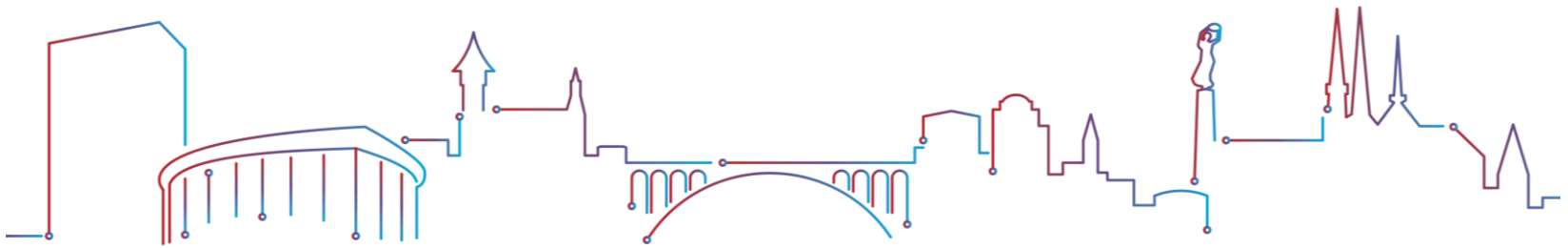
Securing Luxembourg's Digital Future: Government-Backed Cybersecurity Initiatives and Funding Opportunities

by Luxembourg House of Cybersecurity

Luxembourg House of Cybersecurity

THE GATEWAY TO CYBER RESILIENCE



Luxembourg, a pioneer in the open cybersecurity data economy

lhc.lu

310+ ACTIVE ACTORS IN CYBERSECURITY

90+ WITH CYBERSECURITY AS A CORE BUSINESS

70+ STARTUPS

CYBERSECURITY LUXEMBOURG

More about the ecosystem

CYBERSECURITY LUXEMBOURG

The Ecosystem

Ecosystem Overview

314

Companies ar
the ecosystem

Access the full list →

Created during
years

32

366

Entities are part of the ecosystem

Public Entities

40

Private Companies

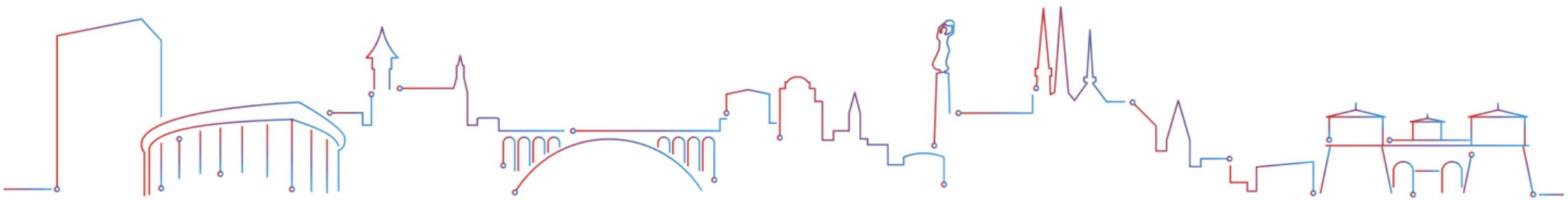
314

Clubs, Associations & Initiatives

12

tem

250



CYBERSECURITY TIPS & BEST PRACTICES

Stay safe online with these Cybersecurity best practices

CYBERSECURITY LUXEMBOURG

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 →

Wireless network

Password

Common incidents

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.

