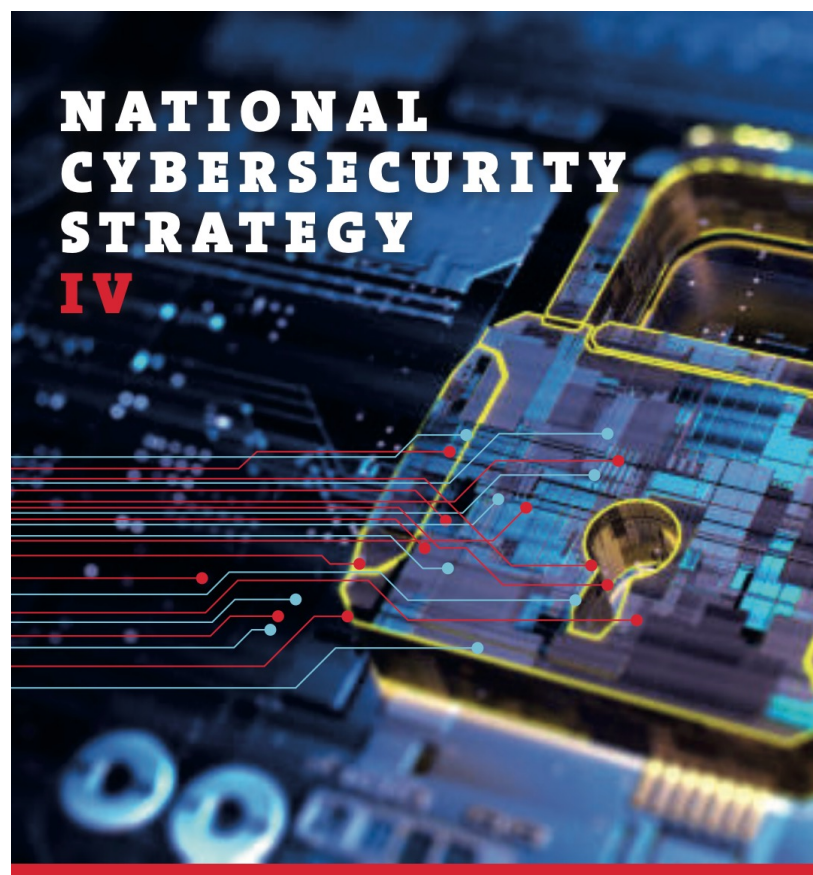


TODAY

# 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

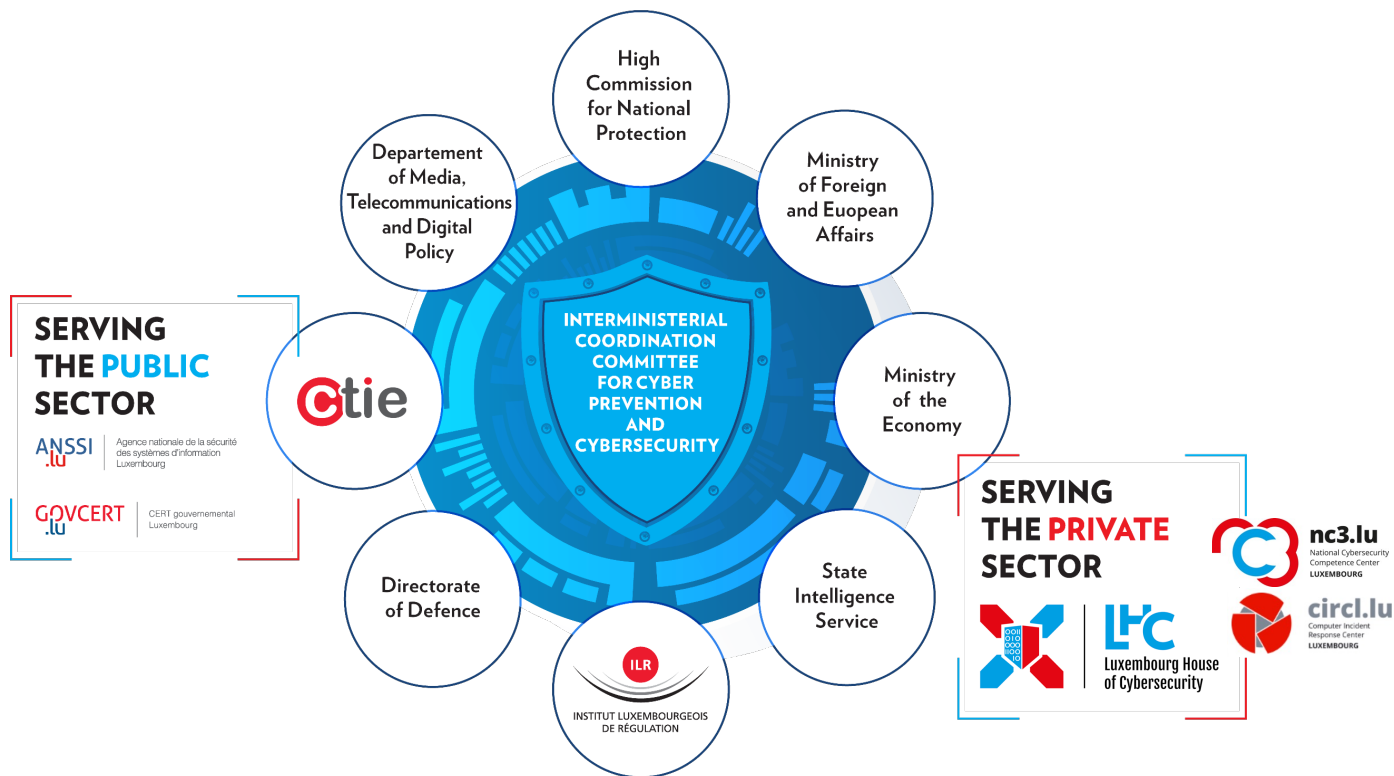


National Cybersecurity Strategy IV

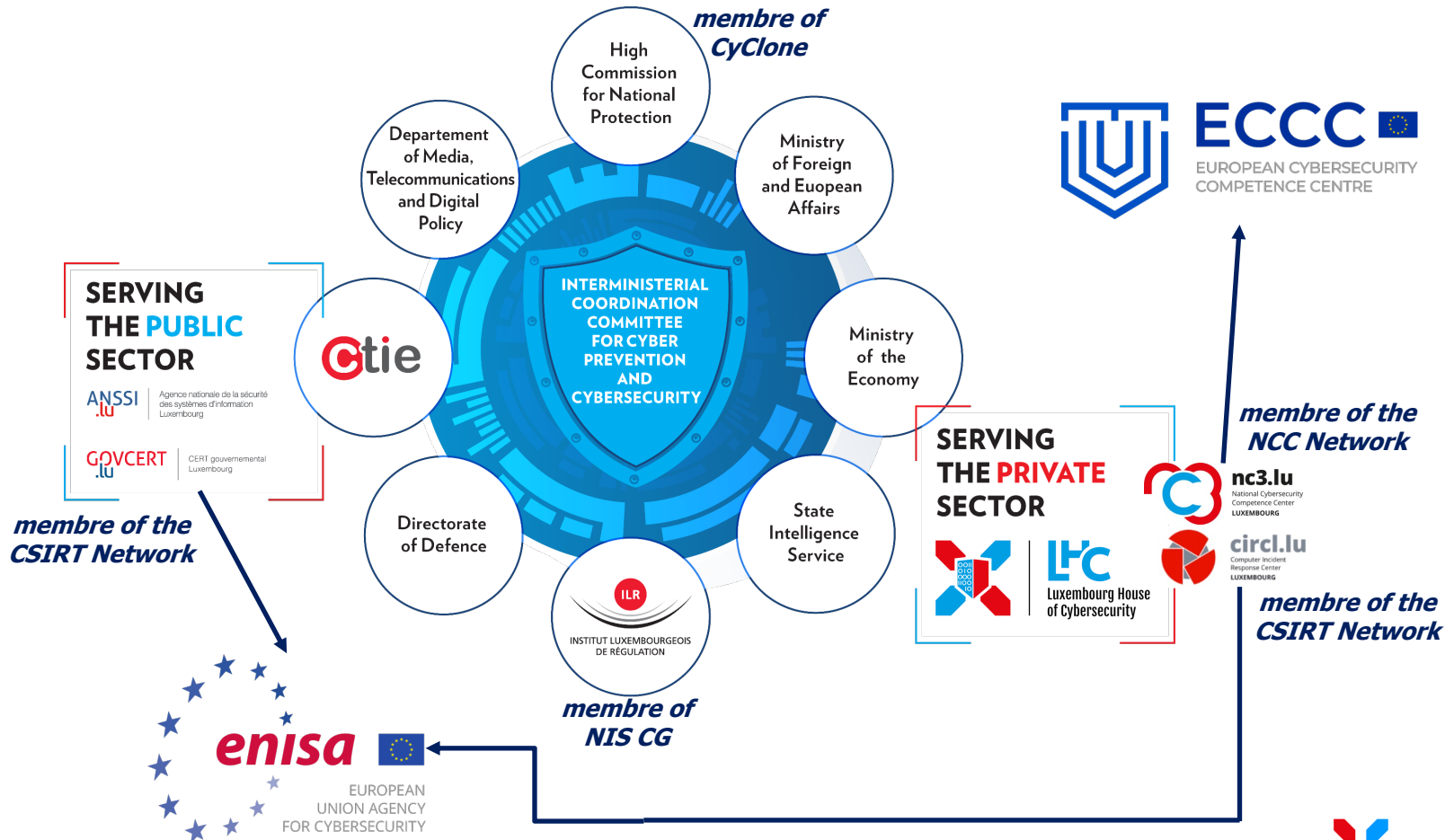




# NATIONAL GOVERNANCE



# NATIONAL GOVERNANCE



# AUTHORITIES & REGULATORS



- **CIP** Critical Infrastructure Protection  
(loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale)
- **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)
- **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

The screenshot displays the website for cert.lu, the Cyber Emergency Response Community Luxembourg. The navigation bar includes links for Home, About, Members, Projects, and Contact. The main content area features a grid of partner logos, each with a corresponding CSIRT name in a box below it:

