Services for Essential NIS2 entities

K. Dobbelaere

5th NISDUC conference

May 19, 2026

Brussels

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

TLP:GREEN

The national cybersecurity authority

CENTRE FOR CYBERSECURITY BELGIUM

A government body operating under the authority of the Prime Minister:

- Created in **2014** by Royal Decree
- Over 130 staff members

- Coordinates the implementation of the **National Cybersecurity Strategy**
- Composed of Cyber Emergency Response Team (**CERT**), Cyber Threat Research & Intelligence Sharing (**CyTRIS**), National Cybersecurity Certification Authority (**NCCA**), National Cybersecurity Coordination Centre Belgium (**NCC-BE**)

Our legal mission

High-level mission: Make Belgium one of the least vulnerable countries in the cyber domain

A coordination role at strategic level…

- Drafting the National Cybersecurity Strategy in cooperation with other government departments
- Coordinating implementation of the Strategy at national level
- Supporting national crisis management for cyber aspects
- Monitoring and updating the legal framework on cybersecurity
- Representing Belgium in international cybersecurity forums

... and at operational level

- Issuing alerts and advisories on the latest cyber threats
- Monitoring notifications and reports of cyber incidents at national and international level
- Supporting organisations in responding to cyber incidents
- Developing standards and practical guides on cyber security, etc.


CENTRE FOR
CYBERSECURITY
BELGIUM
2025
INCIDENTS
8 National incidents
+167% (3)
103 Emergency response interventions
+41% (73)
105 Ransomware
-4% (109)
144 Accounts compromise
+100% (72)
63 DDoS
-2% (64)
AWARENESS
78 News on Safeonweb
1 891 220 Visits on Safeonweb
PHISHING
9 929 354 E-mails send to suspicious@safeonweb.be
+9% (9 083 629)
176 183 Unique URLs tagged as malicious
-88% (1 456 724)
40 815 Unique domains tagged as malicious
-91,3% (466 177)
WARNINGS
264 Technical advisories published online
-4% (276)
32 005 Spear warnings: automated and manually
+43% (22 417)
568 CTI reports EWS portal
+3% (549)
152 Spear warnings campaigns
-21% (193)
219 Disclosed vulnerabilities
+92% (114)
185 011 157 Amount of hits on the BAPS warning page
-23% (240 633 935)
EVENTS
15 Connect and share events
(8)
*The percentages are compared to 2024.
.be

Our constituents

CENTRE FOR CYBERSECURITY BELGIUM

The population as a whole:
Educate & involve individuals in their own security

@Home

@Work

Organisations:
Large companies, SMEs, associations…

Organisations of vital interest:
NIS2 entities,
Critical infrastructures, etc.

@OVI

@Gov

Public authorities:
Federal, but also regional and local

CCB services for organisations

CENTRE FOR CYBERSECURITY BELGIUM

Cyber security expertise

Cyberresilience building

Proactive CCB services

Reactive CCB services

Open access

Registration required

Restricted to essential NIS2 entities & gov services

Cyber security expertise

CENTRE FOR CYBERSECURITY BELGIUM

- Tools & Resources
- Webinars & talks
- CyFun® framework
- Investment strategy & funding coordination

Open access

Registration required

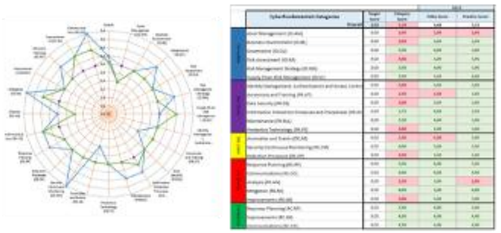
Restricted to essential NIS2 entities & gov services

The CyberFundamentals ecosystem

CyFun®
Framework mapping

CyFun®
Selection tool
(Risk Assessment)
(National Tool)

CyFun®
Self-Assessment tool



CyFun® BASIC
Policy templates

CyFun®
Conformity
Assessment
Scheme
for CAB's
Under accreditation

CyberFundamentals Labels

CyberFundamentals Toolbox is **publicly available** ➔ **www.cyfun.eu**

More info: https://www.cyfun.eu

TLP:GREEN

Investment strategy & funding coordination

EU funding navigation
Find relevant European cybersecurity calls, understand where you fit, and connect with partners.

