uni.lu

UNIVERSITÉ DU
LUXEMBOURG

Part 2 & exam

Incident Management

in the context of an Information Security Policy

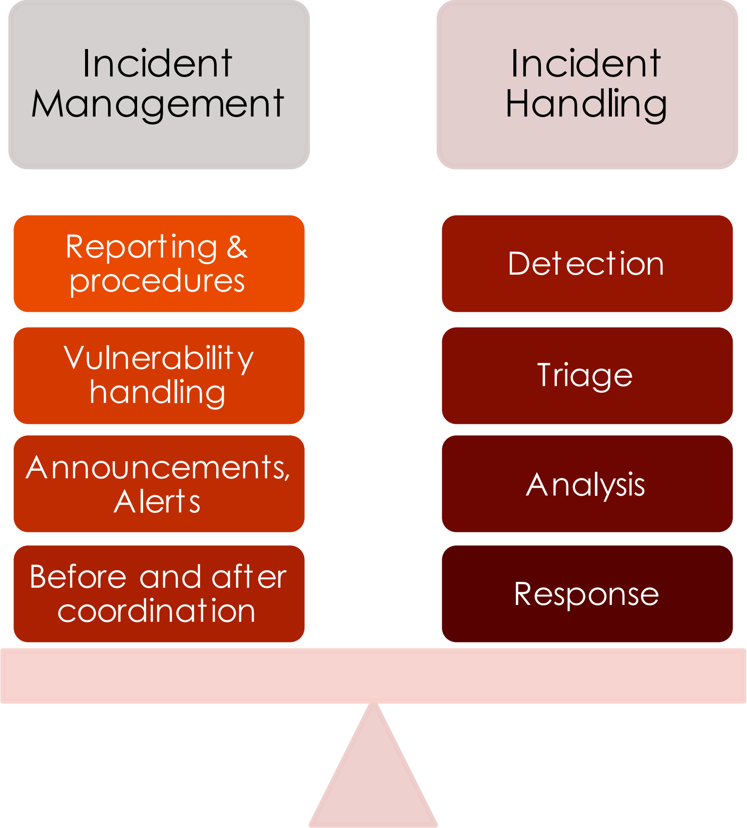
Master in Information System Security Management

2

Part 2

Incident **reporting**, **handling** and **resolution**

Management & Handling


Incident Management

Reporting & procedures

Vulnerability handling

Announcements, Alerts

Before and after coordination

Incident Handling

Detection

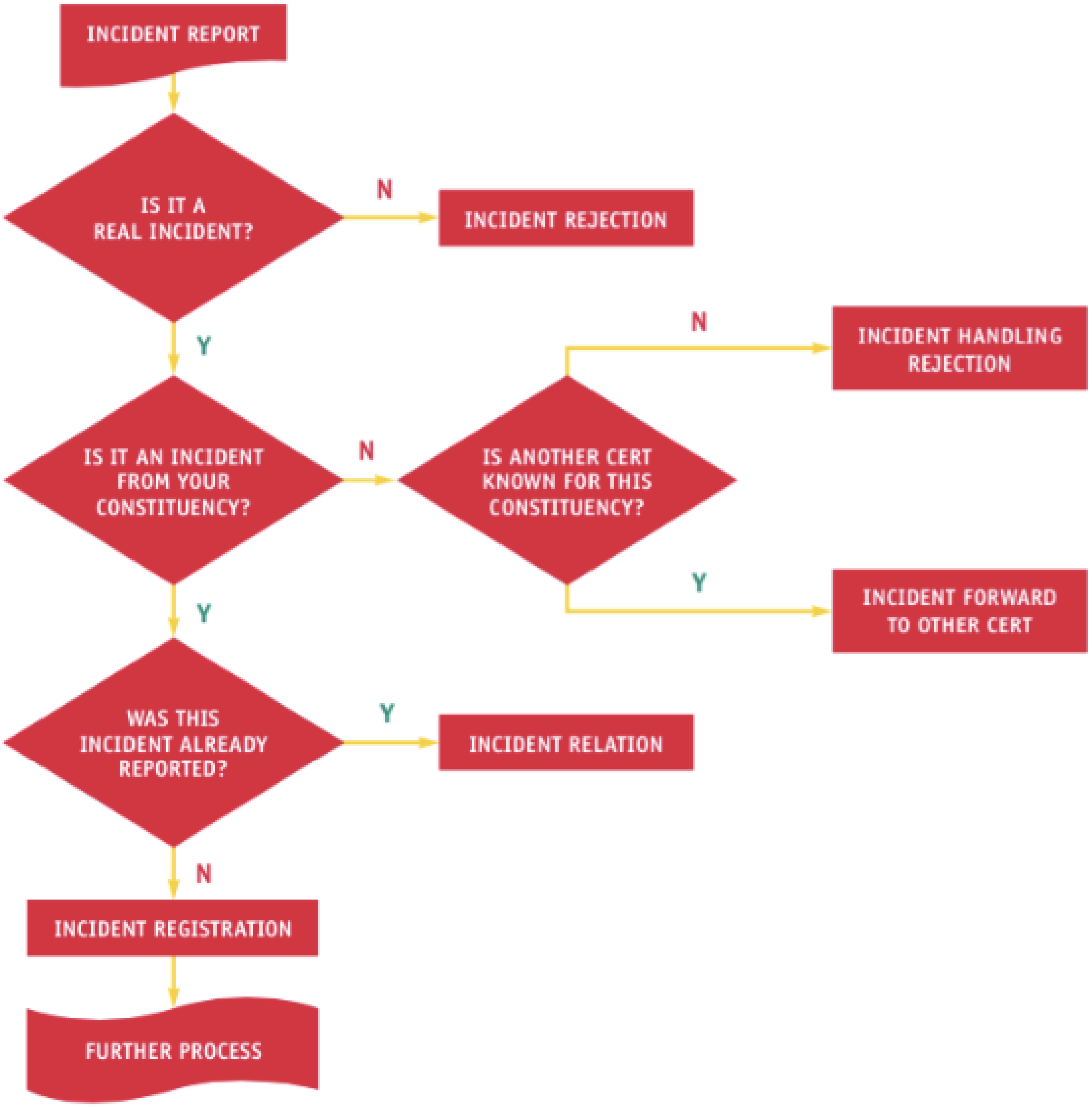
Triage

Analysis

Response

Reporting

Following: ENISA – Incident Management Guide



INCIDENT REPORT

IS IT A REAL INCIDENT?

N

INCIDENT REJECTION

Y

IS IT AN INCIDENT FROM YOUR CONSTITUENCY?

N

IS ANOTHER CERT KNOWN FOR THIS CONSTITUENCY?

N

INCIDENT HANDLING REJECTION

Y

INCIDENT FORWARD TO OTHER CERT

Y

WAS THIS INCIDENT ALREADY REPORTED?

Y

INCIDENT RELATION

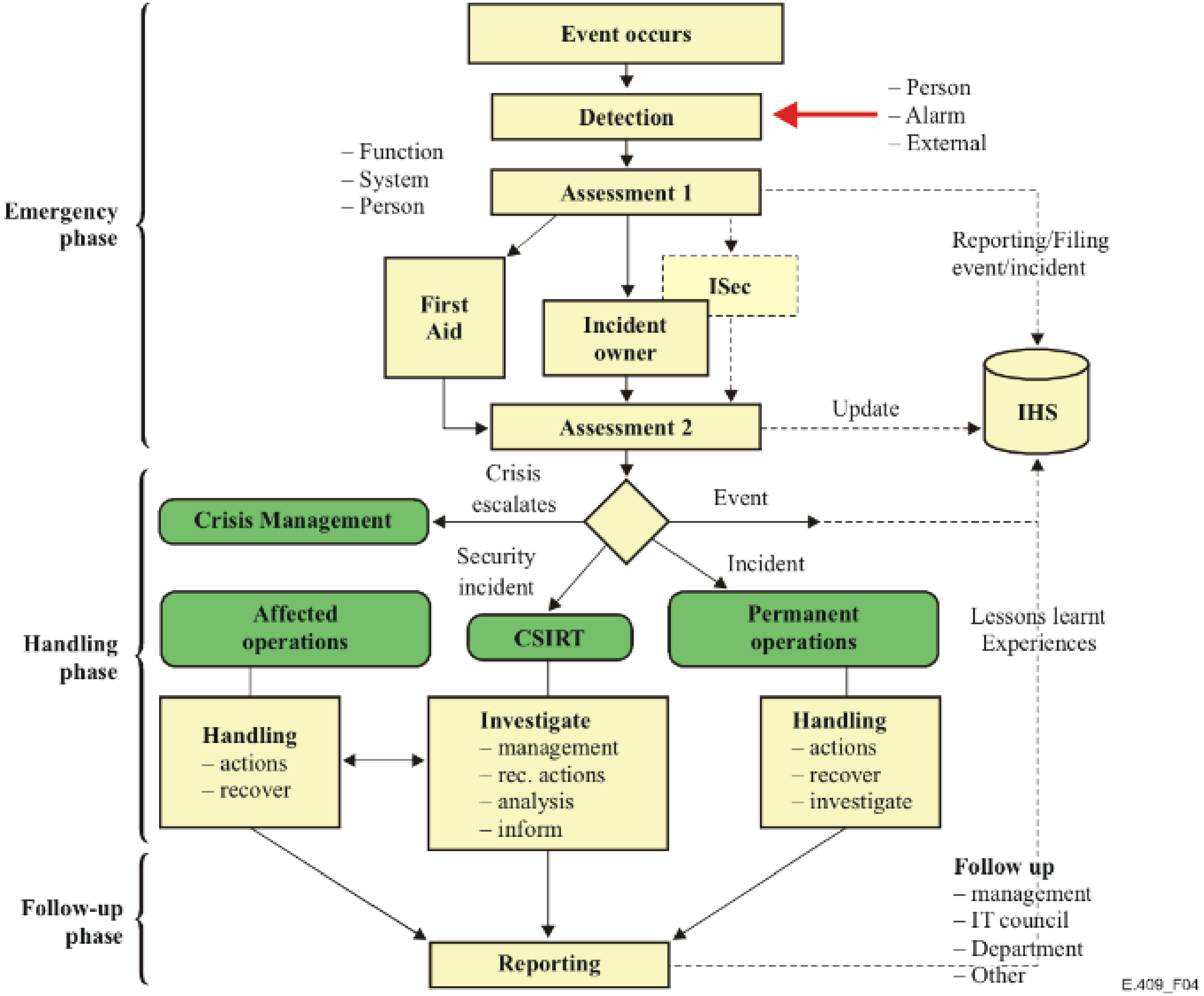
N

INCIDENT REGISTRATION

FURTHER PROCESS

Handling

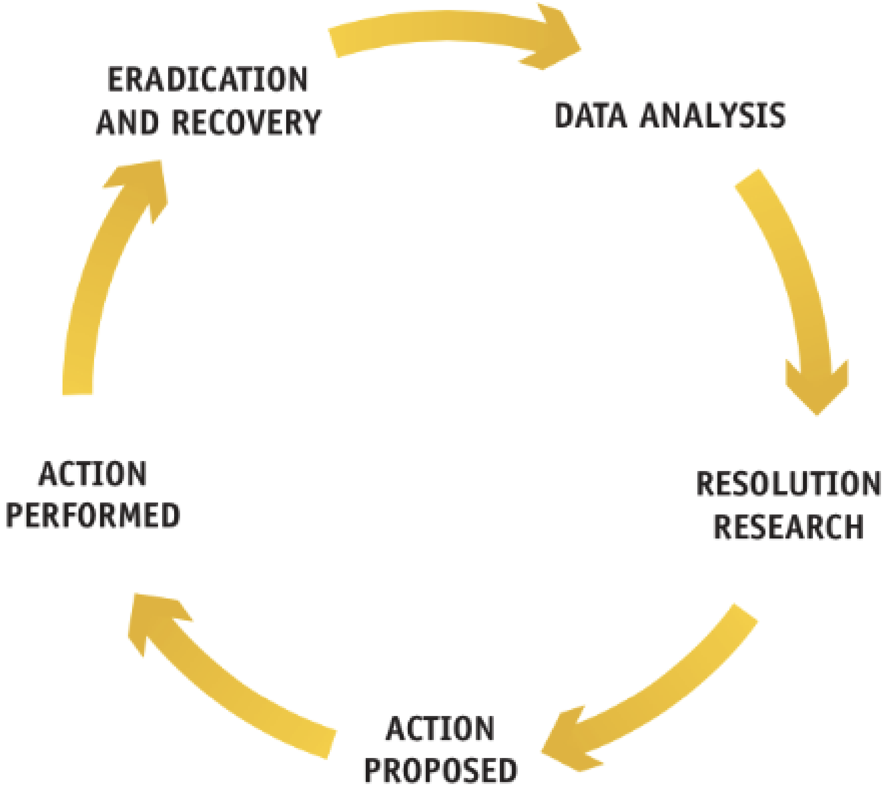
Following: ITU-T E.409 – Incident organization and security incident handling