- restena** (EDUCATION & RESEARCH)
- CIRCL** Computer Incident Response Center Luxembourg (ECONOMY & LOCAL GOVERNMENT)
- GOVCERT .lu** CERT gouvernemental Luxembourg (NAT / GOV / MIL & CRITICAL INFRA.)
- eSanté LUXEMBOURG** (HEALTH CARE)
- itrust consulting** (MALWARE.LU CERT)
- EXCELLIUM** (CERT XLM)
- clearstream** DEUTSCHE BÖRSE GROUP (DBG-CERT)
- European Commission** (EC DIGIT CSIRC)
- Post LUXEMBOURG** (CSIRT POST CYBERFORCE)
- telindus** (TELINDUS-CSIRT)
- pwc** (PWC CSIRT)
- Hacknowledge** (CSIRT HACKNOWLEDGE)



# PREPAREDNESS & RESPONSE

## PIU CYBER



THE GOVERNMENT  
OF THE GRAND DUCHY OF LUXEMBOURG

Français | Deutsch | **English**

# Info crise

Search



NUCLEAR  
EMERGENCY



VIGILNAT



POWER  
CUT



CYBER



EXTREME  
WEATHER  
CONDITIONS



INFLUENZA  
AND  
PANDEMICS



EBOLA



MASS  
CASUALTIES



CBRN



FLOODING



DRINKING  
WATER

# LU-CIX

DDoS Scrubbing Center



## Education & Research



## 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 →](#)

National contact point

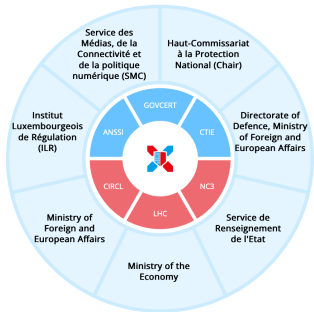


Access the latest and upcoming International, European and National Legal Frameworks

[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 →](#)

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

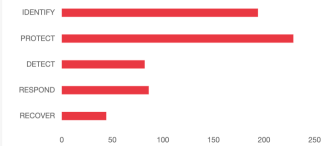


316 Companies

● ALL COMPANIES ● COMPANIES WITH CYBERSECURITY AS CORE BUSINESS

[See more →](#)

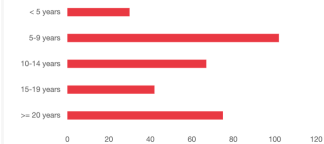
#### Diversified solutions offered by the ecosystem



● 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!

