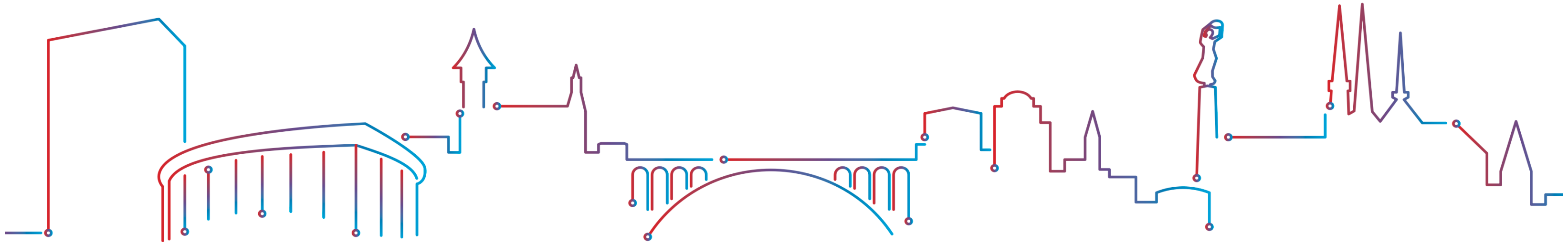
Cybersecurity

Where to start?

What's next?