Emergency phase
Handling phase
Follow-up phase
Event occurs
Detection
– Person
– Alarm
– External
– Function
– System
– Person
Assessment 1
First Aid
Incident owner
ISec
Reporting/Filing event/incident
IHS
Assessment 2
Update
Crisis escalates
Event
Crisis Management
Security incident
Incident
Affected operations
CSIRT
Permanent operations
Lessons learnt Experiences
Handling
– actions
– recover
Investigate
– management
– rec. actions
– analysis
– inform
Handling
– actions
– recover
– investigate
Follow up
– management
– IT council
– Department
– Other
Reporting
E.409_F04

Resolution Cycle

Following: ENISA – Incident Management Guide

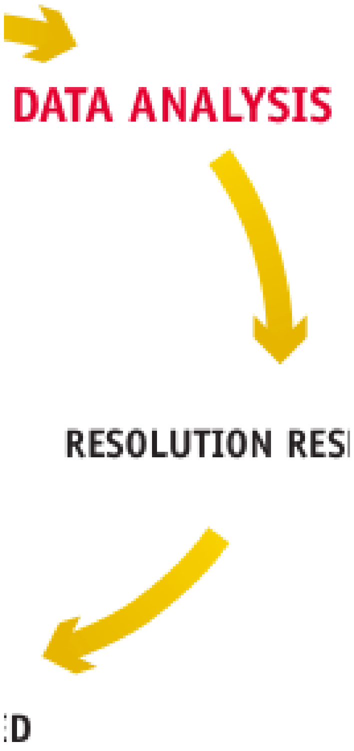
Incident resolution cycle



(I) Data analysis - collection

- Information to get from the reporter:
  - detailed contact information
  - detailed description of the incident
  - incident classification suggested by the incident reporter
  - logs
  - the exact time of the incident
  - operating systems and network setup
  - security systems setup (eg, antivirus software or firewall)
  - incident severity (in the incident reporter's opinion)

(I) Data analysis - correlation



- Monitoring systems:
  - information related to the IP addresses involved in network monitoring systems (e.g., netflow database).
- Referring database:
  - check if this kind of incident or this incident reporter are already in your incident database.
- Other sources:
  - relevant log-files (routers, firewalls, proxy servers, switches, web application, mail servers, DHCP servers, authentication servers, etc.).

(II) Research resolution

ANALYSIS

RESOLUTION RESEARCH

- Based on analysis, team brainstorming on resolution
- Avoid the pitfall of perfectionism
- Sometimes a quick response has the same or a higher value than a comprehensive and complete understanding

(III) Actions - preparation

- Prepare a set of concrete and practical tasks for each party involved
- Remember to adjust your language

(III) Actions - internal

- Attack target
  - How to stop and mitigate an ongoing attack:
    - turn off a service
    - check the system for malware
    - patch a system or an application
    - perform or order an audit if you are not able to improve your system security yourself
  - How to deliver more data:
    - concrete practical instructions (e.g. how to obtain a full e-mail header)

(III) Actions - external

- ISP/ICP
  - To collect, save and archive data.
  - To monitor network traffic related to the case and inform you if something important happens.
  - To filter network traffic in the case of an ongoing attack if such filtering can help to stop or mitigate it.

(III) Actions - external

- CERTs
  - To contact the local ISP/ICP within its constituency
  - To ask for advice on how to deal with an incident
- Law enforcement:
  - To follow a case if it is significant (e.g. you suspect organised crime activity)
  - To assist the reporter of a crime if an incident is to be reported to the police

(IV) Monitor performance

ERADICATIO
AND RECOVE
ACTION
PERFORMED

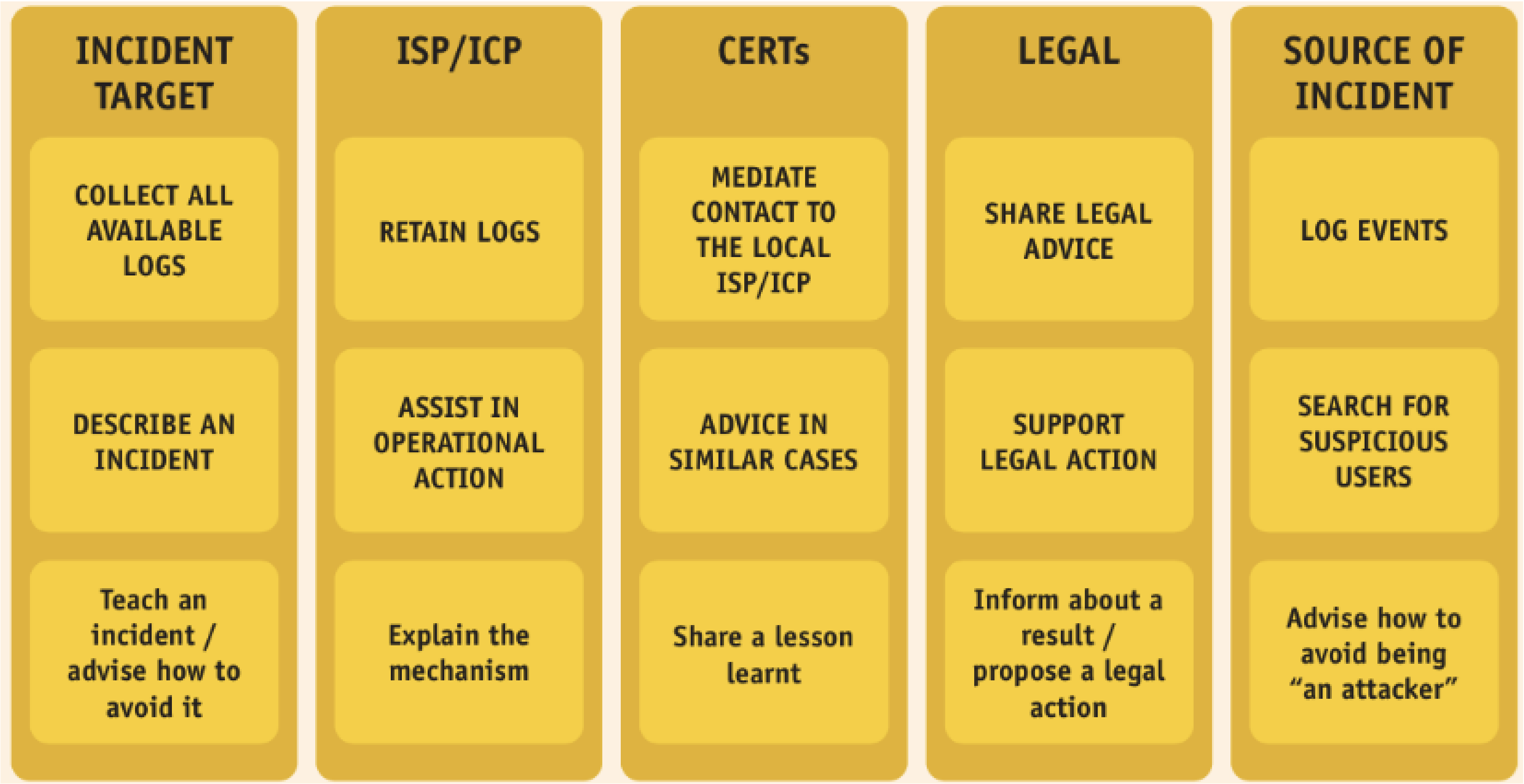
- Basic rules for monitoring the performance of actions:
  - Is the attack target's service turned off?
  - Is the attack target's service still vulnerable?
  - Is the traffic which should be filtered still visible in the network?

(V) Recovery

ERADICATION AND RECOVERY
ACTION PERFORMED

- Recover or restore to normal the service that was attacked during the incident

Incident closure, lessons learned & improvements



INCIDENT TARGET	ISP/ICP	CERTs	LEGAL	SOURCE OF INCIDENT
COLLECT ALL AVAILABLE LOGS	RETAIN LOGS	MEDIATE CONTACT TO THE LOCAL ISP/ICP	SHARE LEGAL ADVICE	LOG EVENTS
DESCRIBE AN INCIDENT	ASSIST IN OPERATIONAL ACTION	ADVICE IN SIMILAR CASES	SUPPORT LEGAL ACTION	SEARCH FOR SUSPICIOUS USERS
Teach an incident / advise how to avoid it	Explain the mechanism	Share a lesson learnt	Inform about a result / propose a legal action	Advise how to avoid being "an attacker"

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

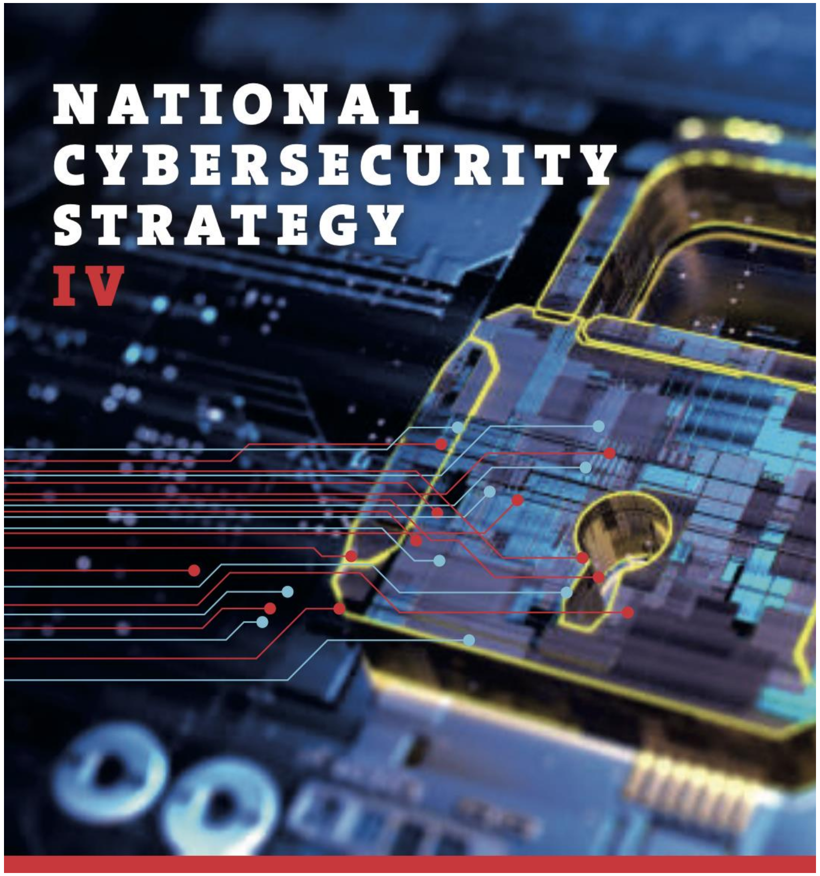
OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS (2002)