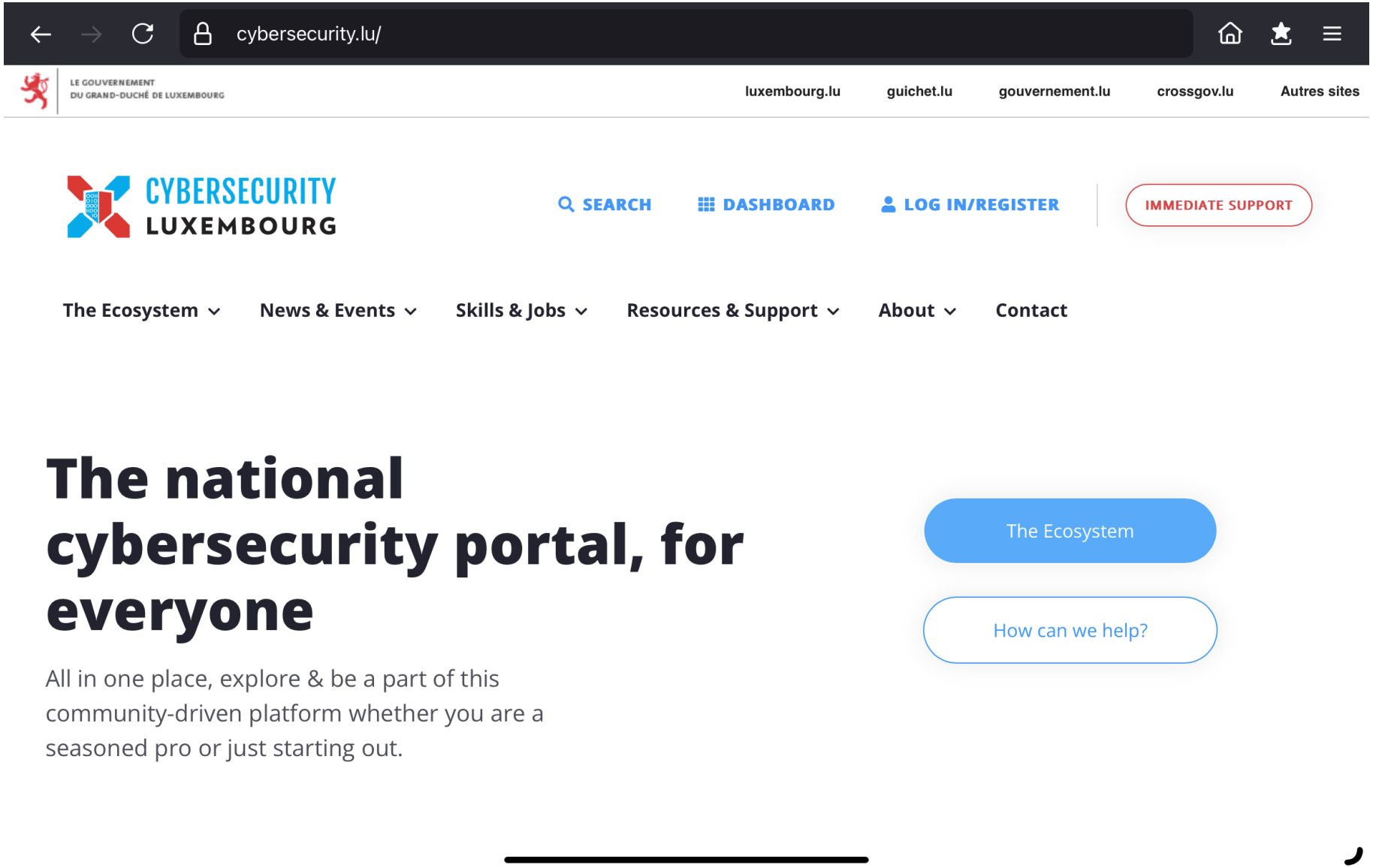
Read more →

Infected computer

Suspicious e-mail

National cybersecurity portal

CYBERSECURITY LUXEMBOURG



The national cybersecurity brand and ecosystem

Host for all types of cybersecurity-related activities

part of

Incident Response &
Cyber Threat Intelligence

Competence & Capacity Building
Research & Innovation
Market Intelligence

WE SUPPORT
WE FOSTER
WE SERVE

and more

Startups

Privacy

NIS

Research

Defence

Health

Municipalities

Education

Industry

Citizens

WE HOST

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.

Where to start ?

Welcome to the NC3 self-assessment tool: Fit4Cybe

This survey will ask a few questions and provide recommendat
the surface of information security by giving a very basic maturi

Summary:

This is the list of recommendations to improve the information security maturity in your company, provided that your answers did correctly reflect the state in your company. Also keep in mind that it is a self-assessment and only scratches the surface of the information security maturity level and thus, we are not liable for the results of this survey.