LHC
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

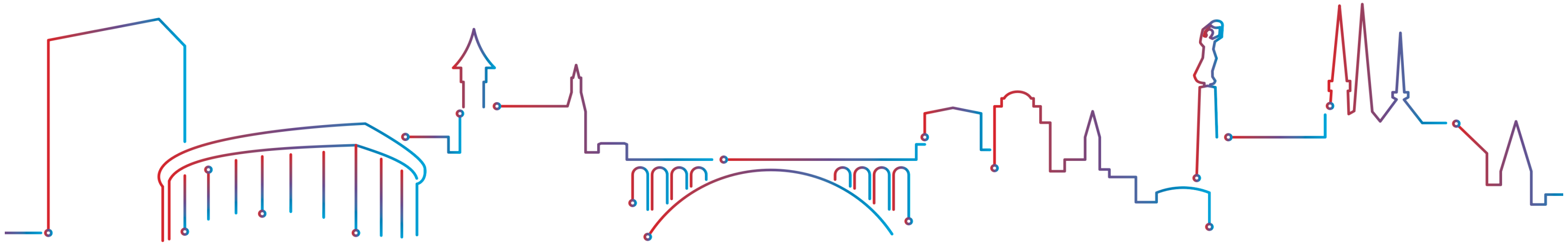
Luxembourg House of Cybersecurity

THE GATEWAY TO CYBER RESILIENCE

part of

circl.lu
Computer Incident
Response Center
LUXEMBOURG

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

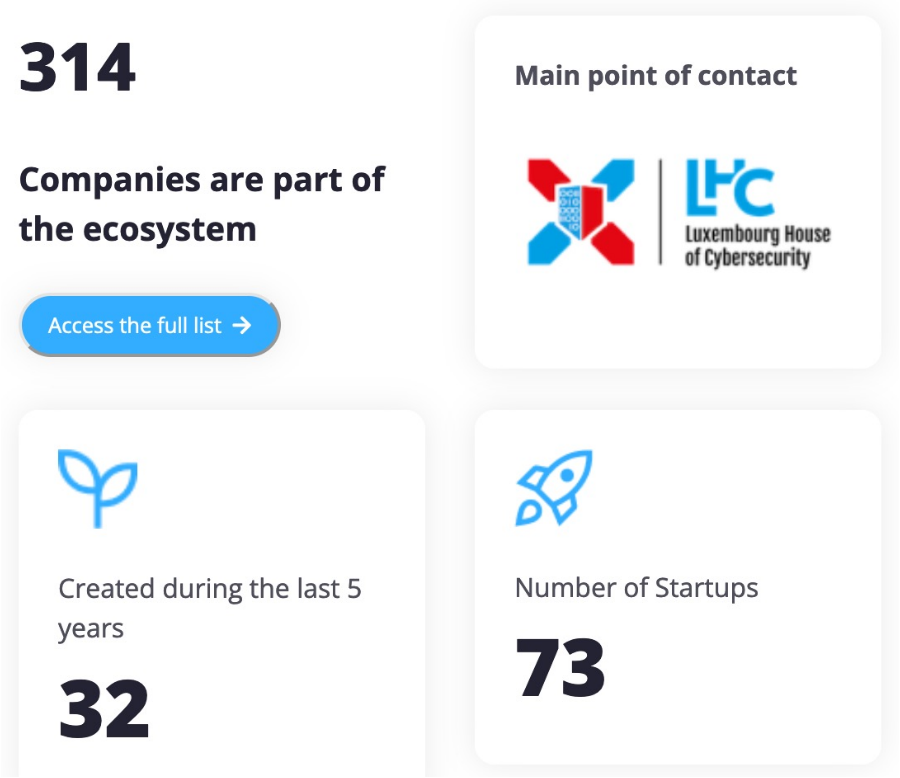


Luxembourg, a pioneer in the open cybersecurity data economy

lhc.lu

CYBERSECURITY LUXEMBOURG

The Ecosystem



314

Companies are part of the ecosystem

Access the full list →

Main point of contact

LHC Luxembourg House of Cybersecurity