TODAY

NATIONAL STRATEGY

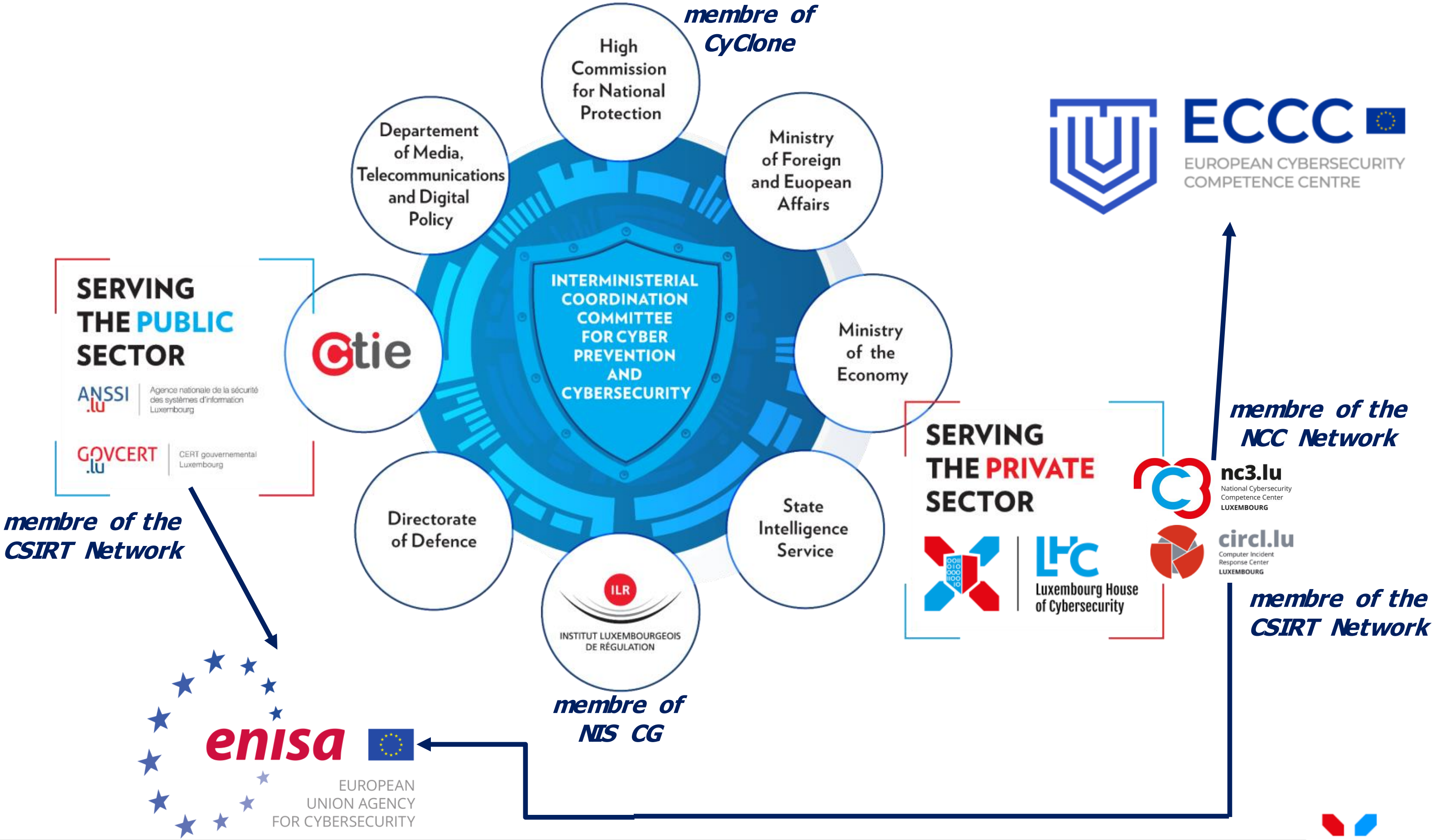
2021-2025

- 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 Cybersecurity Strategy IV

NATIONAL GOVERNANCE



INTERMINISTERIAL COORDINATION COMMITTEE FOR CYBER PREVENTION AND CYBERSECURITY

High Commission for National Protection

membre of CyClone

Ministry of Foreign and Euopean Affairs

Ministry of the Economy

State Intelligence Service

INSTITUT LUXEMBOURGEOIS DE RÉGULATION

membre of NIS CG

Directorate of Defence

ctie

Departement of Media, Telecommunications and Digital Policy

SERVING THE PUBLIC SECTOR

ANSSI .lu Agence nationale de la sécurité des systèmes d'information Luxembourg

GOVCERT .lu CERT gouvernemental Luxembourg

membre of the CSIRT Network

SERVING THE PRIVATE SECTOR

Luxembourg House of Cybersecurity

nc3.lu National Cybersecurity Competence Center LUXEMBOURG

circl.lu Computer Incident Response Center LUXEMBOURG

membre of the NCC Network

membre of the CSIRT Network

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

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)** Network and Information Security **(DORA)**
  (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)

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Haut-Commissariat
à la protection nationale

GOVCERT.lu CERT gouvernemental Luxembourg

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

GOVCERT.lu CERT gouvernemental Luxembourg

CSSF Commission de Surveillance du Secteur Financier

ILR INSTITUT LUXEMBOURGEOIS DE RÉGULATION

circl.lu Computer Incident Response Center LUXEMBOURG

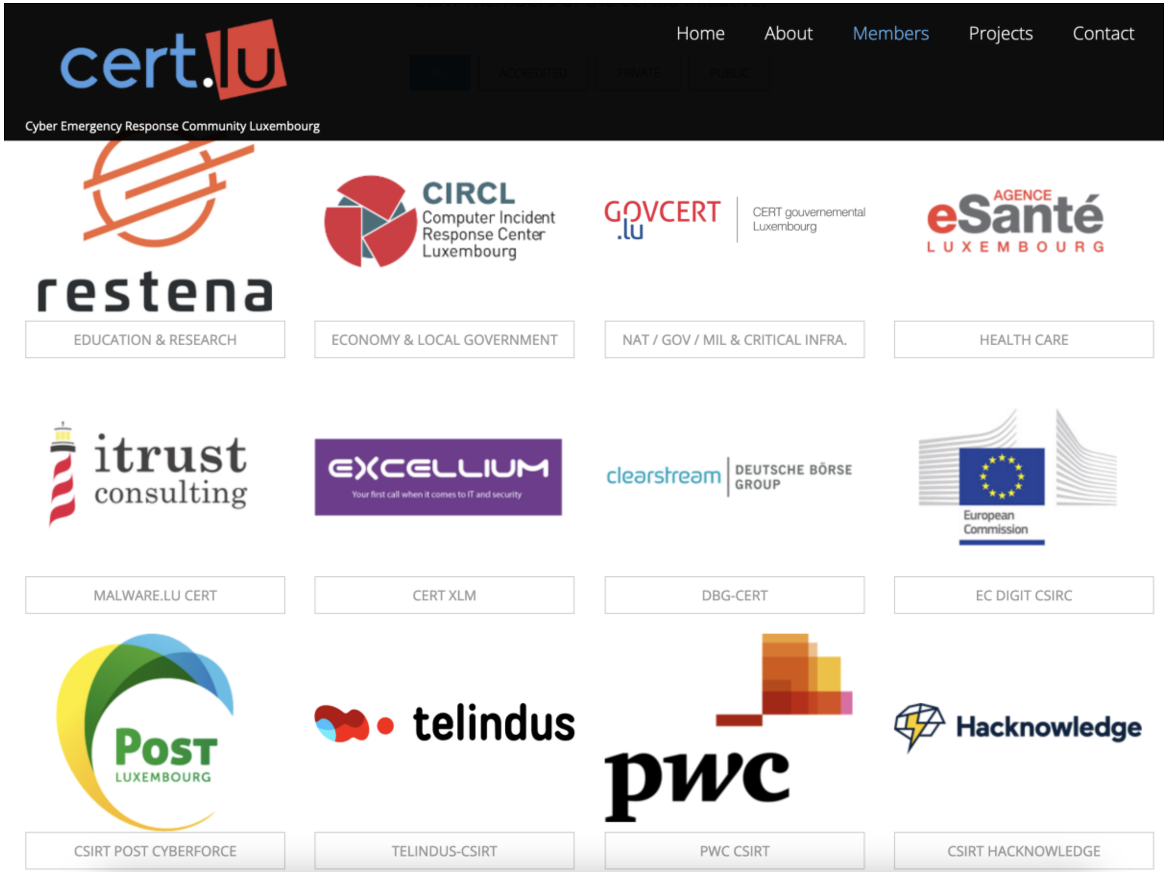
ILNAS Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services

CSSF Commission de Surveillance du Secteur Financier

=> more on cybersecurity.lu

PREPAREDNESS & RESPONSE

PUBLIC-PRIVATE COOPERATION IN ACTION



EDUCATION & RESEARCH

ECONOMY & LOCAL GOVERNMENT

NAT / GOV / MIL & CRITICAL INFRA.