49 /10

Request training offer

Report:

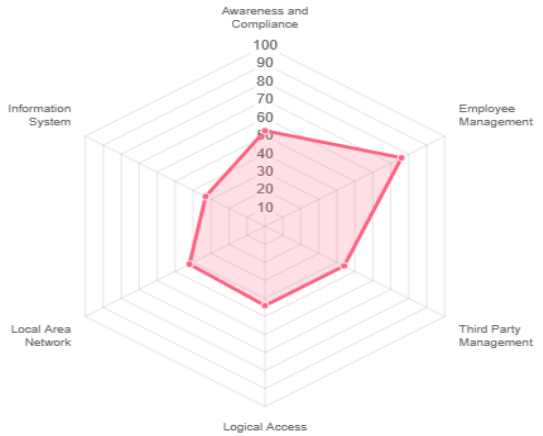
Download

IDENTIFY

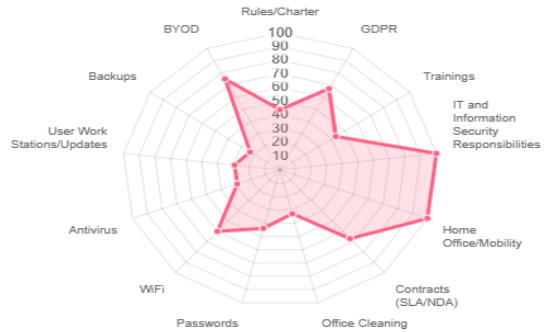
Based on your score 49/100, the NC3 Diagnostic is not available for your organization at this moment. We recommend you improve the information security maturity level by implementing the recommendations listed below. If you need any information security training to raise awareness in your company, do not hesitate to let us know.

Your results link

Score by section



Score by category



Antivirus

1. An antivirus software must be installed on all devices.
2. It should be up to date, preferably automatically to cover as many threats as possible.
3. All devices, like smartphones, tablets should have an antivirus, even if it is the one by default from the operating system.
4. Some tests should be done in case of suspicion of infection.

BYOD

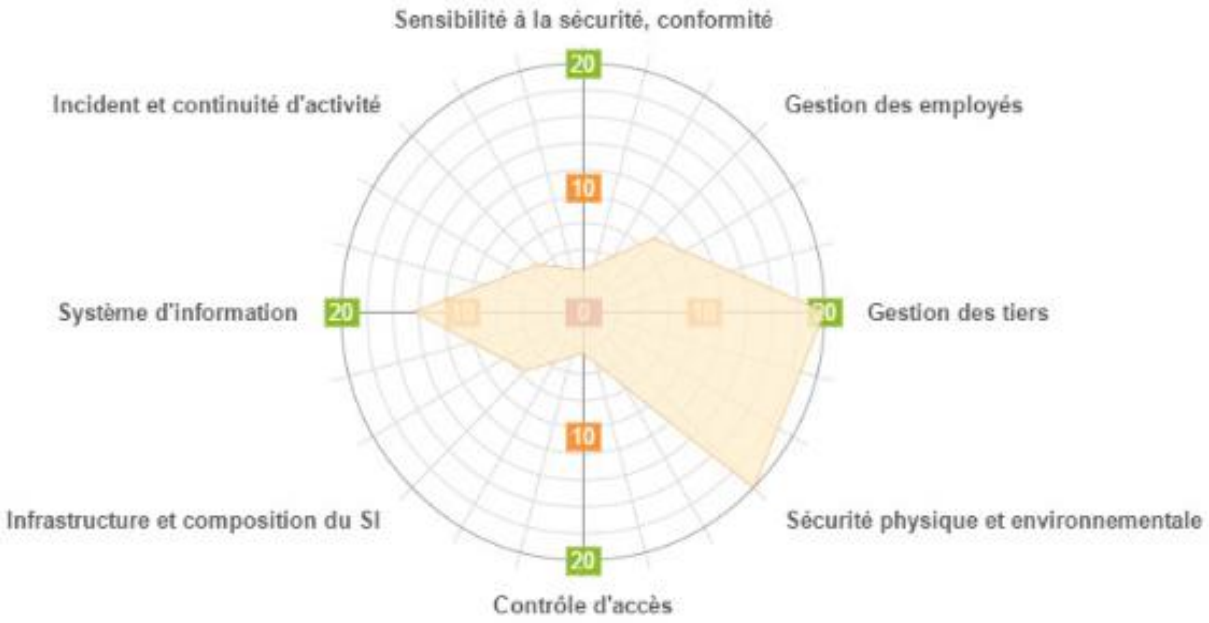
1. Defining rules and best practices help to protect the internal networks.

Backups

1. Backups should concern the whole company, and everyone should be aware to put all data on the systems that are backed up, to ensure to have a copy of them.
2. Backups should be retained at least a month to avoid problems caused by ransomware.
3. Backups should be disconnected, outside the local network, to be invisible by crypto-ransomwares.
4. Backups should be tested (restored) from time to time, just to ensure that the data is readable and has integrity.
5. Backups should be encrypted to avoid problems concerning the data theft, mainly if they are moved.