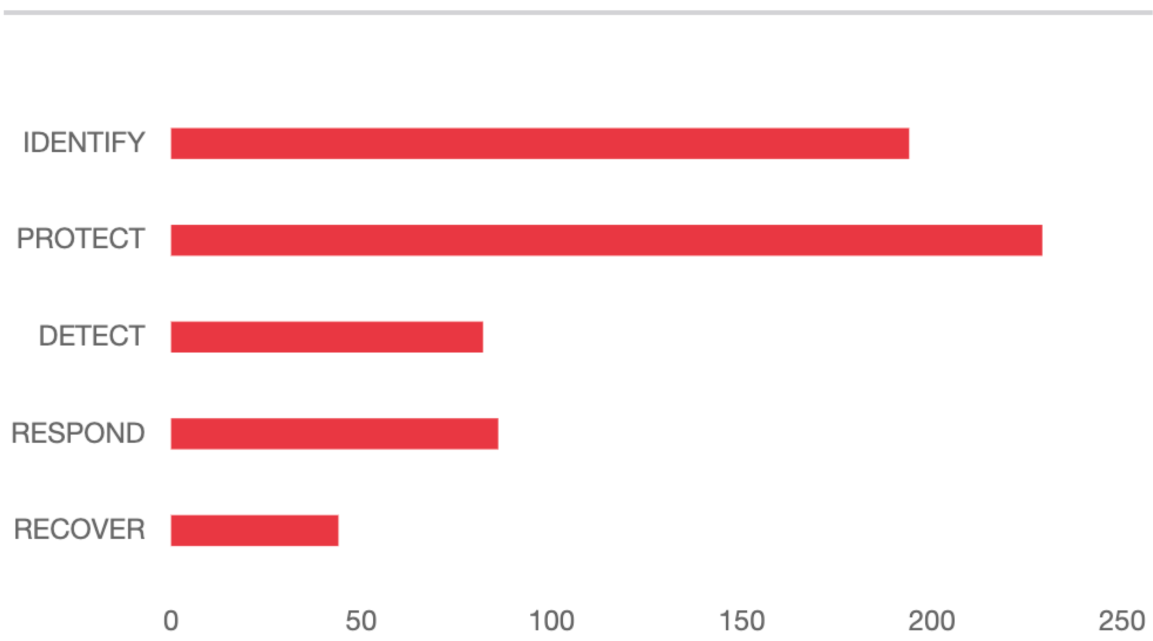
Created during the last 5 years

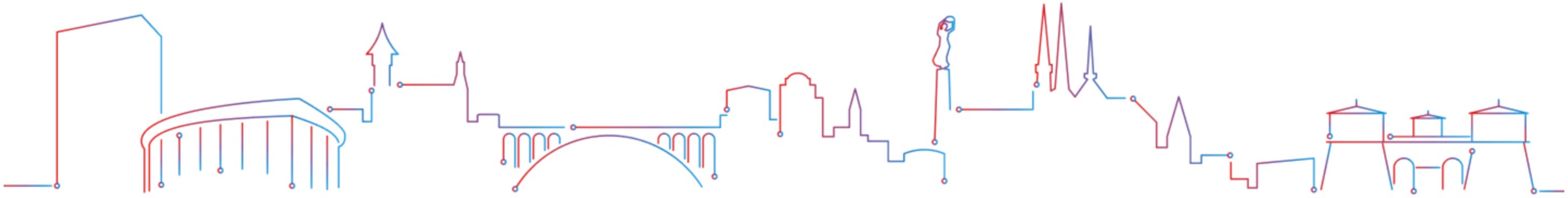
32

Number of Startups

73

Diversified solutions offered by the ecosystem





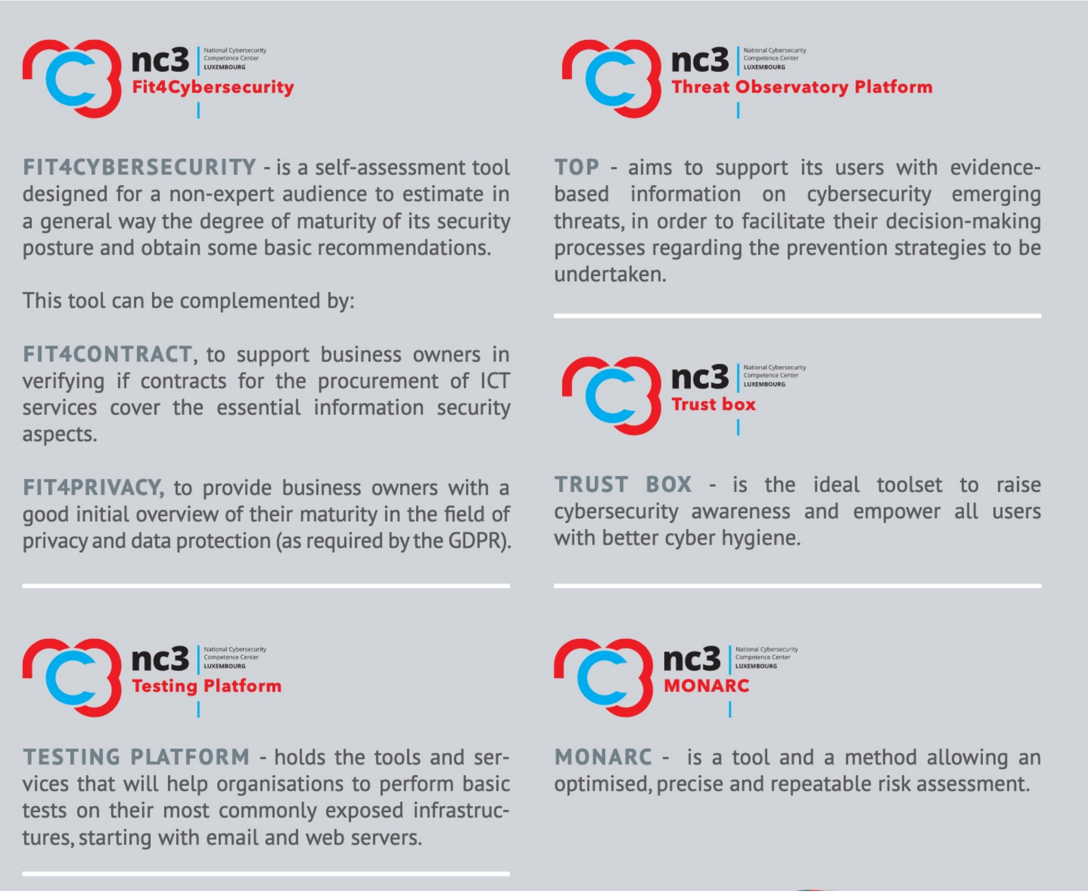
National Cybersecurity Competence Centre

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 **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 **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**

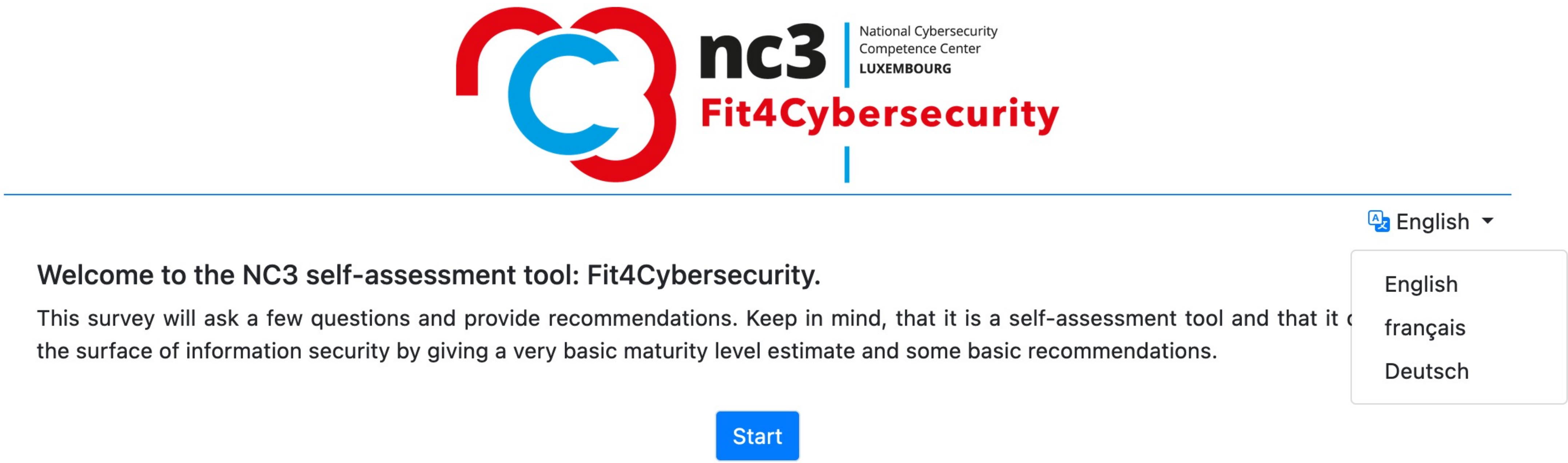
TRUST BOX - is the ideal toolset to raise cybersecurity awareness and empower all users with better cyber hygiene.