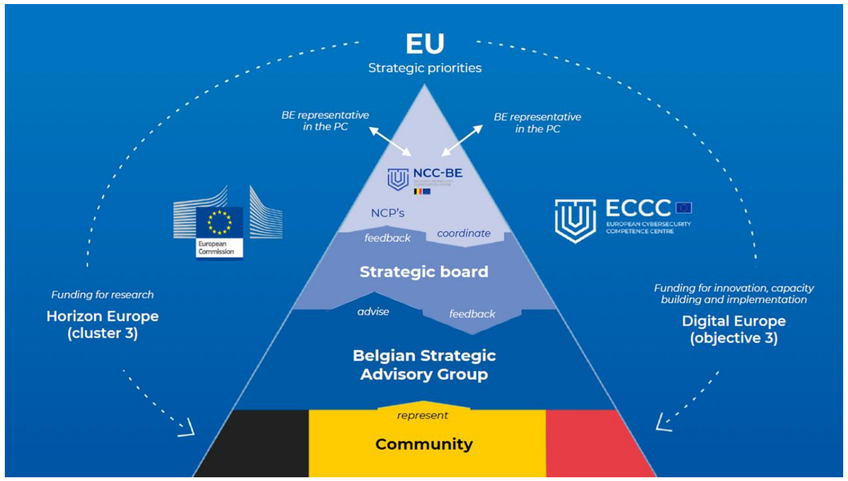
Partnerships & networking
Access Belgian and European cybersecurity networks, matchmaking and collaboration opportunities.

Your voice in Europe
Belgian CS ecosystem represented in ECCC governance and strategic discussions.

Innovation & compliance guidance
Guidance with EU processes, innovation pathways and initiatives like SECURE (compliance & readiness).

CCB was designated as National Coordination Centre for Belgium (NCC-BE) in the framework of **EU Regulation 2021/887.**

The NCC-BE drives **innovation** and strengthens Belgium's **competitiveness** by coordinating **research, technology and industrial** development efforts in cybersecurity.



More info: https://ccb.belgium.be/ncc

TLP:GREEN

Proactive services

CENTRE FOR CYBERSECURITY BELGIUM

Malware Information Sharing Platform (MISP)