HEALTH CARE

MALWARE.LU CERT

CERT XLM

DBG-CERT

EC DIGIT CSIRC

CSIRT POST CYBERFORCE

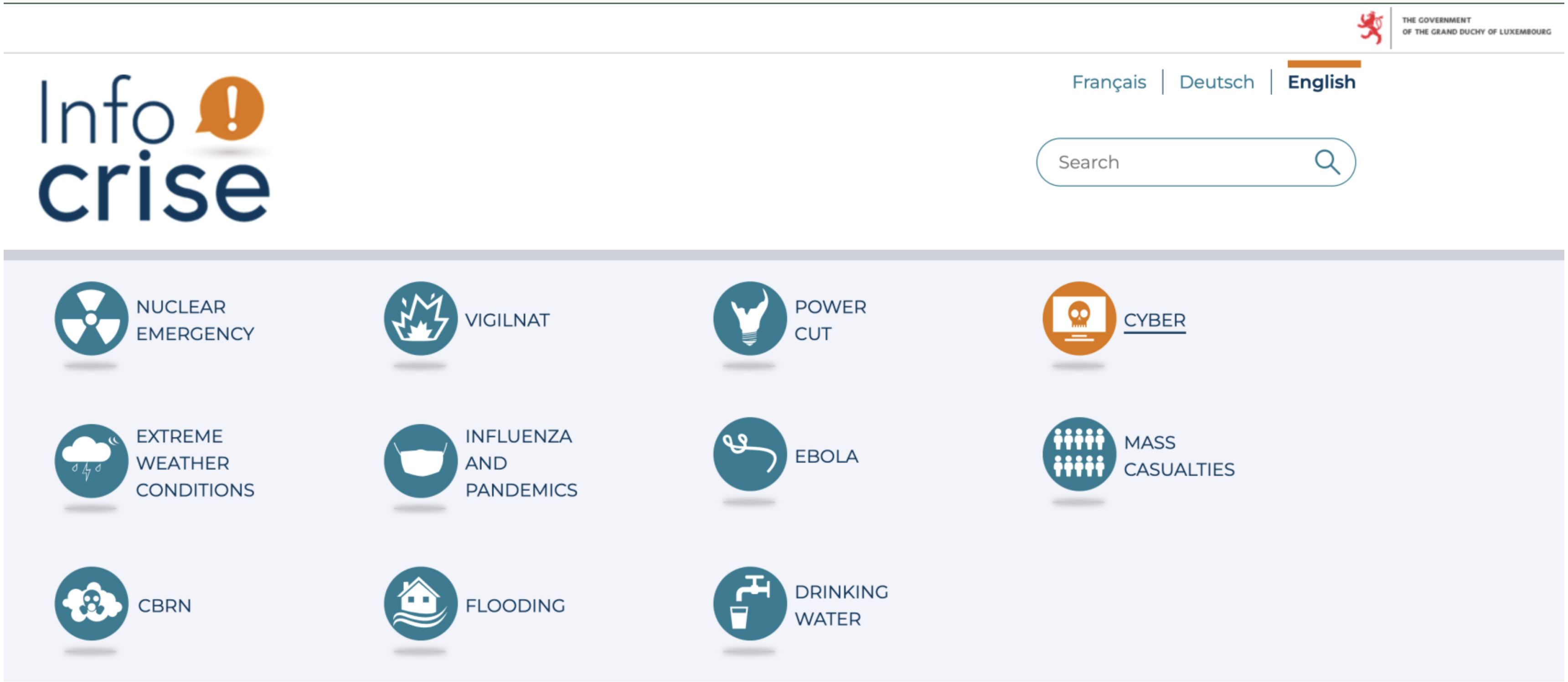
TELINDUS-CSIRT

PWC CSIRT

CSIRT HACKNOWLEDGE

PREPAREDNESS & RESPONSE

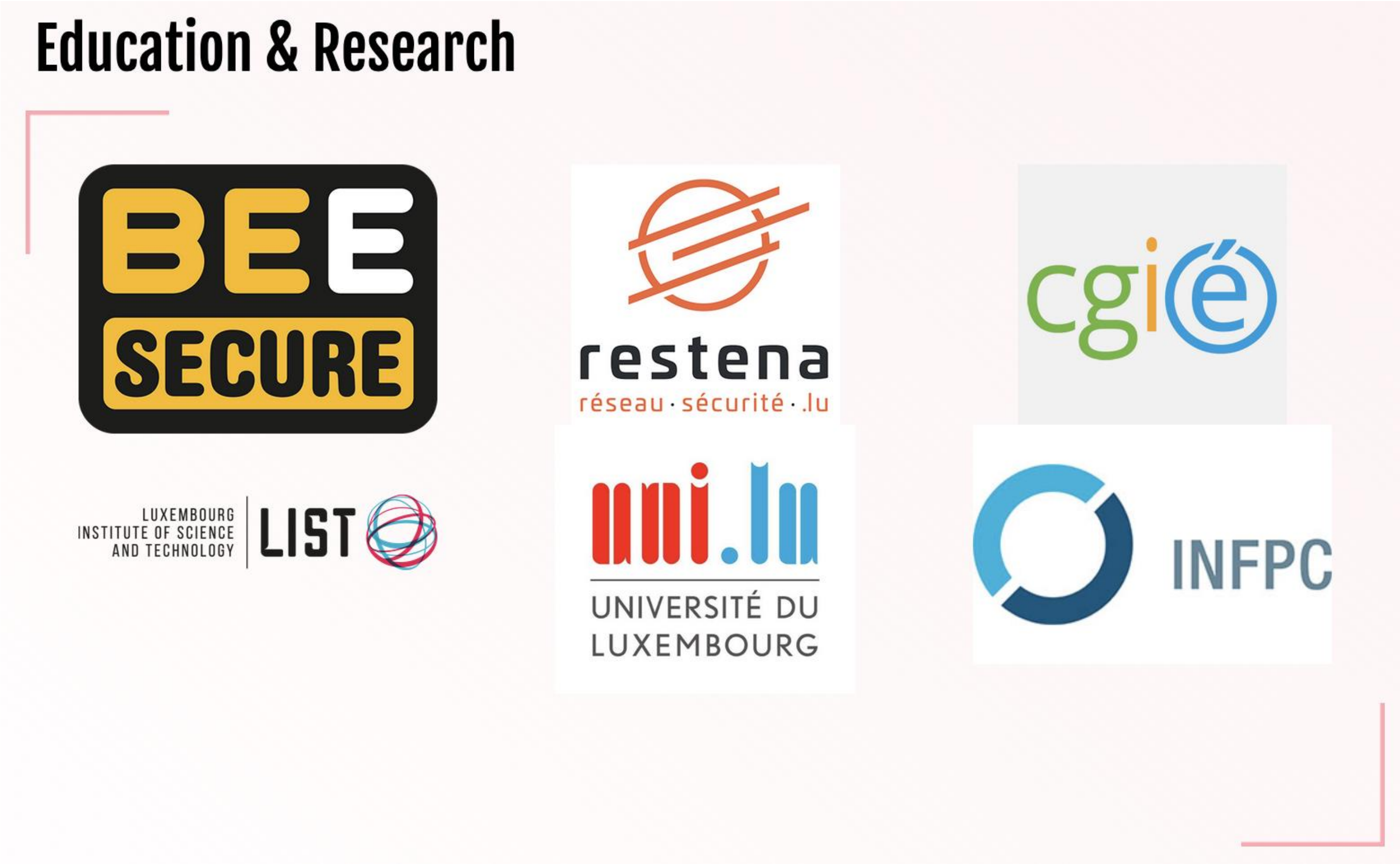
PIU CYBER



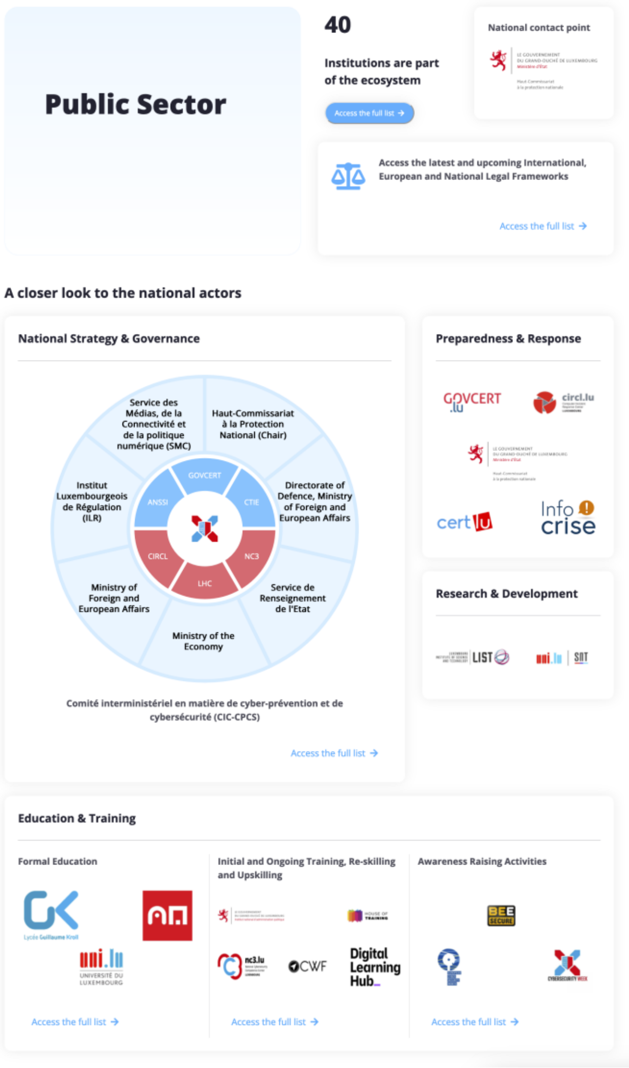
LU-CIX

DDoS Scrubbing Center

EDUCATION & RESEARCH



Education & Research



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

Service des Médias, de la Connectivité et de la politique numérique (SMC)
Haut-Commissariat à la Protection National (Chair)
Directorate of Defence, Ministry of Foreign and European Affairs
Service de Renseignement de l'Etat
Ministry of the Economy
Ministry of Foreign and European Affairs
Institut Luxembourgeois de Régulation (ILR)
GOVCERT
CTIE
NC3
LHC
CIRCL
ANSSI

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 →

luxembourg.lu

ITY
RG

The Ecosystem Dashboar

e interactive dashboard of the Luxembourg Cybersecurity Ecosystem. It presents a com relevant cybersecurity key figures in the Grand-Duchy.

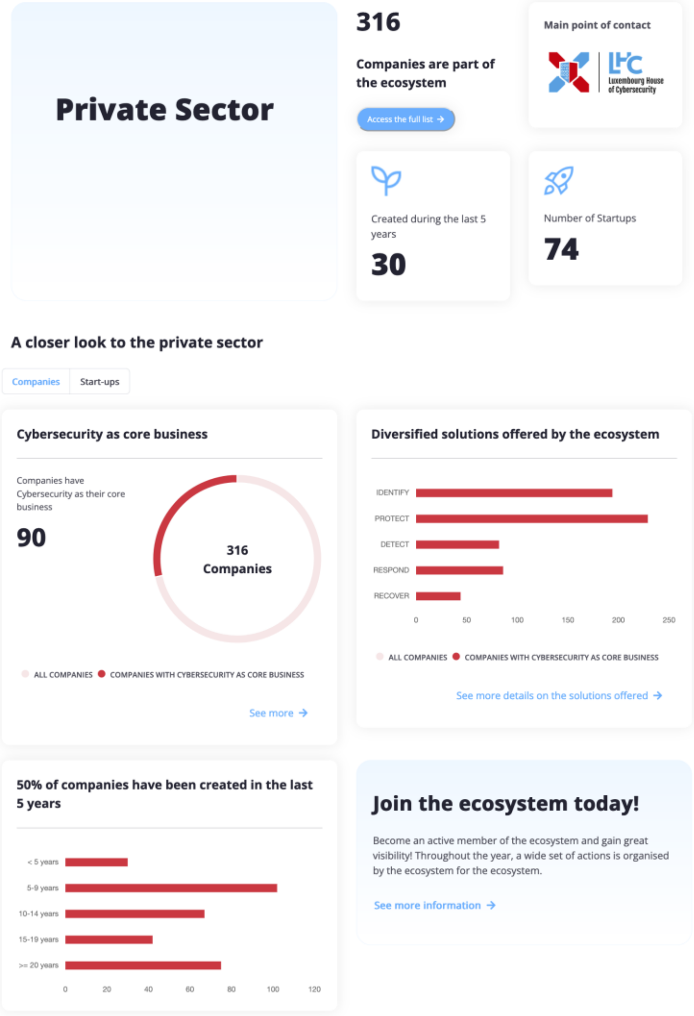
ystem
view

369

Entities are part of the ecosystem

Public Entities

40



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

Cybersecurity as core business

Companies have Cybersecurity as their core business

90

See more →

Diversified solutions offered by the ecosystem

See more details on the solutions offered →

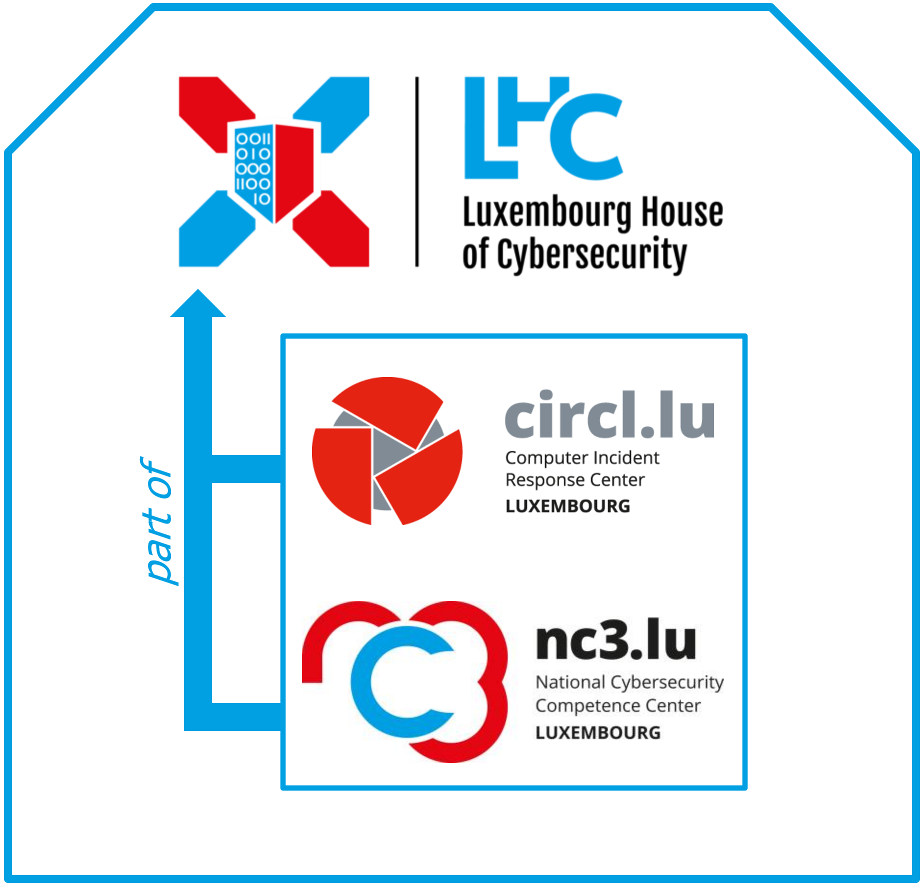
50% of companies have been created in the last 5 years