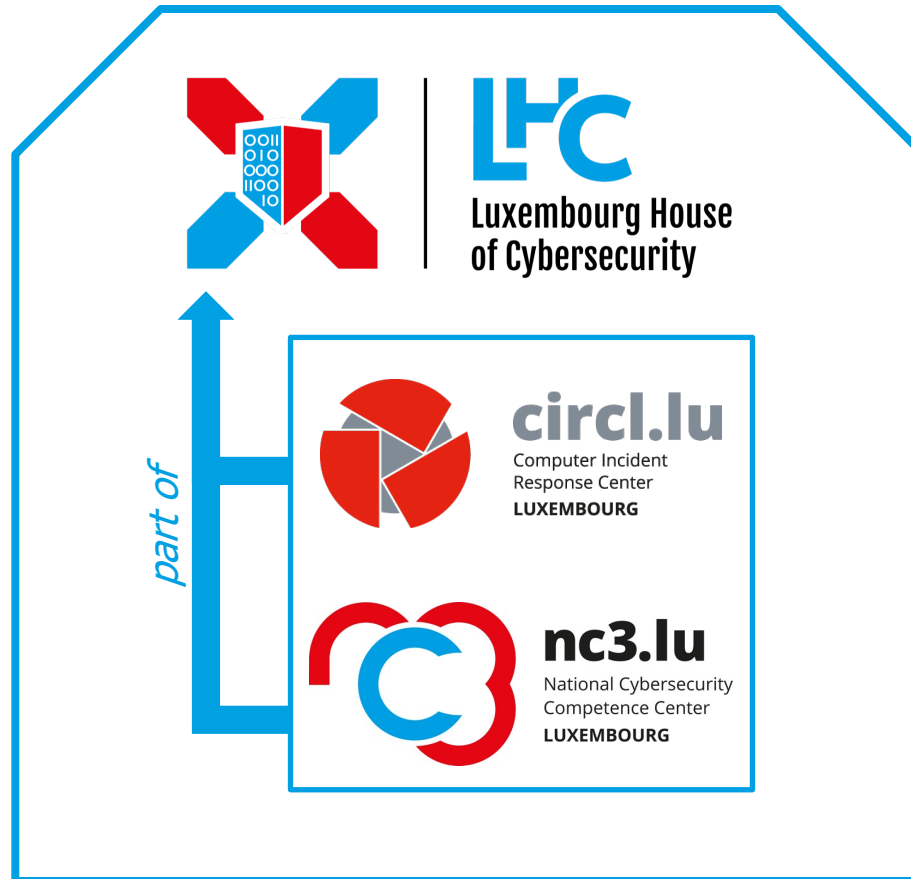
Become an active member of the ecosystem and gain great visibility! Throughout the year, a wide set of actions is organised by the ecosystem for the ecosystem.

[See more information →](#)

