Council of the European Union
General Secretariat

Interinstitutional files:
2023/0109 (COD)

Brussels, 29 November 2023

WK 15896/2023 INIT

REDACTED DOCUMENT ACCESSIBLE TO THE PUBLIC (11.06.2025). ONLY MARGINAL PERSONAL DATA HAVE BEEN REDACTED.

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on cyber issues (attachés)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - Non-paper

Non-paper by EE, FR, LU, LV, PL, SE and SK on the endorsement of the non-paper regarding the Cyber Solidarity Act together with an annex - Non-paper regarding the Cyber Solidarity Act dated 28.10.2023, signed by 21 CSIRTs

Non – paper by EE, FR, LU, LV, PL, SE and SK

On the endorsement of the non - paper regarding the Cyber Solidarity Act

The undersigned Member States endorse the attached non paper regarding the Cyber Solidarity Act dated 26.11.2023 (version 10) , signed by 21 CSIRTs and hereby present its findings as their position in the negotiations of the Cyber Solidarity Act.

Annex

Non - paper regarding the Cyber Solidarity Act dated 26.11.2023 (version 10), signed by 21 CSIRTs

TLP:GREEN

Non-Paper regarding the Cyber Solidarity Act

Date: 2023-11-26
Version: 10

Initially, CSIRTs have operated as the IT security function of organisations and countries. With the increasing importance of the Internet and the ubiquity of connections over the last 20 years, new concepts and names have appeared. The terminology has not finally settled, thus creating the possibility for misunderstandings or ambiguities in policy proposals.

This document describes some of the thoughts of a subset of members of the CSIRTs Network regarding the proposed EU Cyber Solidarity Act (CSoA), in particular Chapter 2 (The European Cyber Shield). **It does not necessarily reflect opinions of the respective member states.**

As of 2023-11-26, the following teams endorse the present non-paper:

- Austrian Energy CERT
- CCB/CERT.be
- CERT.AT
- CERT-Bund
- CERT-EE
- CERT-EU
- CERT-FR
- CERT.hr
- CERT.LV
- CERT Polska
- CERT-SE
- CIRCL
- CSIRT-IE
- GovCERT Austria
- GovCERT.CZ
- GOVCERT.LU
- INCIBE-CERT
- NCSC-FI
- NCSC HU
- SI-CERT
- SK-CERT

Computer Security Incident Response Teams

While the literal meaning of the name "Computer Security Incident Response Team"[1] centers on Incident Response, the CSIRT Services Framework defined by FIRST.org (in collaboration with TF-CSIRT and the ITU) describes a much broader spectrum of services that CSIRTs provide. We will refer to this framework, as it is widely adopted worldwide and in the EU. Version 2.1 of the framework includes the following service areas:

- Information Security Event Management
- Information Security Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer

Not every team has the same focus. There are significant differences in the choice of services provided by different teams. The NIS 2 directive also assigns task other than Incident Response to the CSIRTs. Specifically, Article 11(3) lists these other tasks of CSIRTs:

> (a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, **providing assistance** to essential and important entities concerned **regarding real-time or near real-time monitoring of their network and information systems**;
>
> (b) providing **early warnings, alerts, announcements and dissemination of information** to […] relevant stakeholders on **cyber threats, vulnerabilities** and incidents, if possible in near real-time;
>
> (d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

Article 12 adds coordinated vulnerability disclosure as another task to a designated CSIRT.

In the context of discussion around CSoA, it is worth to point out that that the CSIRT services include using sensors and other data sources to detect and analyze security events in real time (services: "Monitoring and detection" and "Event analysis"). CSIRTs can – and in many cases do – monitor the IT infrastructure of the entities they are protecting, collecting detailed low-level data and use systems like SIEM (Security Information Event Management System) to facilitate detection. Of course whether a CSIRT provides such a service, depends on its mandate.