Registration platform

External attack surface protection

Open access

Registration required

Restricted to essential NIS2 entities & gov services

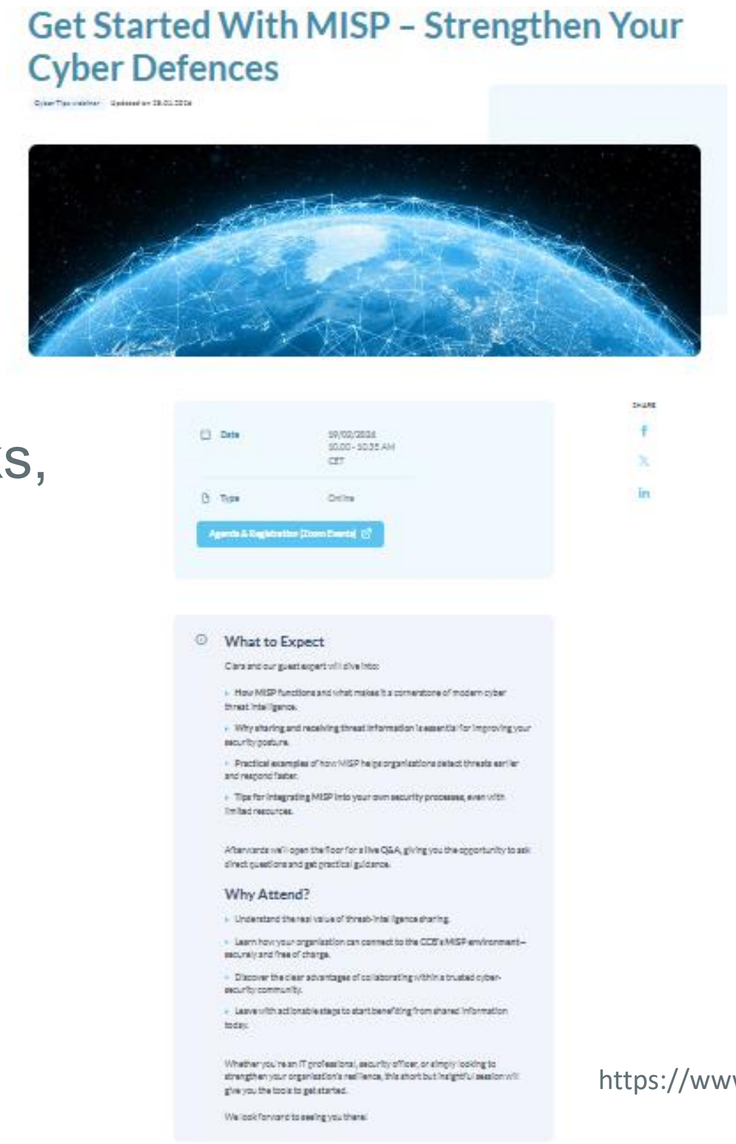
Malware Information Sharing Platform (MISP)

CENTRE FOR CYBERSECURITY BELGIUM

Threat intelligence platform
for sharing, storing and correlating

- indicators of Compromise of targeted attacks,
- threat intelligence,
- financial fraud information,
- vulnerability information
- or even counter-terrorism information.

