Information Sharing Arrangements in the Cyber Security Coalition

Organisational unit: Cyber Security Coalition
Line of activity: Operational Collaboration through Focus Groups
Contact: Christian Mathijs, Business Development Manager
info@cybersecuritycoalition.be

Version 1.0

1. Introduction

This document specifies the information sharing arrangements of the Focus Groups of the Cyber Security Coalition with respect to article 29 NIS2 and article 45.2 of DORA.

Article 29 NIS2 Directive
Cybersecurity information sharing arrangements

1. Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

2. Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

3. Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).
4. Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.
5. ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.

Article 45.2 DORA Directive
Information sharing arrangements on cyber threat information and intelligence
1. Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:
(a) aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;
(b) takes places within trusted communities of financial entities;
(c) is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with Regulation (EU) 2016/679 and guidelines on competition policy.
2. For the purpose of paragraph 1, point (c), the information-sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which they may be associated to the information-sharing arrangements, on the involvement of ICT third-party service providers, and on operational elements, including the use of dedicated IT platforms.
3. Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their

membership, or, as applicable, of the cessation of their membership, once it takes effect."

2. Cyber Security Coalition

The Cyber Security Coalition is the largest community of cybersecurity experts in Belgium. An overview of our members can be found on our website.

Our **Mission** is to bolster Belgium's cyber security resilience by **building a strong cyber security ecosystem** at national level. We do so by bringing together the skills and expertise of the **academic world**, the **private sector** and **public authorities** on a **trust-based platform** aimed at fostering information exchange and implementing joint actions.

The 12 Focus Groups constitute the core of our value proposition:

- Application Security
- Awareness
- Cloud Security
- Cryptography
- Cyber Incident Detection & Response (CIDR)
- Cybersecurity for Hospitals
- Enterprise Security Architecture (ESA)
- Governance, Risk & Compliance (GRC)
- Identity & Access Management (IAM)
- OT/ ICS Security
- Privacy & Data Protection
- Regulations & Standardizations

The description of these Focus Groups scope can be found on our website or in the brochure "CSC-Brochure Focus Groups Description 2024", available at request.