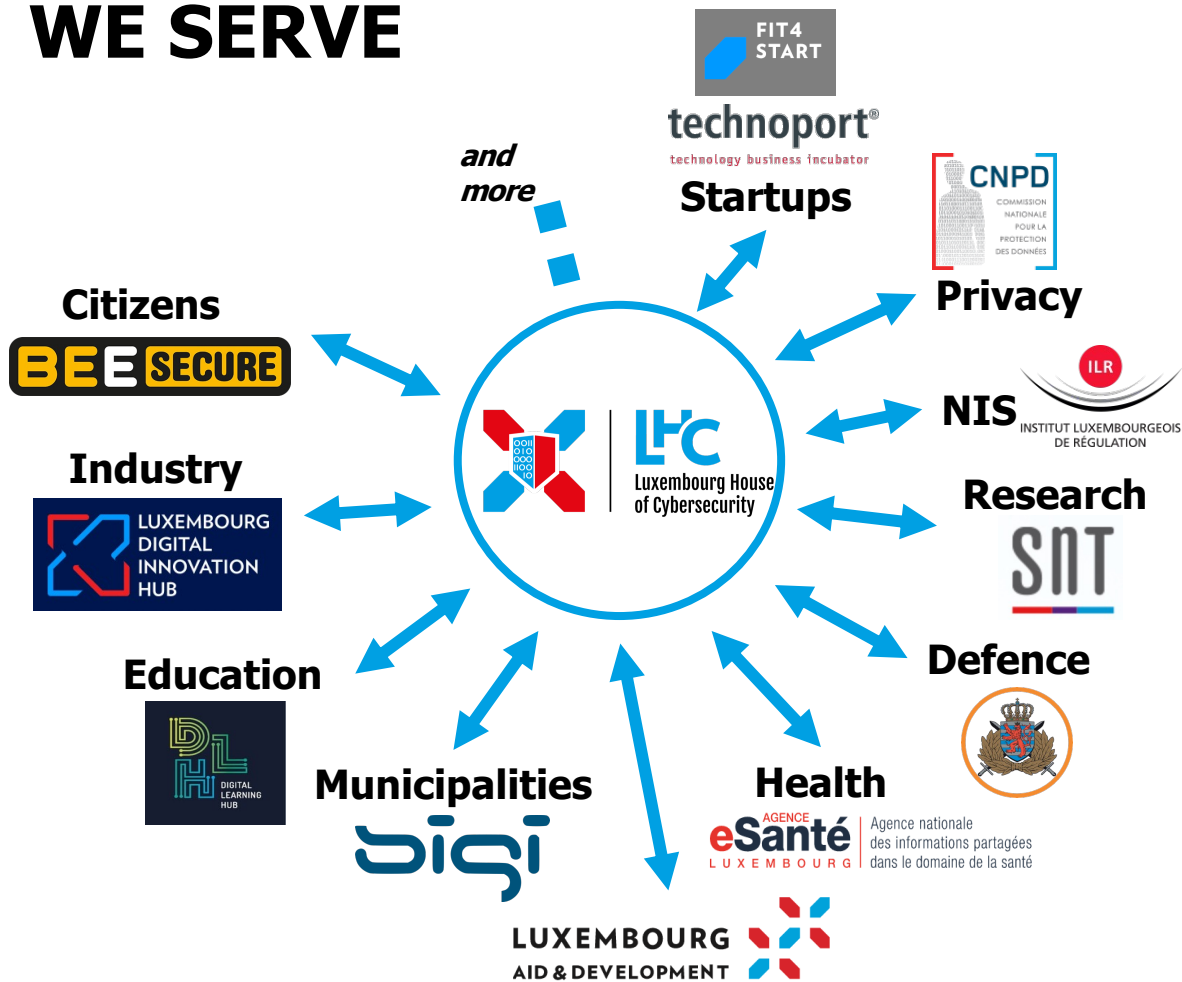


# Protecting & Strengthening the Economy

at national and European levels



**WE SUPPORT**  
**WE FOSTER**  
**WE SERVE**



# 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.

# 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.



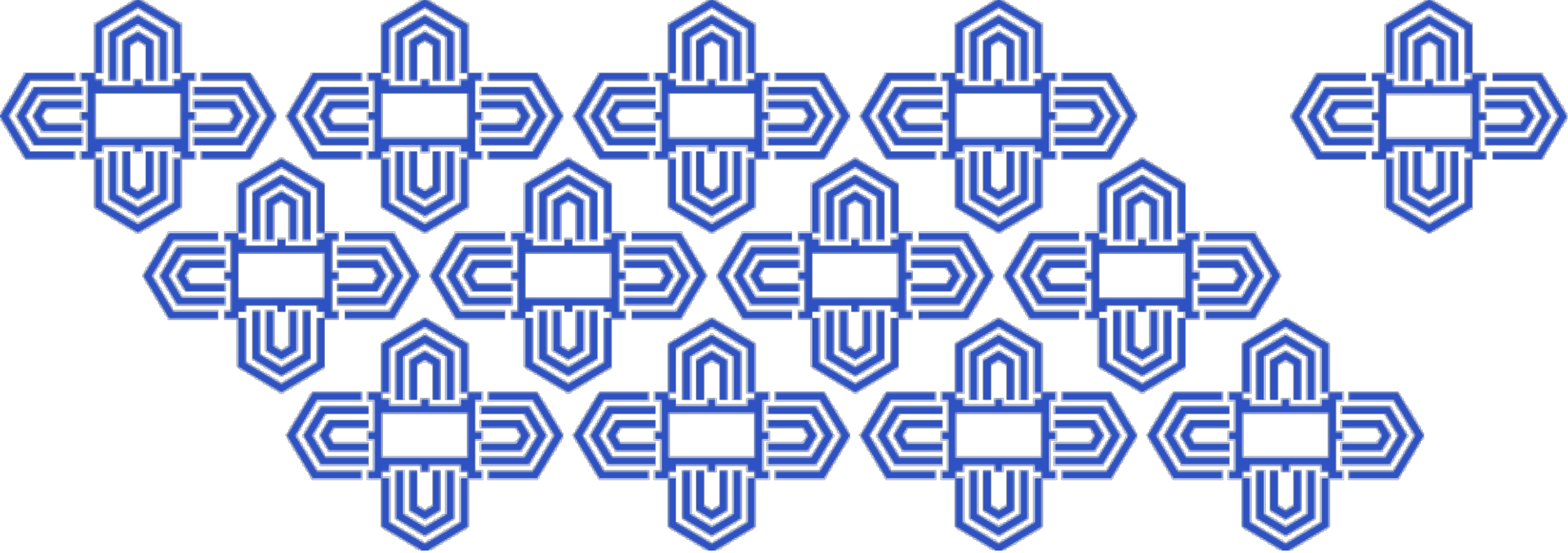
# Digital Security Risk Management for Economic and Social Prosperity