open source project driven by CIRCL.LU



YouTube BE

https://www.youtube.com/@cybersecuritybelgium

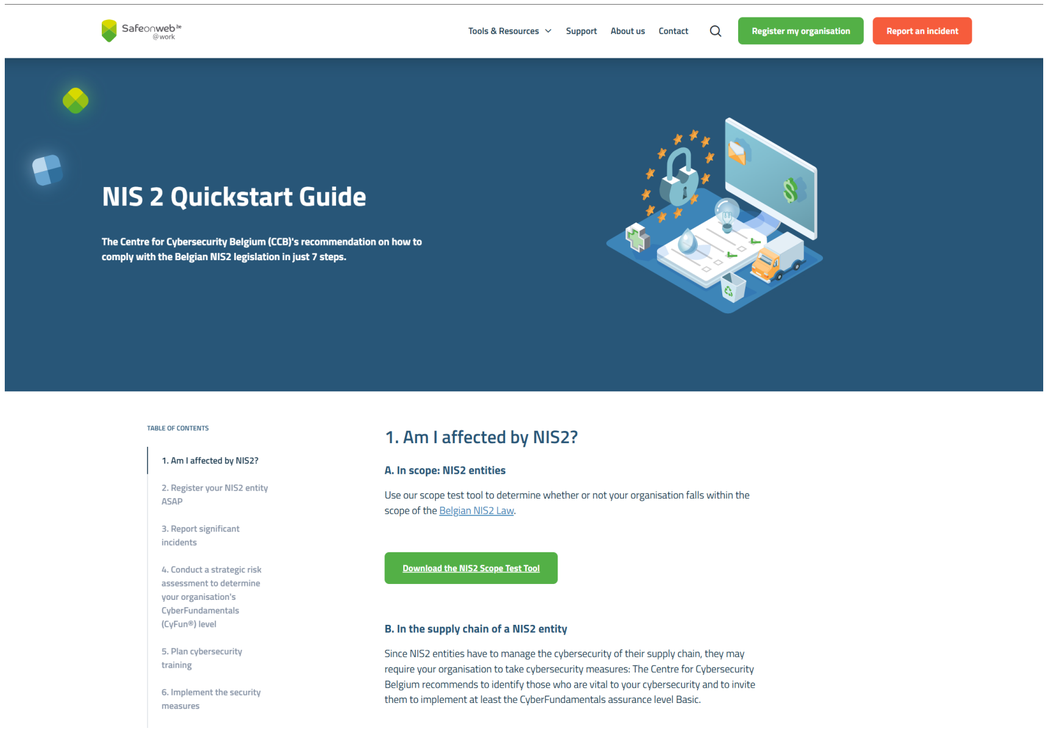
More info: info@ccb.belgium.be

TLP:GREEN

Registration platform

@work and/or NIS2

- Optional safeonweb@work registration (CTI & CyFun)
- Mandatory registration as NIS2 entity with the CCB
  - Indication of activity, entity size, network information and contact information
- Criterium: KBO/BCE number

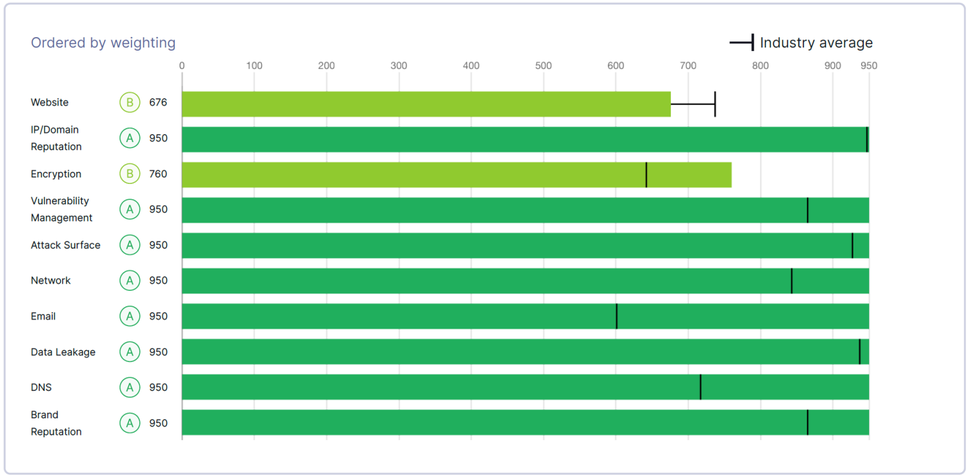


More info: info@ccb.belgium.be

TLP:GREEN

Quick Scan Report

Security rating by category



TLP:GREEN

External attack surface protection

CENTRE FOR CYBERSECURITY BELGIUM

Early Warning System

- CCB's automated Spear Warning service based on Arctic Hub technology, with premium intelligence feeds
- EWS: CCB database with up-to-date contact information
- Spear warnings are individualized targeted warnings to alert for observed vulnerabilities or infections on your network
- Weekly check for vulnerabilities, daily for infections

Early Warning System (Reports & Alerts)

- Threat landscape reports
- Flash alerts (for which imminent action required)
- ? Media articles

More info & onboarding requests:
info@ccb.belgium.be

Access Journey Program

- Free access (2x45d/Year) to an external attack surface mgt tool
- Tailored & individualized training on remediation

More info & onboarding requests:
intelligence@ccb.belgium.be

Reactive services

CENTRE FOR CYBERSECURITY BELGIUM

- (NIS2) Incident Notification & Assessment
- Digital forensics & Incident Response (DFIR)
- (Emergency) Security Monitoring
- Cyber crisis management (coordination)