The CSoA proposal defines the concept of the "national SOC" which is supposed to coordinate the information flow between the security function of individual constituents as well as the managed security service providers who serve them. It should "act as a reference point and gateway at national level for participation in the European Cyber Shield and should ensure that **cyber threat information from public and private entities is shared and collected** at national level". This fits almost perfectly with the NIS2 mandate of CSIRTs "providing assistance […] regarding real-time or near real-time monitoring of network and information systems".

Therefore, it is clear to us that the intention of CSoA is to improve upon activities that are already in scope of the services provided by European CSIRTs.

[1] For clarity, we will avoid using the term "Computer Emergency Response Team" (CERT) in this paper, as for all practical purposes it is equivalent to CSIRT.

The NIS2 directive also includes in Article 29 requirements for national 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;

Thus, the concept of getting organizations to cooperate on incident detection, e.g., by sharing cyber threat intelligence (CTI), is already in the NIS framework. The directive doesn't assign the task of arranging this collaboration to a specific entity, but given the Article 11(3) tasks for CSIRTs, it is not a stretch to assume that CSIRTs will both do the top-down sharing of CTI, as well as the facilitating the horizontal sharing between entities and their SOCs.

Security Operations Centers

There is no universal definition of a Security Operations Center (SOC), we provide some of the noteworthy in the references section. This paper does not attempt to create a complete definition of a SOC or its services.

Nevertheless, in practice there is a common understanding among the cybersecurity professionals of some fundamental properties of a SOC:

- The primary goal of a SOC is to detect and – at least to some degree – react to incidents.
- To perform detection, a SOC needs access to detailed data from the protected infrastructure, for example, endpoint and network logs.

While focus on detection and processing of raw data are essential for a SOC, it is important to note, that the same services can be provided by CSIRTs. These tasks are included in the Information Security Event Management service area defined by FIRST, as explained in the previous section. The definition contains an explicit reference to SOCs:

"Information Security Event Management aims to identify information security incidents based on the correlation and analysis of security events from by a wide variety of event and contextual data sources. In larger organizations, this service area is sometimes fully or partially assigned to a Security Operations Center (SOC) (…)"

The lack of a universally adopted definition and the significant overlap with the functions of CSIRTs means that there is no consistency among entities in the public and private sectors in naming different units responsible for cybersecurity. An organization may have both CSIRT and a SOC, where responsibilities related to cybersecurity are divided between the two; only SOC performing all tasks related to detection and incident response; only CSIRT that may provide detection services; or use a different naming convention entirely.

Thus, one cannot rely on the name "SOC" or "CSIRT" to understand what is the actual function of the particular team. **To avoid ambiguity we should refer to concrete services or functions that these entities provide.**

Information Sharing and Analysis Centers

Information Sharing and Analysis Centers (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents, and threats, as well as sharing experience, knowledge, and analysis. Membership is often (but not always) sector-based, for example, the Energy ISAC. They can be national or cross-border.

The main purpose of ISACs is information sharing among its members, however, there are also many forums which have a similar role, even if they use a different name. Examples include national CSIRT/SOC networks, associations like FIRST or TF-CSIRT, and the EU's CSIRTs Network.

National CSIRTs

National CSIRTs[2] are a special class of CSIRTs, commonly referred to as "coordinating CSIRTs". CSIRT Services Framework describes the difference between enterprise and coordinating CSIRTs:

"Inside an organization, an Enterprise CSIRT is focused on the security of computer systems and networks that make up the infrastructure of an organization. If there are multiple security teams and CSIRTs inside a large organization, one of them might serve as coordinator and single point of contact to the external parties. Such teams are called Coordinating CSIRTs.

Such Coordinating CSIRTs are also established as independent entities serving a specific set of individuals and/or organizations known as a constituency. (…) The Coordinating CSIRT acts as single point of contact for the whole group and is focused on the overall security aspects of these organizations.

Today, national CSIRTs have been established as a distinctive type of Coordinating CSIRT to facilitate and often coordinate the activities of CSIRTs located in a particular nation or offer limited services for all citizens, specific sectors of critical infrastructure entities, etc. of this nation."