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)



The Network (NCCs)

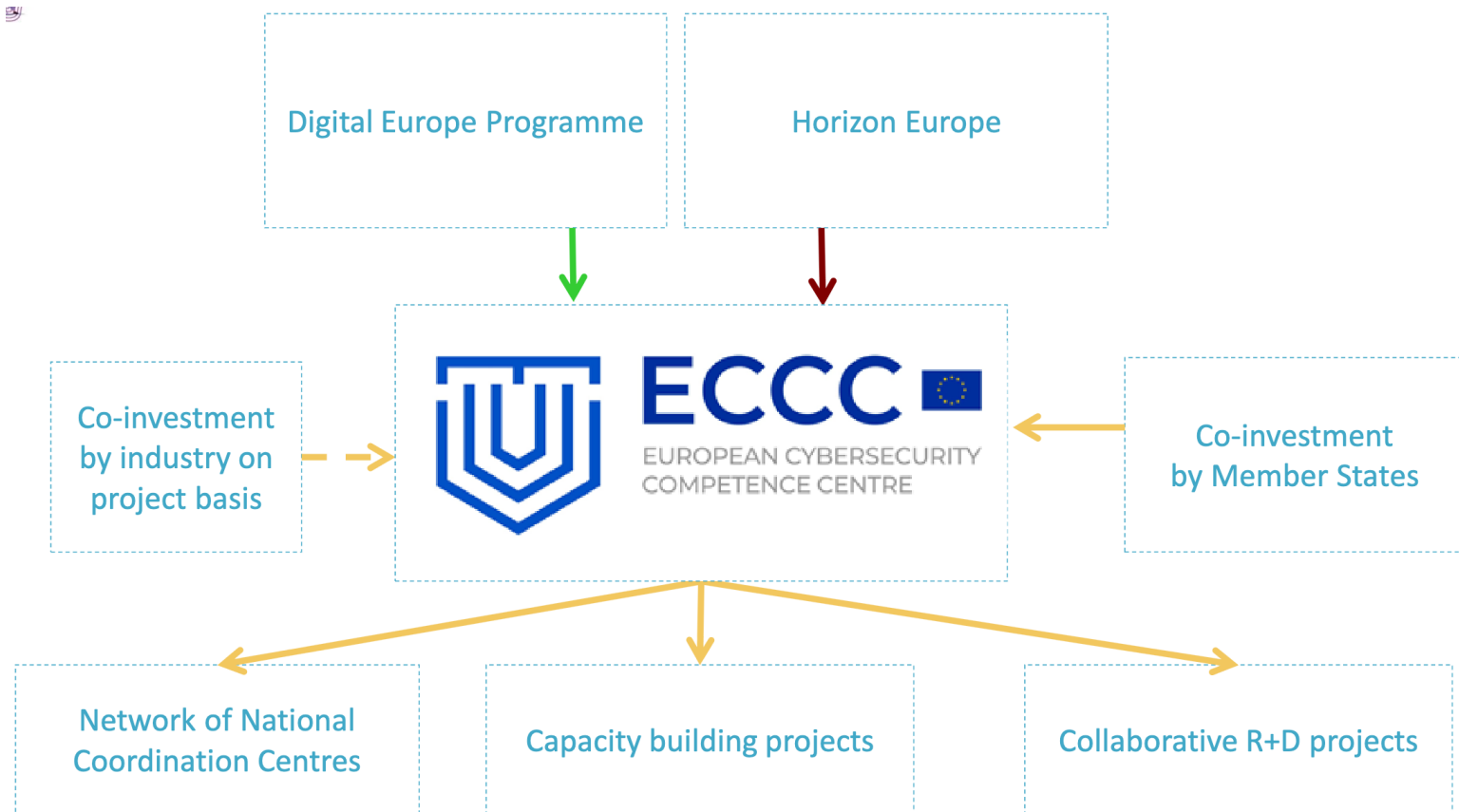
The Community  
(Research, Academia,  
Industry & Civil Society)