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 the private sector



LHC

Luxembourg House of Cybersecurity

part of

circl.lu

Computer Incident Response Center

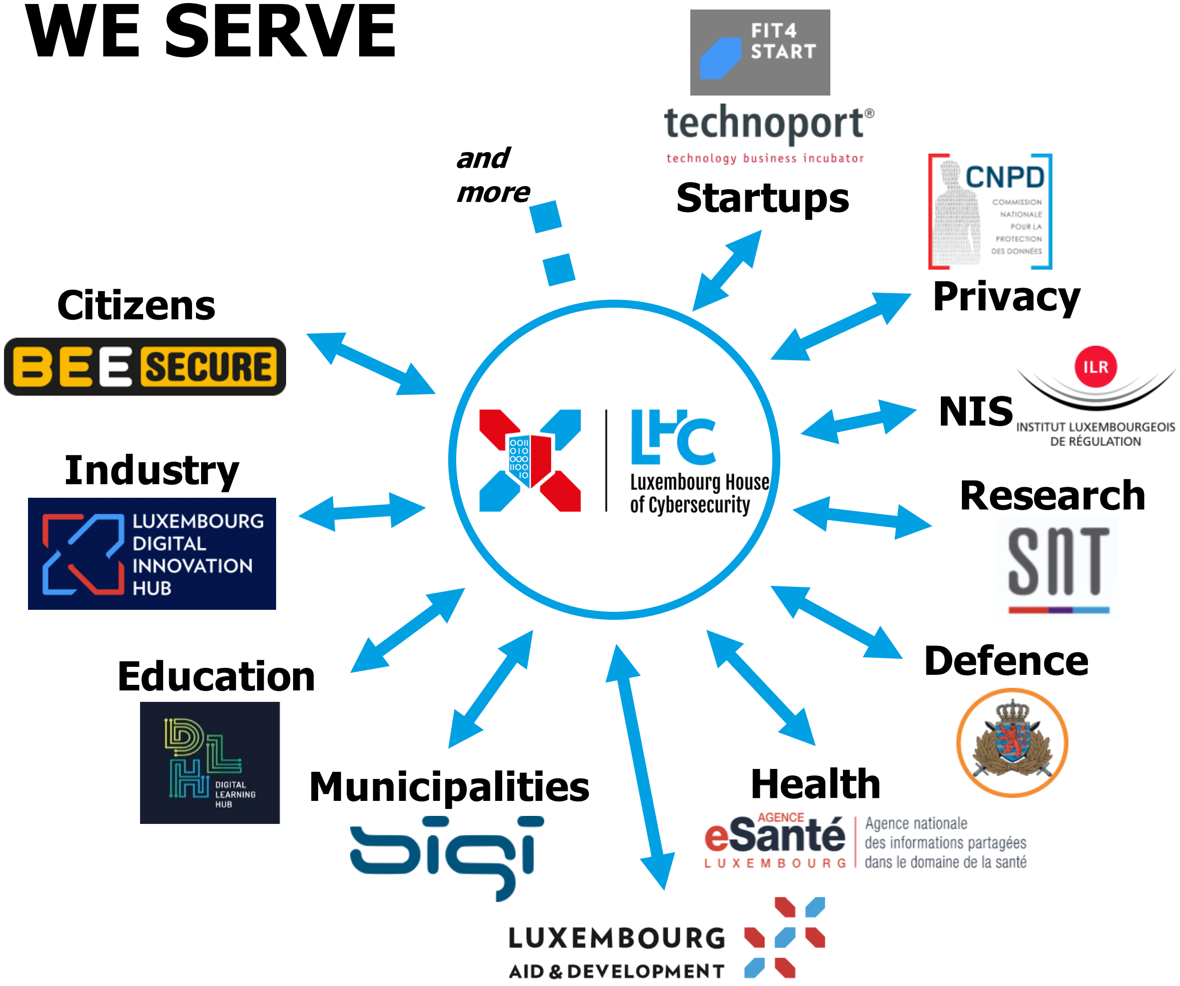
LUXEMBOURG

nc3.lu

National Cybersecurity Competence Center

LUXEMBOURG

WE SUPPORT
WE FOSTER
WE SERVE



Luxembourg House of Cybersecurity

and more

Startups

FIT4 START

technoport®
technology business incubator

Privacy

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

NIS

ILR
INSTITUT LUXEMBOURGEOIS DE RÉGULATION

Research

SnT

Defence

Health

AGENCE eSanté LUXEMBOURG
Agence nationale des informations partagées dans le domaine de la santé

LUXEMBOURG AID & DEVELOPMENT

Municipalities

SIGI

Education

DIGITAL LEARNING HUB

Industry

LUXEMBOURG DIGITAL INNOVATION HUB

Citizens

BEE SECURE

WE HOST

ENCRYPTION EUROPE

ISACA
Luxembourg Chapter

CWF
DIVERSITY & INNOVATION IN CYBERSECURITY
BRUSSELS | LUXEMBOURG

Women Cyber Force

clusil

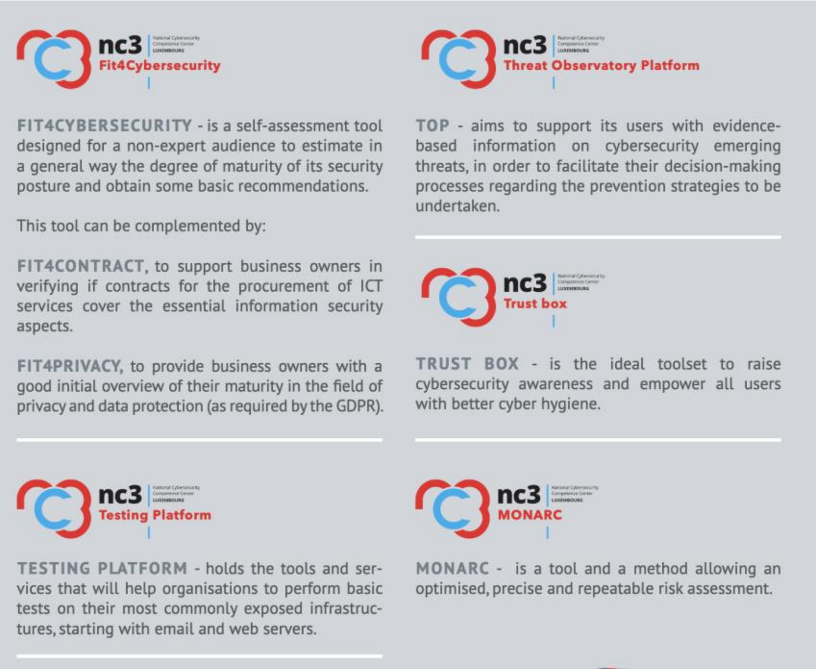
National Cybersecurity Competence Centre

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

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

ROOM #42
room42.eu DØ[N'T]PANIC

SPAMBEE



nc3 Fit4Cybersecurity

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).

nc3 Threat Observatory Platform

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.

nc3 Trust box

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

nc3 Testing Platform

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.

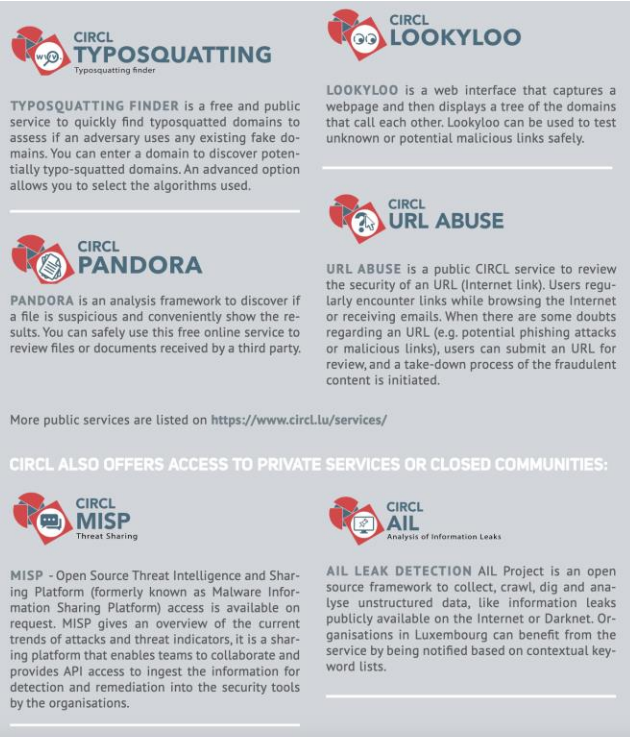
nc3 MONARC

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

Computer Incident Response Center Luxembourg

circl.lu
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
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
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
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.

MISP
Threat Sharing

pandora
analysis framework

ail project

Digital Security Risk Management for Economic and Social Prosperity

OECD Recommendation and Companion Document

OECD

BETTER POLICIES FOR BETTER LIVES

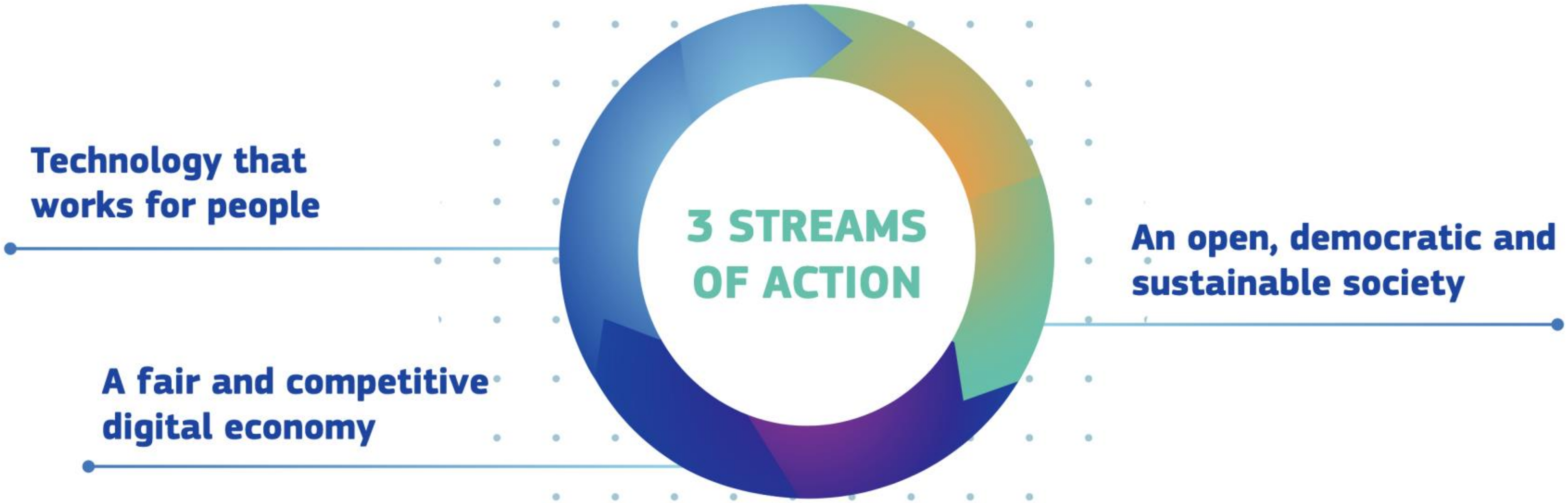
2015

"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"