nc3 **MONARC**

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

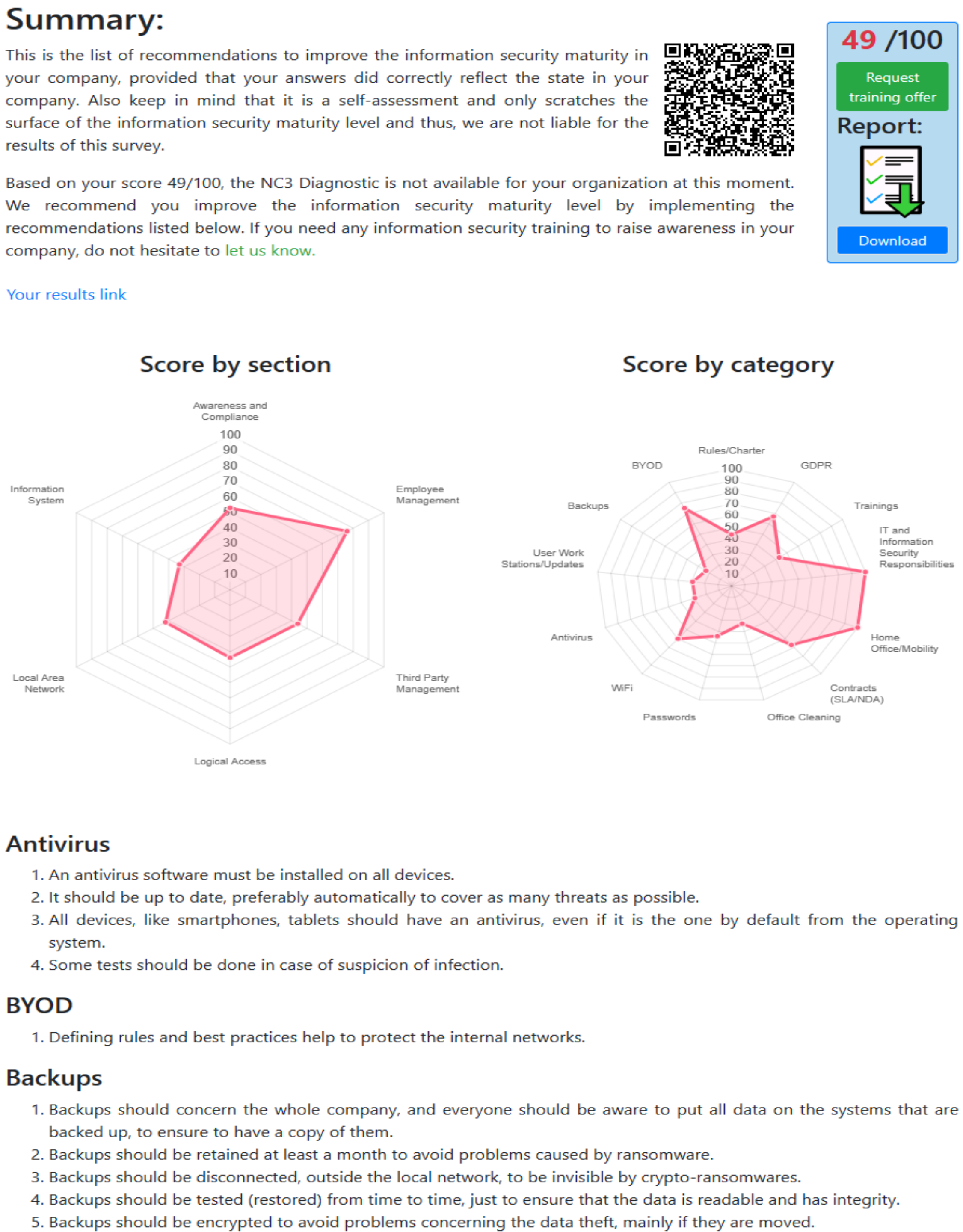
IDENTIFY

Where to start ?



Welcome to the NC3 self-assessment tool: Fit4Cybersecurity.

This survey will ask a few questions and provide recommendations. Keep in mind, that it is a self-assessment tool and that it c the surface of information security by giving a very basic maturity level estimate and some basic recommendations.