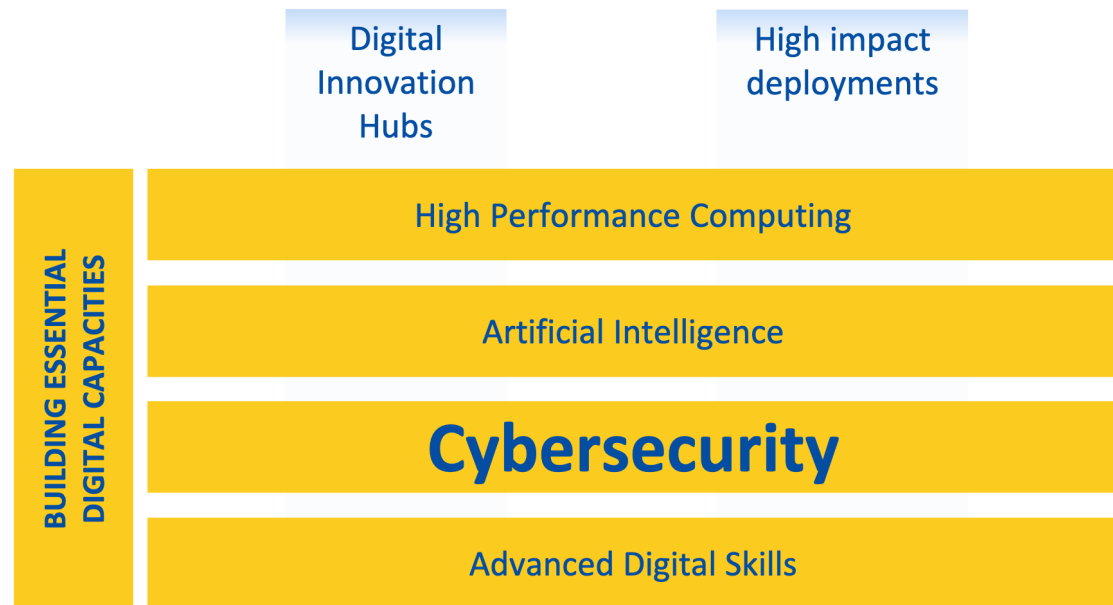
# ECDC mission

- **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;

# ECCC 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

Enlarging existing or Launching  
New Cross-Border SOC Platforms

Joint Acquisition of Infrastructure,  
Tools and Services

National SOC

Novel applications of AI ... for  
Security Operation Centres

Strengthening the SOC ecosystem

# ECCC in action



## KNOWLEDGE-SHARING EVENT

8 NOVEMBER 2023 HYBRID FROM BRUSSELS

```
0101 001011 10101
11011 001 1101 01
100 110101 000110
11 01110 01 11010
0110 11 01 10 100
```

Cybersecurity Atlas

A knowledge management platform to map, categorise and stimulate collaboration between European cybersecurity experts in support of the EU Digital Strategy.



## EUROPEAN CYBERSECURITY COMPETENCE CENTRE ACCESS-2-FINANCE SERIES

9th May 2023: Copenhagen, Denmark

#CyberMatchmaking



## EUROPEAN CYBERSECURITY COMPETENCE CENTRE ACCESS-2-MARKET SERIES

21 November 2023: Rennes, France

#CyberMatchmaking

# Strategic Agenda



**ECCC**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE

## Strategic Agenda

March 2023



# 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 ?