Many countries decided to use the "National Cyber Security Centre" (NCSC) term instead of national CSIRT, to make it clear that these entities provide a far broader range of services on a country level than pure incident response. Nevertheless, the NCSC label by itself does not mandate any particular set of services and NCSC and national CSIRT can be considered synonyms.[3]

While National CSIRTs have a special coordination role, they can still provide all services that enterprise CSIRTs do (as long as it is compatible with their mandate, of course). This includes real-time monitoring and detection capabilities.

They also typically act as an information-sharing hub for the national cyber security community. Many national CSIRTs even run ISACs for national constituency groups.

---

[2] In the EU context, "national CSIRT" should be read as "CSIRT in a Member State that has been designated under the national transposition of the NIS-D's Article 9 or NIS2-D's Article 10 respectively". More on the definition of a national CSIRT can be found here: https://cert.at/en/blog/2018/8/blog-20180731155524-2252

[3] Some countries may have both a NCSC and a National CSIRT as separate entities, similarly how some countries have multiple National CSIRTs. Exact services and responsibilities depend on regulations and policies that are specific to the particular country.

A National CSIRT can combine services that are provided by enterprise CSIRTs, SOCs and ISACs. **To avoid confusion, regulations should refer to specific services or functions that should be provided and not create new entities that would duplicate activities that can be implemented by National CSIRTs currently.**

Moreover, as the basic role of National CSIRTs in the EU is defined in the NIS directive, any future regulations should build upon these existing organizational structures. Whenever a functional gap is identified, it should be addressed using precise terms, to avoid the risk of misunderstanding.

Collaboration in the CSIRTs Network

Created by the original NIS directive in 2016, the CSIRTs Network became operational in 2017. It connects the designated CSIRTs of all member states plus CERT-EU.

Members of the Network actively collaborate with each other, primarily through the voluntary exchange of high-quality information. A set of Standard Operating Procedures governs the collaboration: these range from simple information classification rules up to predefined rules for large-scale cyber incidents.

The scope of the information exchanged as of 2023 includes: threat intelligence (indicators of compromise for, tactics techniques and procedures of threat actors, strategic reports), information about incidents and their impact, information on vulnerabilities, situational awareness, best practices and more.

Intelligence shared in the Network is used for detecting and preventing incidents in the Member States, including ones targeting critical infrastructure and governmental networks. Collaboration happens on a continuous basis, in case of active incidents the information can be shared almost immediately.

The CSIRTs Network itself selects collaboration tools and the necessary infrastructure is provided by ENISA and, voluntarily, members of the Network. Most human-to-human operational communication is happening on a chat (instant messaging) platform, while machine-to-machine data sharing is primarily handled by MISP[4].

Large amounts of information shared in the CSIRTs Network provide substantial value to all members. **This proves that the Network is an effective platform for collaboration between European CSIRTs and it should be further supported. The creation of any parallel sharing groups should be avoided unless they address specific use case that the CSIRTs Network cannot.**

[4] https://www.misp-project.org/

Proposal for cross-border platforms vs. existing CSIRTs' tasks

The CSoA proposal aims to increase collaboration in the EU and improve activities that are already implemented by CSIRTs. Article 2 of CSoA ("Definitions") calls for cross-border "information sharing", and "exchange of data from various sources". These activities are covered by the "Information security incident coordination", "Crisis management support" and "Communication" CSIRT services. Similarly, "production of high-quality intelligence" can be mapped to "Data acquisition", "Analysis and synthesis" and "Information security incident analysis" services. The NIS2 directive also tasks the CSIRTs in the member states to collaborate and share relevant information. In Article 15(3), the directive lists 16 tasks for the CSIRTs Network, including

> (b) to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;
>
> (c) to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;
>
> (d) to exchange information with regard to cybersecurity publications and recommendations;
>
> (e) to ensure interoperability with regard to information-sharing specifications and protocols;
>
> (f) at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities;
>
> (n) to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union;

We conclude that another intention of the CSoA is to improve the existing cross-border collaboration of the national CSIRTs by funding smaller groups of member states to improve on the level of integration that is provided by the existing CSIRTs Network.