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 /100

Request training offer

Report:

Download

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

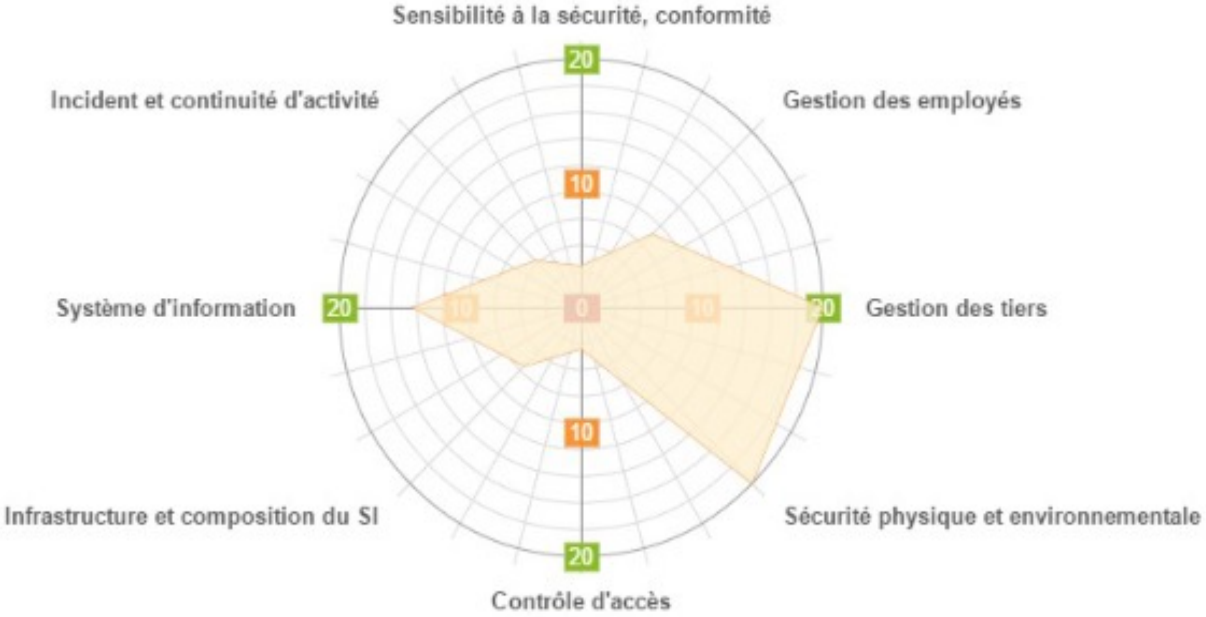
1. Defining rules and best practices help to protect the internal networks.