Open access

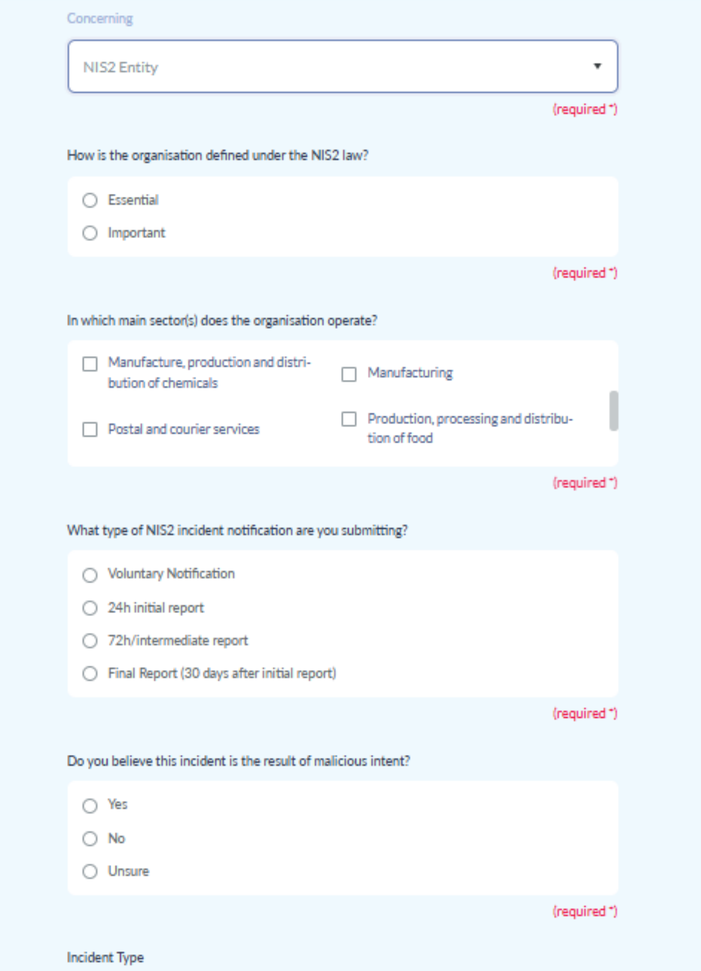
Registration required

Restricted to essential NIS2 entities & gov services

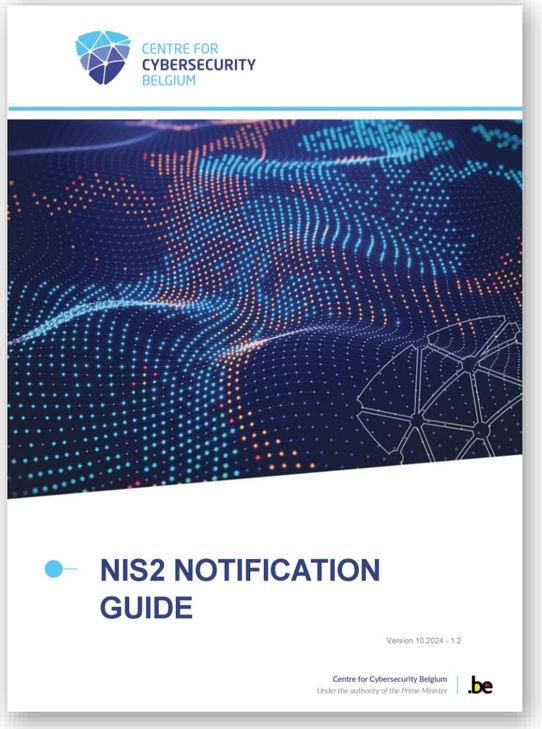
TLP:GREEN

(NIS2) Incident Notification & Assessment

CENTRE FOR CYBERSECURITY BELGIUM



Pragmatic reporting tool, that is integrated in CCB's current incident handling process



→ Incident notification guide: https://atwork.safeonweb.be/tools-resources/nis-2-quickstart-guide

→ Incident notification platform: https://notif.safeonweb.be/

More info: nis@ccb.belgium.be

TLP:GREEN

Digital forensics & Incident Response (DFIR)

CENTRE FOR CYBERSECURITY BELGIUM

- *Assistance* (=advise) with coordination and/or analysis of a cyber security incident (on request)
- Performed together with internal IT/security team
- Collection and analysis of forensic evidence
- Goal for CERT: helping to contain the incident and if possible to answer following questions:
  - How did the attacker get in ?
  - What exactly did the attacker do ?
  - Is there still a risk ?