Cybersecurity for Europe

- The 3 strategies shaping EU’s *cyber* future
- “Team cyber” for Europe
- Horizon & Digital Europe Programmes
- ECCC, the Network & the Community
  a bottom-up approach to achieve cybersecurity excellence for Europe

Strategy for Shaping Europe's Digital Future



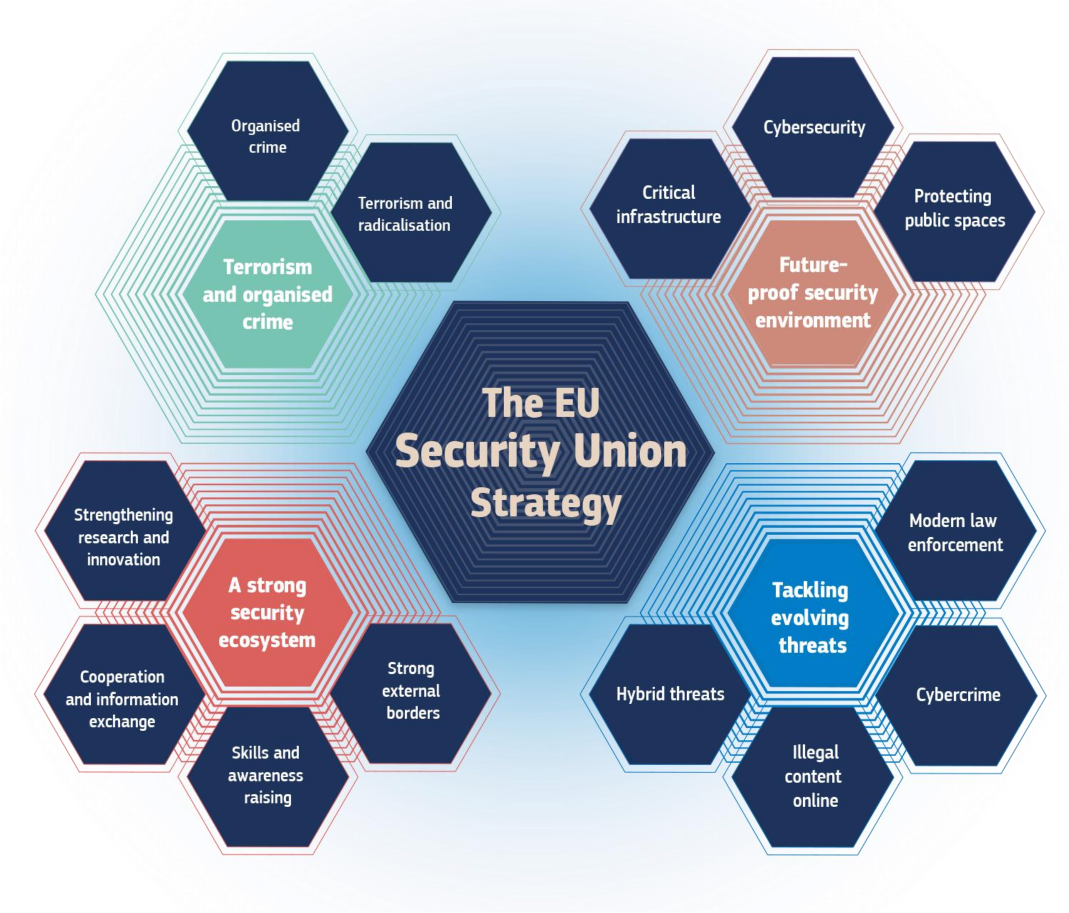
Technology that works for people

3 STREAMS OF ACTION

An open, democratic and sustainable society

A fair and competitive digital economy

European Security Union Strategy


Organised crime
Terrorism and radicalisation
Terrorism and organised crime
Cybersecurity
Critical infrastructure
Protecting public spaces
Future-proof security environment
The EU Security Union Strategy
Strengthening research and innovation
A strong security ecosystem
Cooperation and information exchange
Skills and awareness raising
Strong external borders
Modern law enforcement
Tackling evolving threats
Hybrid threats
Cybercrime
Illegal content online

EU Cybersecurity Strategy

1. Resilience, technological sovereignty and leadership
2. Building operational capacity to prevent, deter and respond
3. Advancing a global and open cyberspace through increased cooperation

- NIS2, **ECCC**, cybersecurity shield (SOC), DIHs
- **ENISA**, CERT-EU, JCU, Defense Fund
- Cyber Diplomacy, UN AHC, EUCybernet

“Team cyber” for Europe

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

- NIS Coordination Group
- CSIRT Network
- CyCLONe (Cyber Crisis Liaison Network)

ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- The Network (NCCs)
- The Community (Research, Academia, Industry & Civil Society)

ECCC missions

Cybersecurity is a common responsibility and effort, only together can we achieve to cybersecure the EU

- 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;
- 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.

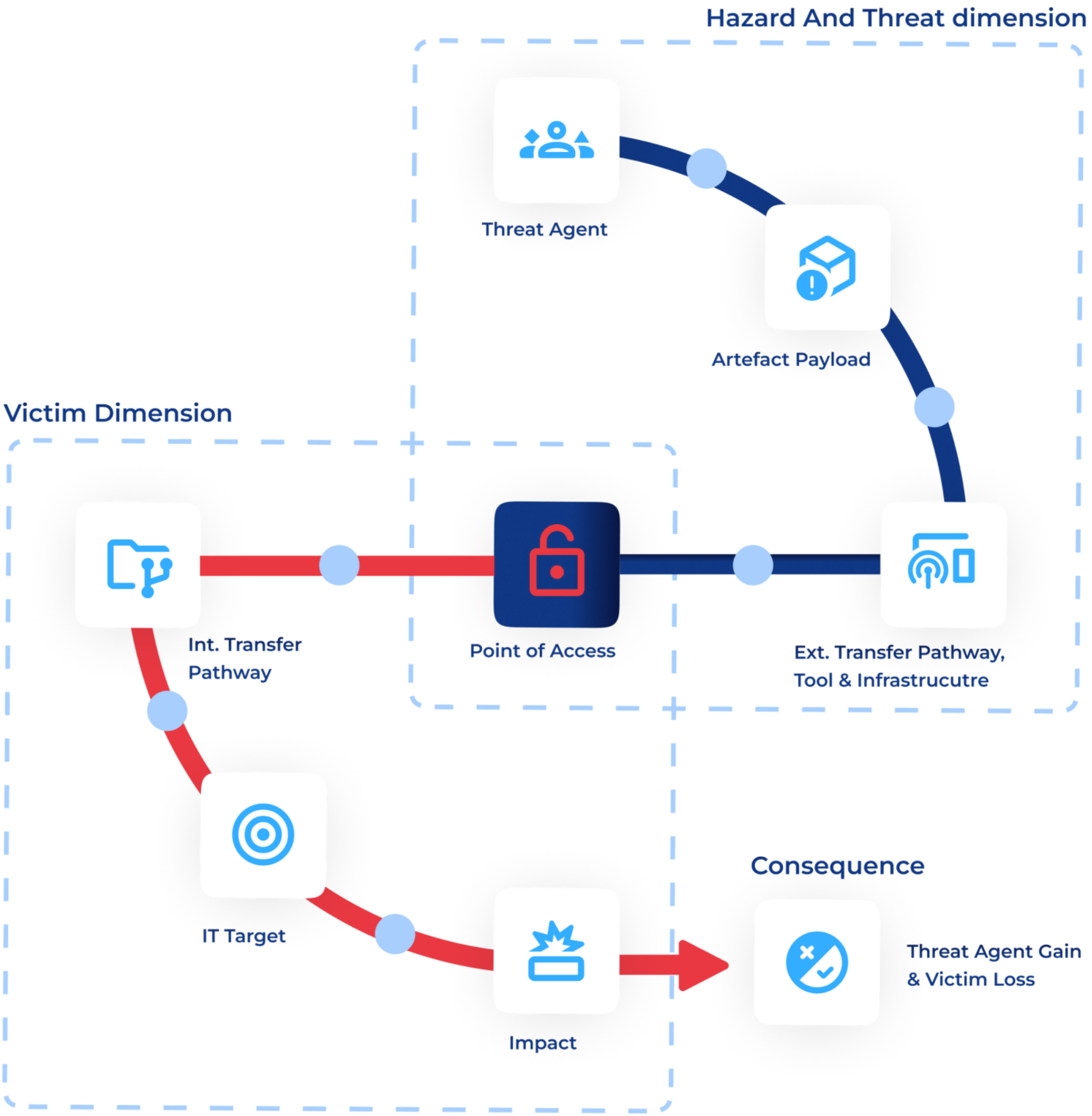
Exam

Homework / Exercice

nc3
Cybersecurity
Observatory

Threat Observatory

By NC3 – National Cybersecurity Competence Centre



Hazard And Threat dimension

Threat Agent

Artefact Payload

Victim Dimension

Int. Transfer Pathway

Point of Access

Ext. Transfer Pathway, Tool & Infrastrucutre

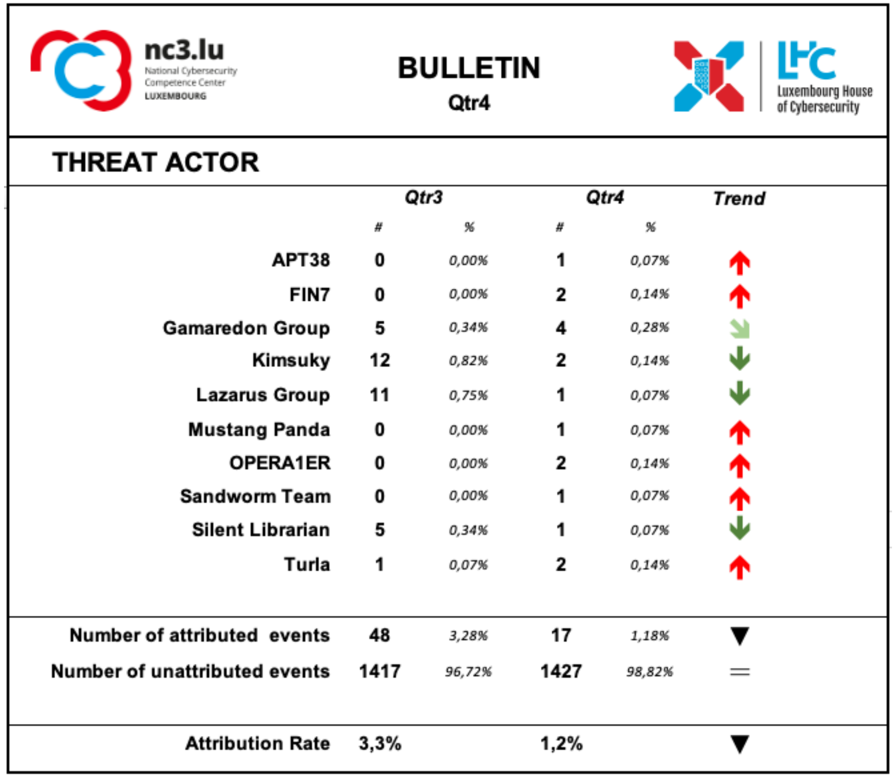
IT Target

Impact

Consequence

Threat Agent Gain & Victim Loss

2022 IV – Quarterly Bulletin



nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

BULLETIN
Qtr4

LHC
Luxembourg House
of Cybersecurity

THREAT ACTOR

	Qtr3		*Qtr4*		*Trend*
	#	*%*	*#*	*%*	
APT38	**0**	*0,00%*	**1**	*0,07%*	↑
FIN7	**0**	*0,00%*	**2**	*0,14%*	↑
Gamaredon Group	**5**	*0,34%*	**4**	*0,28%*	↘
Kimsuky	**12**	*0,82%*	**2**	*0,14%*	↓
Lazarus Group	**11**	*0,75%*	**1**	*0,07%*	↓
Mustang Panda	**0**	*0,00%*	**1**	*0,07%*	↑
OPERA1ER	**0**	*0,00%*	**2**	*0,14%*	↑
Sandworm Team	**0**	*0,00%*	**1**	*0,07%*	↑
Silent Librarian	**5**	*0,34%*	**1**	*0,07%*	↓
Turla	**1**	*0,07%*	**2**	*0,14%*	↑
Number of attributed events	**48**	*3,28%*	**17**	*1,18%*	▼
Number of unattributed events	**1417**	*96,72%*	**1427**	*98,82%*	=
Attribution Rate	**3,3%**		**1,2%**		▼