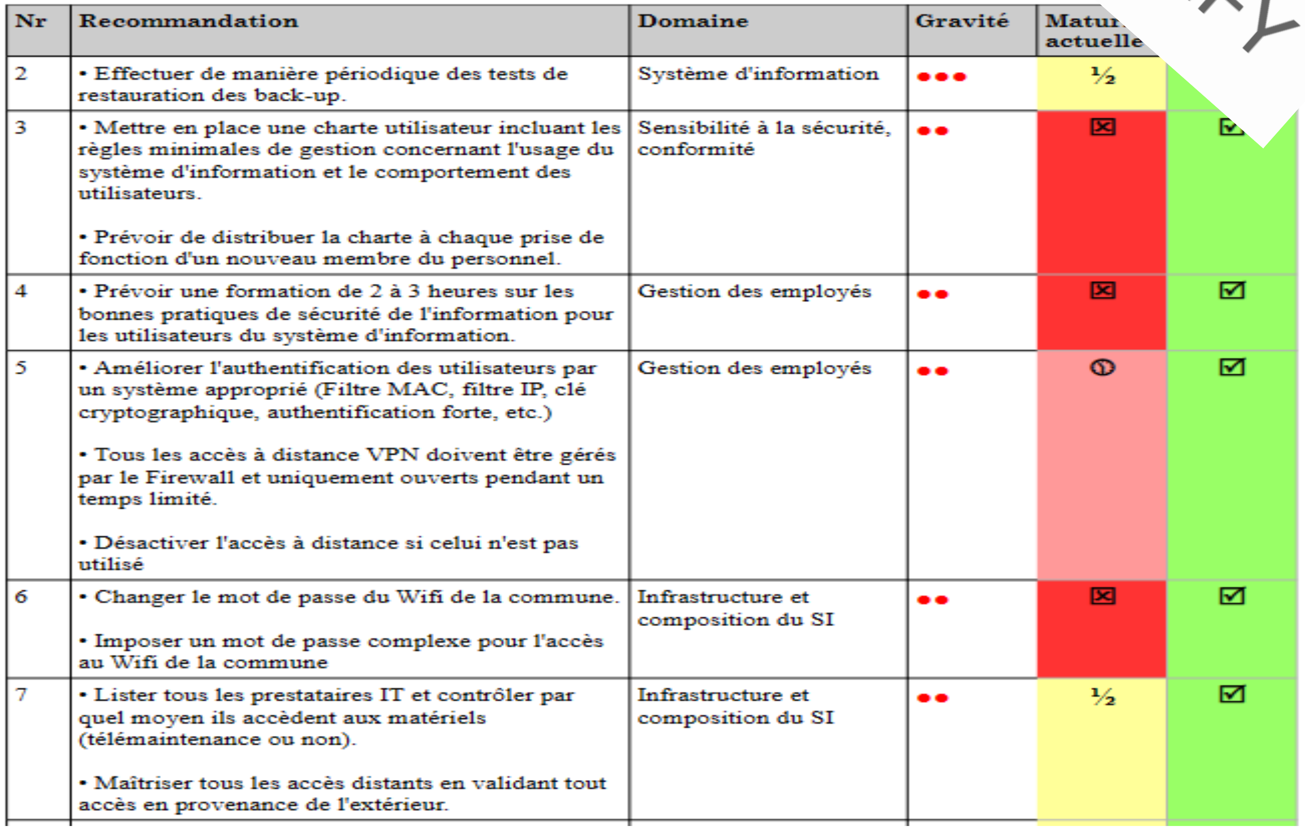
Backups

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	Matur 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	●●	①	☑
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

Fake news **et al.**

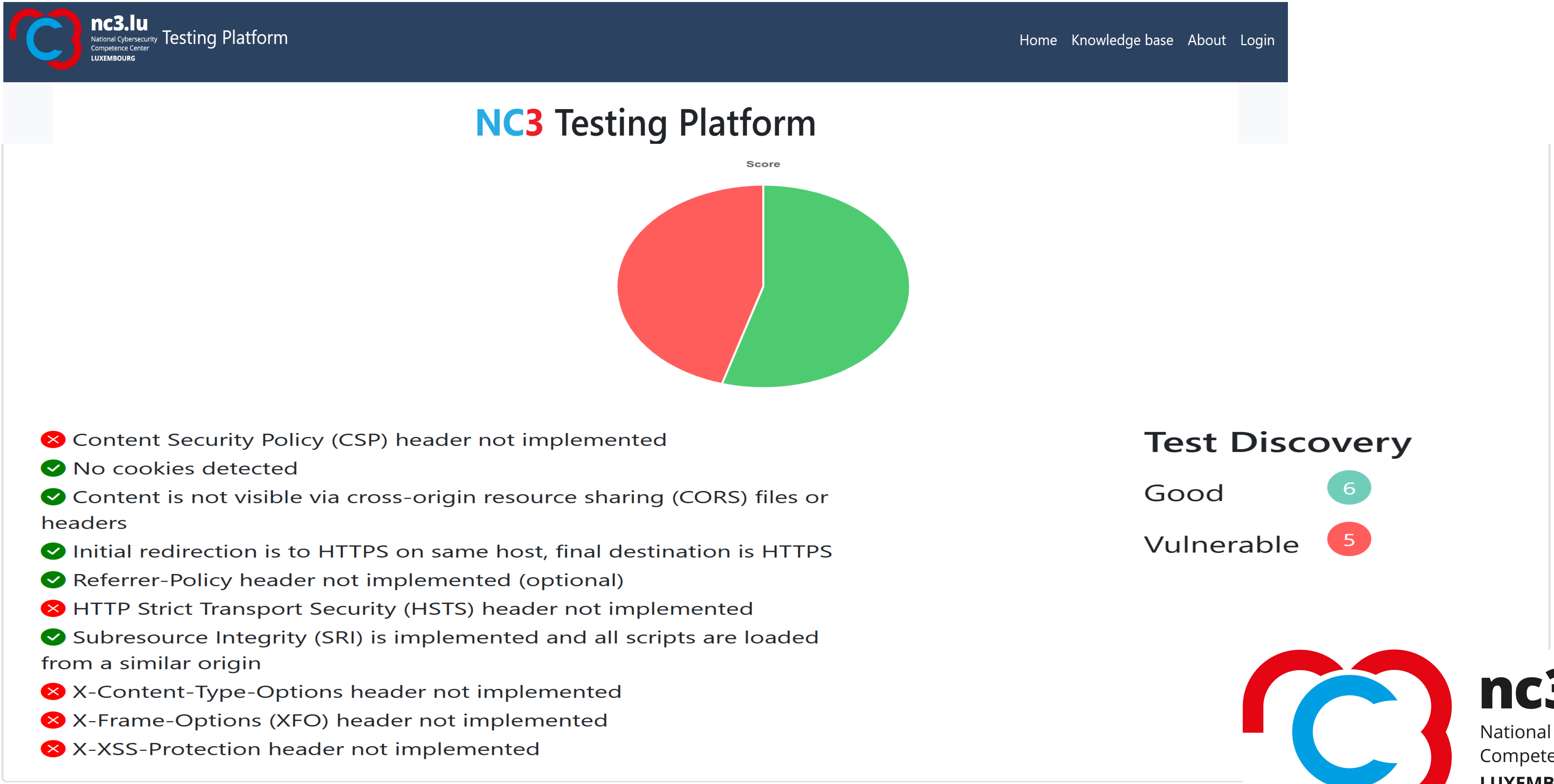
IDENTIFY

Thorn hub
CAKE NEWS
YOU ARE THE
♥ 0
#checkyourfacts
MEMES
LIVE YOUR PERFECT LIFE ON SOCIAL MEDIA!
Gleef net alles um Internet!
féissbook