Diagnostic

IDENTIFY



Nr	Recommandation	Domaine	Gravité	Matu... actuelle	
2	• Effectuer de manière périodique des tests de restauration des back-up.	Système d'information	●●●	½	
3	• Mettre en place une charte utilisateur incluant les règles minimales de gestion concernant l'usage du système d'information et le comportement des utilisateurs. • Prévoir de distribuer la charte à chaque prise de fonction d'un nouveau membre du personnel.	Sensibilité à la sécurité, conformité	●●	☒	☑
4	• Prévoir une formation de 2 à 3 heures sur les bonnes pratiques de sécurité de l'information pour les utilisateurs du système d'information.	Gestion des employés	●●	☒	☑
5	• Améliorer l'authentification des utilisateurs par un système approprié (Filtre MAC, filtre IP, clé cryptographique, authentification forte, etc.) • Tous les accès à distance VPN doivent être gérés par le Firewall et uniquement ouverts pendant un temps limité. • Désactiver l'accès à distance si celui n'est pas utilisé	Gestion des employés	●●	⊘	☑
6	• Changer le mot de passe du Wifi de la commune. • Imposer un mot de passe complexe pour l'accès au Wifi de la commune	Infrastructure et composition du SI	●●	☒	☑
7	• Lister tous les prestataires IT et contrôler par quel moyen ils accèdent aux matériels (télémaintenance ou non). • Maîtriser tous les accès distants en validant tout accès en provenance de l'extérieur.	Infrastructure et composition du SI	●●	½	☑

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

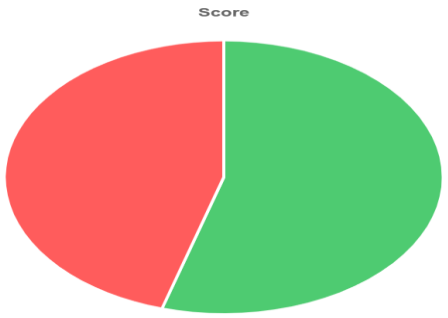
Testing Platform

DETECT

nc3.lu National Cybersecurity Competence Center LUXEMBOURG Testing Platform

Home Knowledge base About Login

NC3 Testing Platform



- ✗ Content Security Policy (CSP) header not implemented
- ✓ No cookies detected
- ✓ Content is not visible via cross-origin resource sharing (CORS) files or headers
- ✓ Initial redirection is to HTTPS on same host, final destination is HTTPS
- ✓ Referrer-Policy header not implemented (optional)
- ✗ HTTP Strict Transport Security (HSTS) header not implemented
- ✓ Subresource Integrity (SRI) is implemented and all scripts are loaded from a similar origin
- ✗ X-Content-Type-Options header not implemented
- ✗ X-Frame-Options (XFO) header not implemented
- ✗ X-XSS-Protection header not implemented

Test Discovery

Good 6

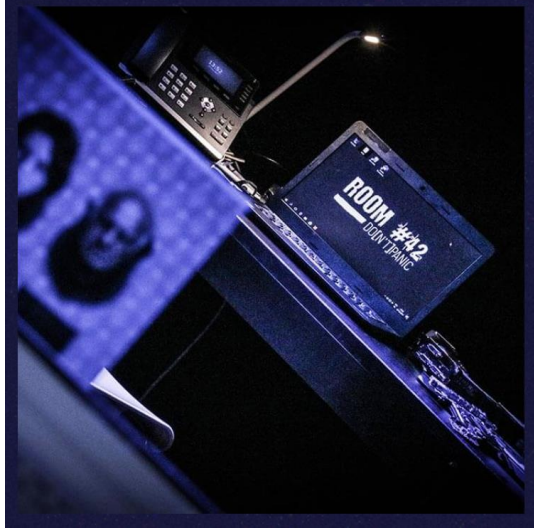
Vulnerable 5

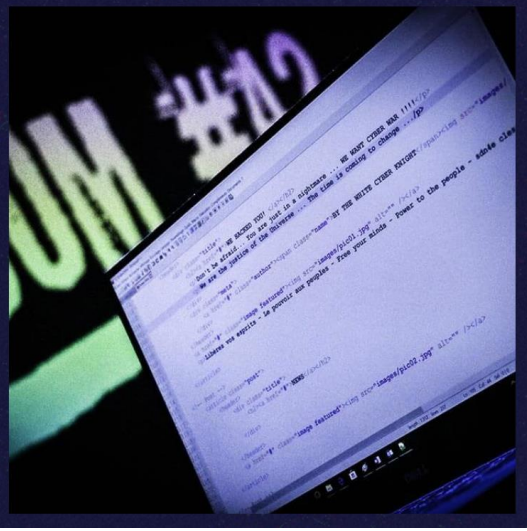
nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

Crisis preparedness

RESPOND

The cyberattack simulation made in Luxembourg.