https://nc3.lu/pages/b2022/q4/b2022q4.html

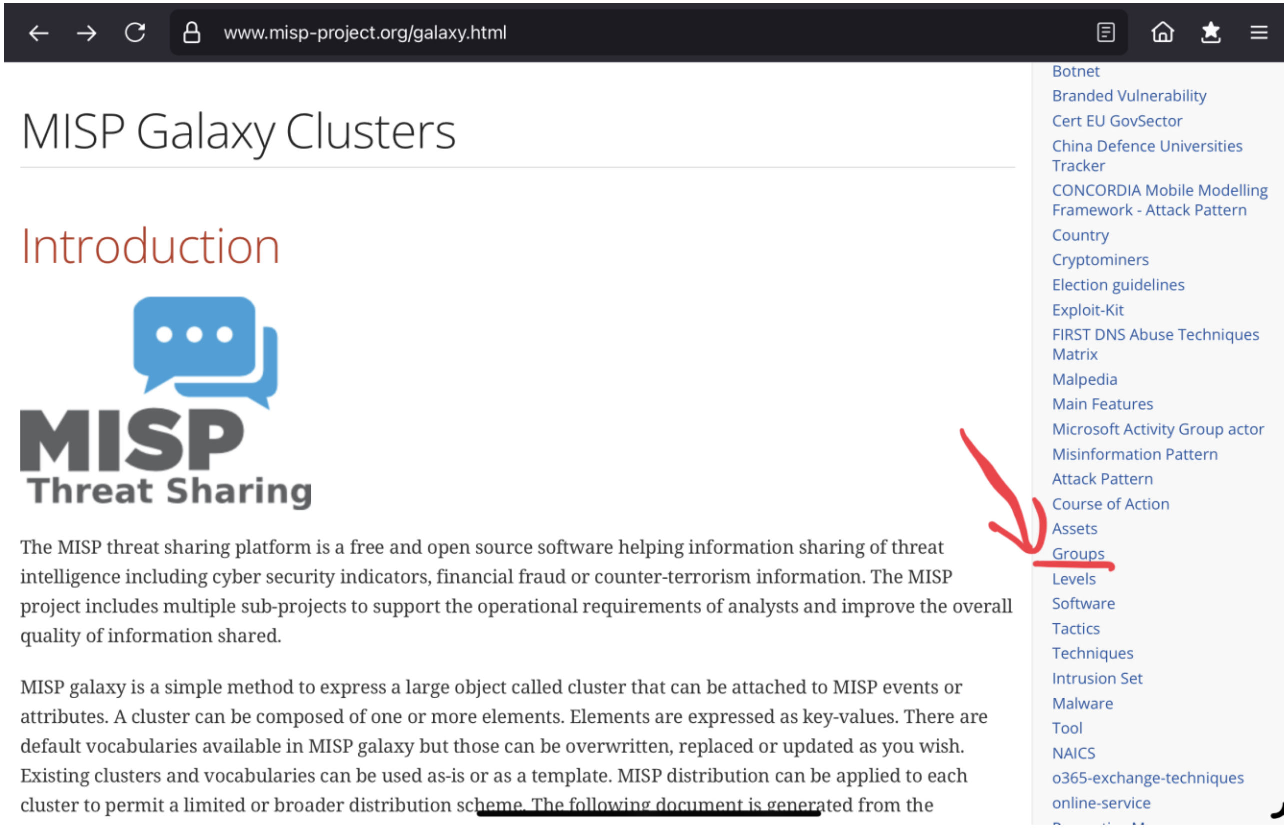
Exercise

- Choose and understand the threat actor
- Identify and select relevant counter-measures (ISO 27002:2022 controls)
- Define implementation
  - In-house: resources (processes, budget, HR, tools, services, etc.)
  - Out-sourced: partners from the ecosystem
- Describe and argument your choices/decisions
- MAX 3-4 pages

Toolbox

- NC3 Threat Observatory
- MISP *Galaxies*
- ISO 27002:2022
- Cybersecurity Luxembourg Ecosystem
- all other resources you see relevant

MISP *(galaxies)*



MISP Galaxy Clusters

Introduction

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

MISP galaxy is a simple method to express a large object called cluster that can be attached to MISP events or attributes. A cluster can be composed of one or more elements. Elements are expressed as key-values. There are default vocabularies available in MISP galaxy but those can be overwritten, replaced or updated as you wish. Existing clusters and vocabularies can be used as-is or as a template. MISP distribution can be applied to each cluster to permit a limited or broader distribution scheme. The following document is generated from the

- Botnet
- Branded Vulnerability
- Cert EU GovSector
- China Defence Universities Tracker
- CONCORDIA Mobile Modelling Framework - Attack Pattern
- Country
- Cryptominers
- Election guidelines
- Exploit-Kit
- FIRST DNS Abuse Techniques Matrix
- Malpedia
- Main Features
- Microsoft Activity Group actor
- Misinformation Pattern
- Attack Pattern
- Course of Action
- Assets
- Groups
- Levels
- Software
- Tactics
- Techniques
- Intrusion Set
- Malware
- Tool
- NAICS
- o365-exchange-techniques
- online-service

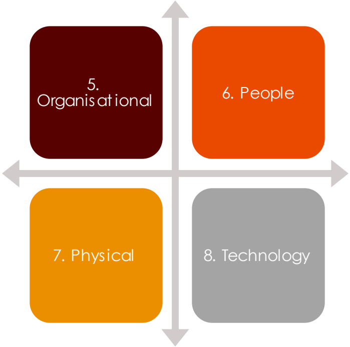
https://www.misp-project.org/galaxy.html

ISO 27002:2022

Information security, cybersecurity and privacy protection – Information security controls

Overview

Themes



The categorisation of controls given in Clauses 5 to 8 are referred to as **themes**:

a) **people**, if they concern individual persons;

b) **physical**, if they concern physical objects;

c) **technological**, if they concern technology;

d) otherwise they are categorised as **organisational**.

Overview

Attributes (1)

Each control has been associated with **five attributes** with corresponding attribute values, as follows:

1) **Control type** is an attribute to view controls from the perspective of **when and how** the control modifies the risk with regard to the occurrence of an information security incident.

2) **Information security** properties is an attribute to view controls from the perspective of which **characteristic of information** the control will contribute to preserving.

3) **Cybersecurity concepts** (ref. ISO/IEC TS 27110)

4) **Operational capabilities** is an attribute to view controls from the **practitioner's perspective** of information security capabilities.

5) **Security domains**

Overview

Attributes (2)

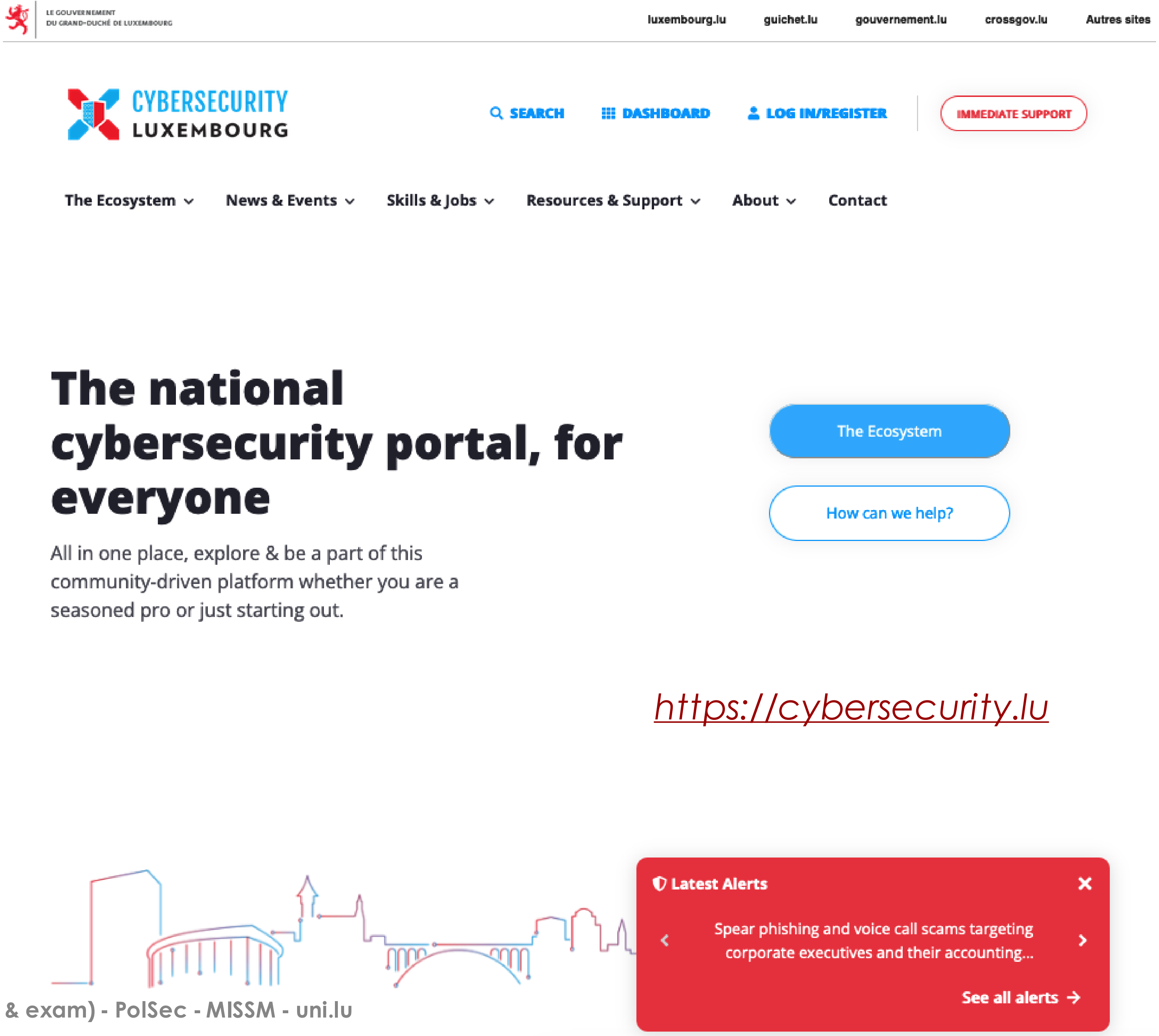
Cybersecurity concepts attribute values consist of:

- **Identify**,
- **Protect**,
- **Detect**,
- **Respond**, and
- **Recover**.