BEE SECURE

DETECT

Testing Platform



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

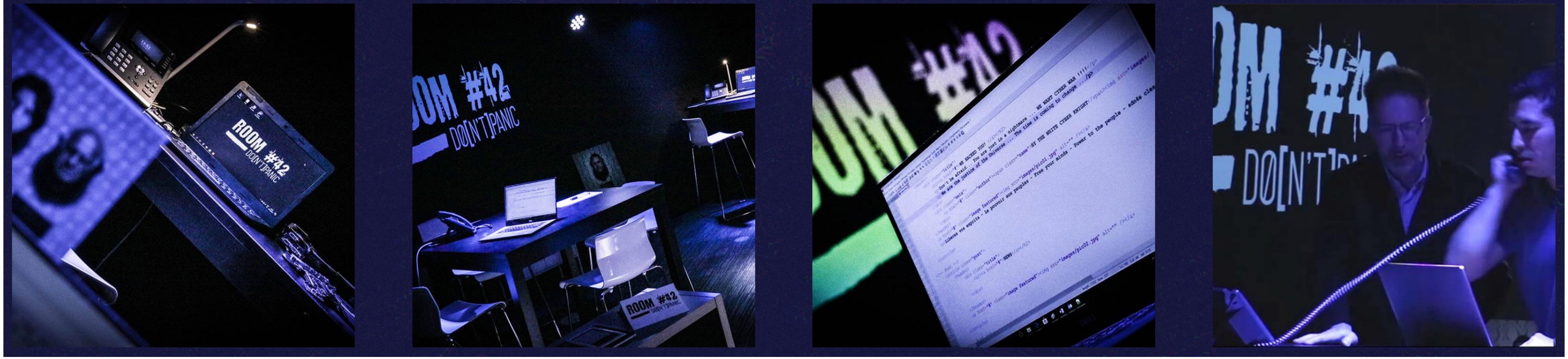
Good	6
Vulnerable	5

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

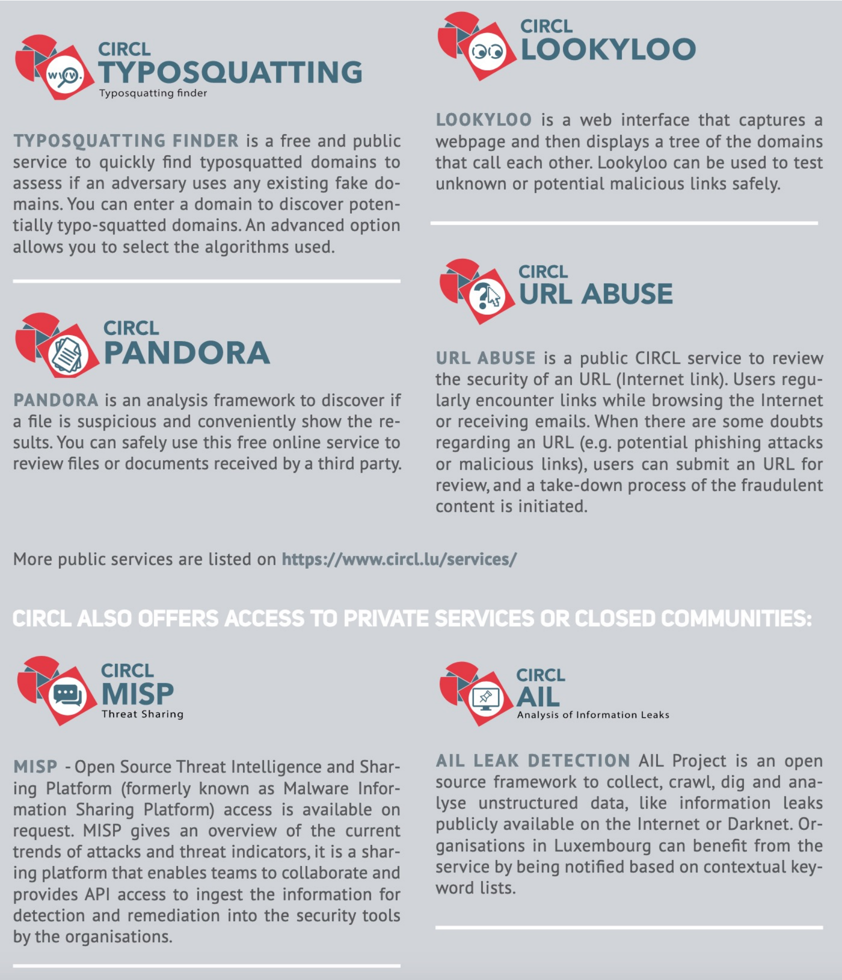
circl.lu
Computer Incident
Response Center
LUXEMBOURG

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

pandora
analysis framework

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
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.