More info: info@ccb.belgium.be

TLP: GREEN

(Emergency) Security Monitoring

CENTRE FOR CYBERSECURITY BELGIUM

- Incident based
- Deployment of our agents or working with your tools
- Assist with follow up of the situation during or shortly after a cyber security incident
- Escalation of findings and quick start of incident response if required
- Limited duration

More info: info@ccb.belgium.be

TLP: GREEN

Generic cyber resilience building in BE

CENTRE FOR CYBERSECURITY BELGIUM

- Belgian Anti-Phishing Shield (BAPS)
  - verdacht@safeonweb.be
  - suspect@safeonaweb.be
- Letter spear warning
- Coordinated Vulnerability Disclosure process
- Cyber security exercises & challenges

Open access

Registration required

Restricted to essential NIS2 entities & gov services

Cybersecurity exercises & challenges

CENTRE FOR CYBERSECURITY BELGIUM

EU level

- Cyber **exercises** within **targeted sectors**
- Organisation: ENISA
- CCB coordinates BE participation
- **Next CyberEurope edition (june 2026) will focus on railway & maritime**

CYBER EUROPE

Blue OLEx

National exercises

- Technical tabletops to test, prepare & train for incidents (& associated incident response playbooks)

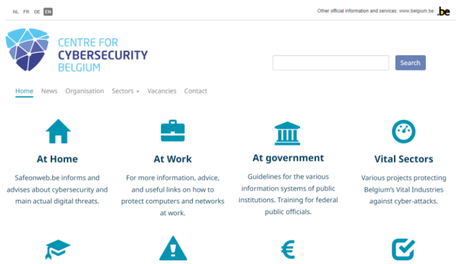
CS challenges & skills

- Support Red Daemons at European Cyber Security Challenge
- Overview of CS training offering within Belgian education system

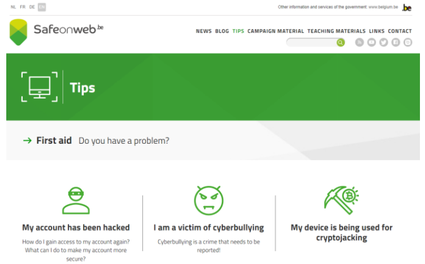
CENTRE FOR CYBERSECURITY BELGIUM

THE CENTRE FOR CYBERSECURITY BELGIUM

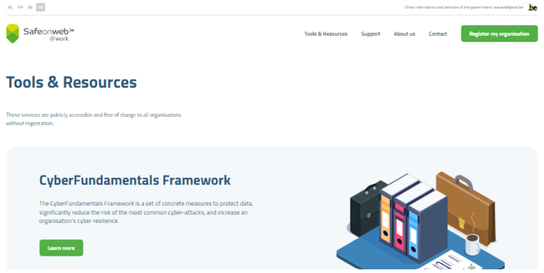
Learn more about us



https://ccb.belgium.be/en



https://safeonweb.be/en



https://atwork.safeonweb.be/

Follow us

Centre for Cybersecurity Belgium

- LinkedIn - CCB
- X - CCB
- X – CCB alert
- YouTube - CCB

Safeonweb

- Facebook - Safeonweb.be
- Instagram - Safeonweb.be
- X – Safeonweb
- YouTube - @safeonwebbe

CENTRE FOR CYBERSECURITY BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

TLP:GREEN