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

CYBERSECURITY LUXEMBOURG

The Luxembourg Cybersecurity Ecosystem



LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

luxembourg.lu guichet.lu gouvernement.lu crossgov.lu Autres sites

CYBERSECURITY LUXEMBOURG

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

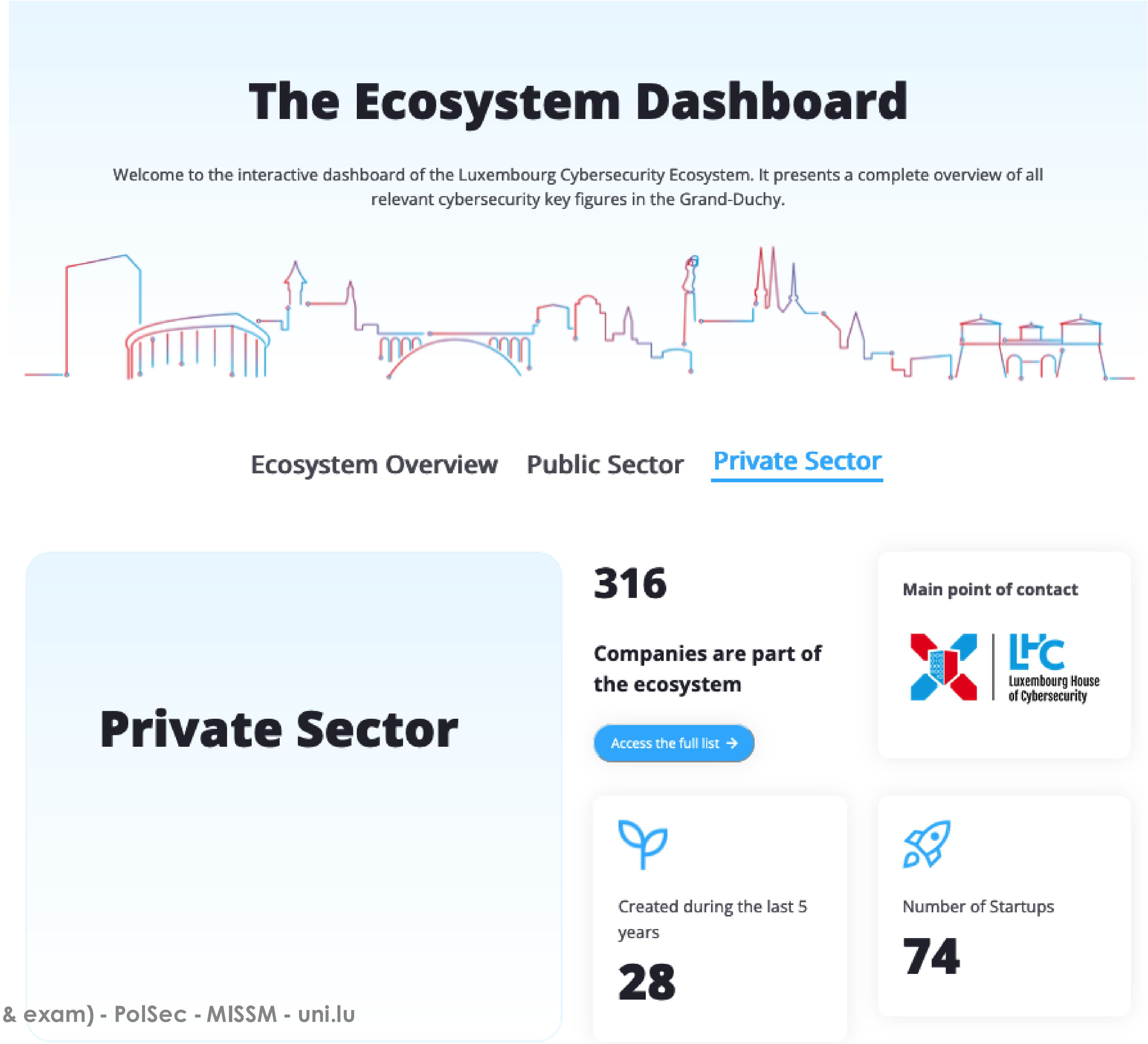
How can we help?

Latest Alerts

Spear phishing and voice call scams targeting corporate executives and their accounting...

See all alerts →

https://cybersecurity.lu



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.

Private Sector

316

Companies are part of the ecosystem

Main point of contact

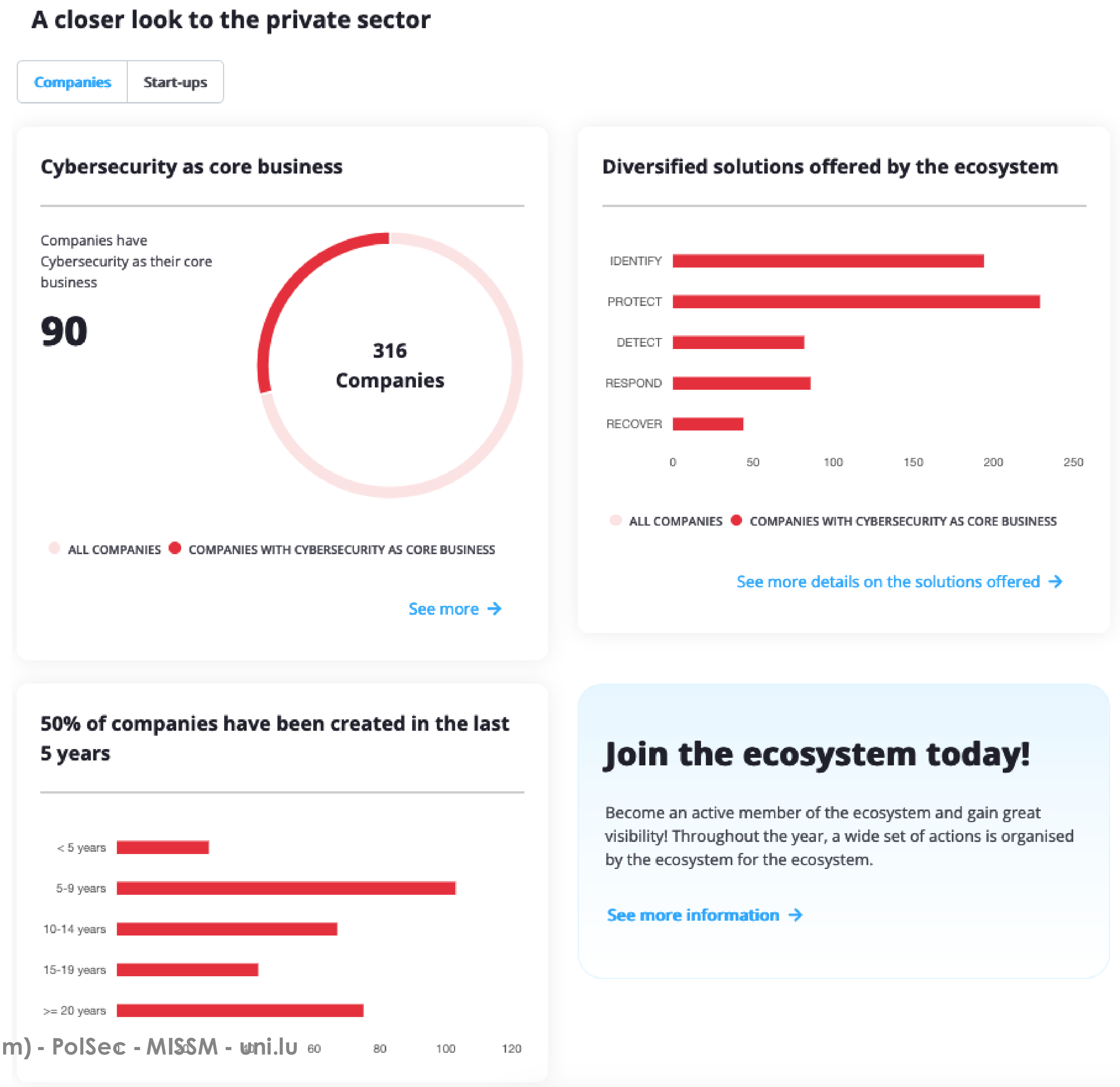
LHC
Luxembourg House
of Cybersecurity

Created during the last 5 years

28

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

See more →

Diversified solutions offered by the ecosystem

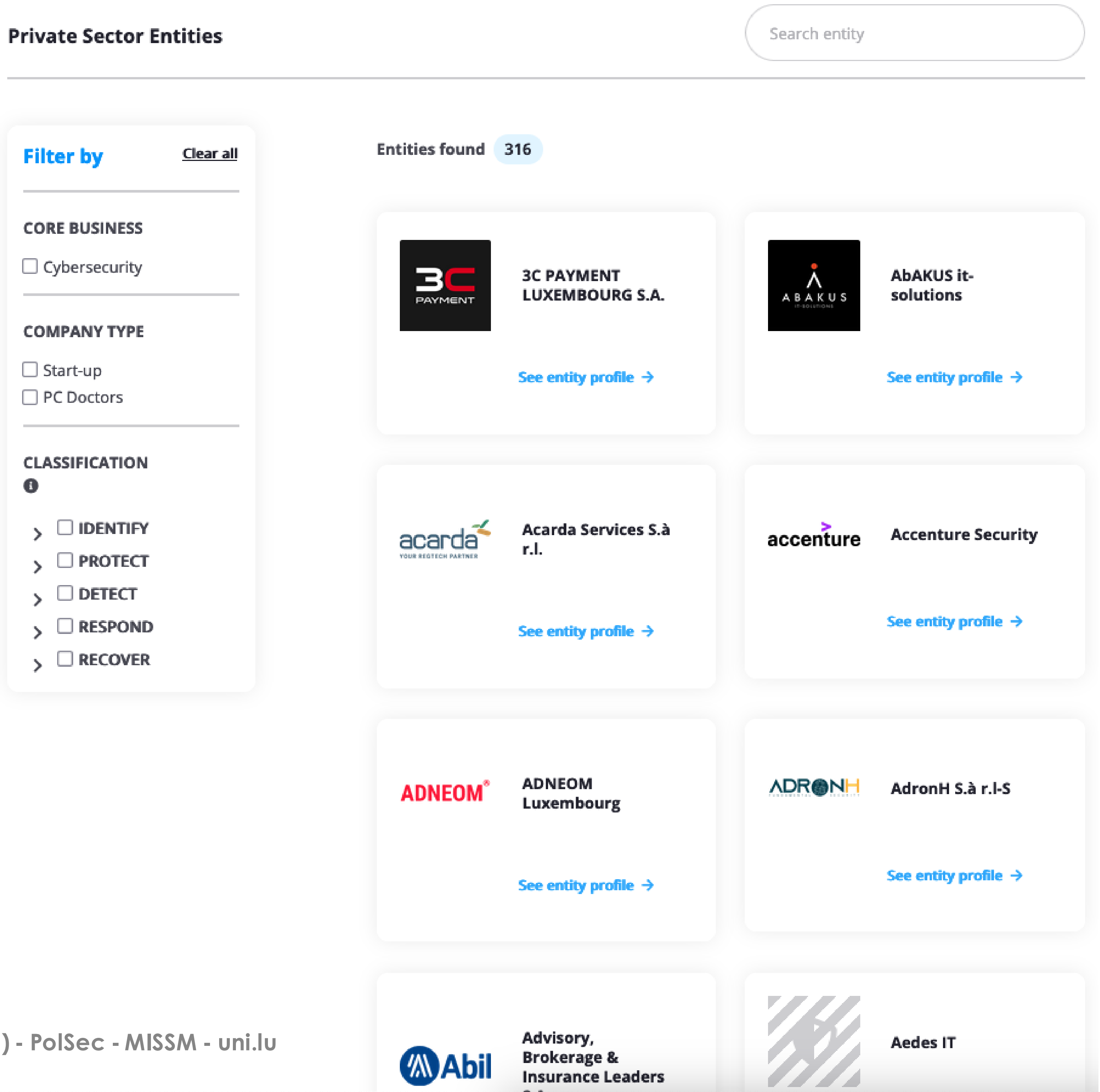
See more details on the solutions offered →

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 Entities

Search entity

Filter by Clear all

CORE BUSINESS

□ Cybersecurity

COMPANY TYPE

□ Start-up
□ PC Doctors

CLASSIFICATION

› □ IDENTIFY
› □ PROTECT
› □ DETECT
› □ RESPOND
› □ RECOVER

Entities found 316

3C PAYMENT LUXEMBOURG S.A.
See entity profile →

AbAKUS it-solutions
See entity profile →

Acarda Services S.à r.l.
See entity profile →

Accenture Security
See entity profile →

ADNEOM Luxembourg
See entity profile →

AdronH S.à r.l-S
See entity profile →

Advisory, Brokerage & Insurance Leaders

Aedes IT

Thank you for your attention

CISO community space

https://lhc.lu/service/luxchat