DETECT

Threat Intelligence

- Early Warning

ail project

- Malware Detection

pandora

- Threat Sharing

MISP
Threat Sharing

Incident Response

RESPOND

Don’t suffer in silence

CIRCL is there to help!

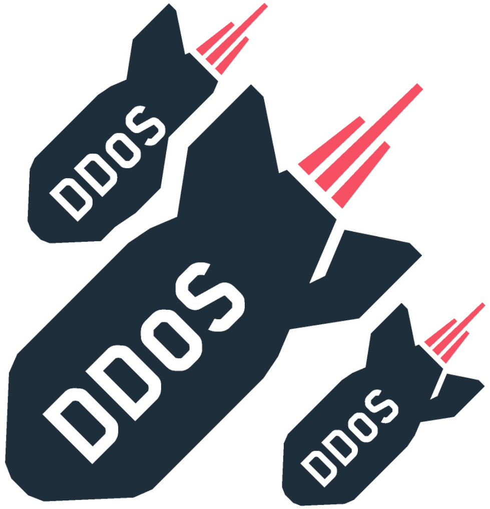
- (+352) 247 88444
- info@circl.lu
- https://www.circl.lu/report/

RESPOND

Anti DDoS

National Scrubbing Center

A crisis instrument!



National
Scrubbing
Center

DDoS

Le gouvernement luxembourgeois | Haut-Commissariat à la protection nationale

What’s next?

Conferences & Community

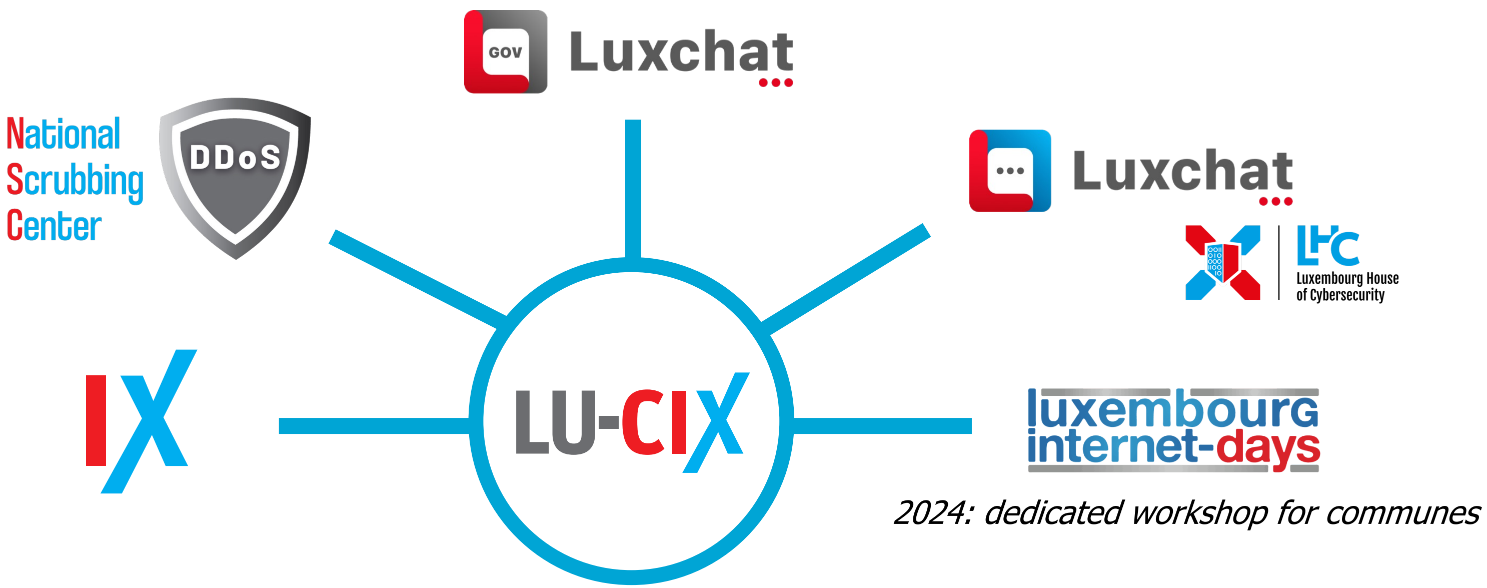
nexus2050

CSWL 2024

hack.lu

CYBERSECURITY LUXEMBOURG

https://cybersecurity.lu



GOV Luxchat
National Scrubbing Center
DDoS
Luxchat
LHC Luxembourg House of Cybersecurity
IX
LU-CIX
luxembourg internet-days

2024: dedicated workshop for communes

Thank you for your attention

Pascal Steichen

LHC

Luxembourg House of Cybersecurity