ROOM #42
DØ[N'T]PANIC

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

pandora

MISP
Threat Sharing

ail project

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.

DETECT

Threat Intelligence

- Early Warning

- Malware Detection

- Threat Sharing

circl.lu
Computer Incident
Response Center
LUXEMBOURG

Incident Response

RESPOND

Don’t suffer in silence

CIRCL is there to help

- (+352) 247 88444
- info@circl.lu
- https://www.circl.lu/contactform/

Financial Support to Third Parties – FSTP *by NCC-LU*

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

FSTP is an EU Mecansim which aims to **distribute funding** in order to **stimulate** the creation of new companies and **increase their scalability**, create new SMEs or mid-cap companies and all that under the development of the digital innovation scheme

➢ *Purpose*
- **Simplify** administrative processes with especially SMEs
- **Assist** beneficiaries in topics such as the uptake or development of digital innovation
- The mission of the NCC-LU is to support **start-ups and SMEs** in the development of the cybersecurity industrial base and community in Europe

➢ *Opportunities*
- FSTP is a unique opportunity to **overcome financial obstacles** at national level by enabling high-risk initiatives so far lacking support from industry
- It has been designed in order to **simplify access** to EU funding, especially for SMEs that don't have the capacity and experience to directly participate in HEP or DEP Calls.

Calls will be published in a dedicated "funding" space on www.nc3.lu

❑ Target **audience**
- **SME'S** and **start-ups**

❑ **Projects** have to be aligned to one of the following 5 areas:
- Supporting the development of cybersecurity start-ups
- Promoting the creation or growth of local entities developing affordable testing tools and services
- Supporting the setup of cybersecurity services with a sustainable Open Source Business model
- Promoting the development of innovating approaches supporting the development of cybersecurity skills for SME's
- Supporting the development of easily accessible self assessment tools (that cover key obligations of existing and upcoming regulations)

❑ Maximum **amount** of funding per project: **60.000,- €**

Timeline

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

I. First FSTP Call

- ❑ Opening: 15.01.2024
- ❑ Closing: 15.03.2024
- ❑ Assessment period: 18.03.2024 – 17.05.2024
- ❑ Projects: 20.05.2024 – 15.11.2024

II. Second FSTP Call

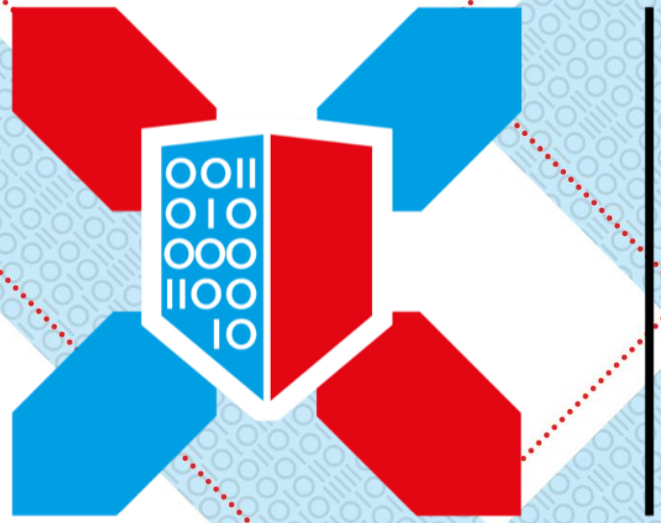
- ❑ Opening: 01.09.2024
- ❑ Closing: 31.10.2024
- ❑ Assessment period: 04.11.2024 – 27.12.2024
- ❑ Projects: 06.01.2025– 04.07.2025

III. Third FSTP Call

- ❑ Opening: 06.01.2025
- ❑ Closing: 28.02.2025
- ❑ Assessment period: 03.03.2025 – 25.04.2025
- ❑ Projects: 28.04.2025 – 31.10.2025

Thank you for your attention

Pascal Steichen



Luxembourg House of Cybersecurity