Value of collaboration platforms developed jointly by Member States

While the CSIRTs Network is the default, EU-defined collaboration network of CSIRTs in Europe, it is far from the only one. TF-CSIRT originated in the framework of the interconnection of the European National Research and Education Networks (NREN), but has grown far beyond its academic roots. FIRST acts as the global forum for incident response teams. Additionally, there are a number of sector-specific collaborations (e.g., linking government or military CSIRTs), regional and national forums.

All national CSIRTs are used to operate in multiple cooperation forums. Each brings its own connections and added value. Some are more high-level, others operate on a strictly technical level.

While there exist some hard-won lessons learned regarding what makes such networks succeed[5], there is still much to be learned on how a tighter collaboration can work. Innovation in this space is very much welcome, and the CSoA proposing cross-border platforms linking national platforms provides the framework – and the funding – for exactly this innovation to happen.

In a way, these smaller collaboration platforms can be seen as laboratories for tighter integration of national CSIRTs. The funding provided by the CSoA can both improve the information sharing in the

[5] The head of CERT-Bund, [redacted], wrote an unpublished paper on the success factors of CSIRT collaboration. It is being shared in the CSIRTs Network.

national context as well as the bridge to partners across borders. Smaller groups can have a higher level of mutual trust than the full EU-27 (+CERT-EU) CSIRTs Network. It is also easier to deploy new technologies and protocols in self-selected groups of early adopters.

Innovation always carries the risk of failure. It is thus also helpful to try such ventures in a smaller environment.

As long as there is a culture of sharing between the CSoA–created cross-border platforms and the CSIRTs Network, both regarding operational information and the lessons learned by these platforms, then the creation of these cross-border platforms is in the long-term interest of all CSIRTs Network members.

Recommendations

Further development of capabilities to detect, react, and prevent cyber threats in the EU is needed. We welcome all initiatives that can support this goal, including new funding opportunities. We also agree with the emphasis on increasing cross-border collaboration in the CSoA, as the existing experiences from the CSIRTs Network prove the value of working together in a pan-European group.

We propose that for upcoming regulations (including CSoA) to achieve maximum efficacy, the following key considerations should be taken into account:

- **Gap identification and resolution.** It is important that these regulations accurately identify and rectify any deficiencies within the present capabilities and cooperation mechanisms. Feedback from entities having an operational role in NIS1 and NIS2 is essential for a comprehensive gap analysis.
- **Duplication avoidance.** Careful consideration should be exercised to prevent establishing entities that might replicate the functions of those already in existence.
- **Precision in terminology.** Precision and clarity in the usage of language and terminology is important to minimize the risk of misunderstandings.

Referring to the original draft of the CSoA in particular, **we consider the term "national SOC" imprecise, as it might suggest creating new operational entities** that provide monitoring services for a national infrastructure. As explained in the previous sections, this overlaps with services that can be provided by National CSIRTs and their mandate as defined in NIS2. Indeed, the CSoA could refer to National CSIRTs themselves as entities coordinating information exchange on the national level or, alternatively, use a term like "national platforms supporting SOC collaboration" which would make it clear that the intention is to build upon existing national collaboration networks.

Similarly, a "cross-border SOC" might be mistaken for a team that performs detection across several Member States, since such teams are common in the private sector. **A term that would better fit the intended purpose of such new mechanism would be "cross-border collaboration platform"**, as described in the previous section.

Our comments in this paper are provided to clarify the role of National CSIRTs and the CSIRTs Network, and how upcoming regulations could build upon the existing well-functioning collaboration model. We hope that these explanations will be of value to stakeholders involved in work on the CSoA.

References

Kathryn Knerler, Ingrid Parker, Carson Zimmerman, 11 Strategies of a World-Class Cybersecurity Operations Center, MITRE, 2022, https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center

CSIRT Services Framework version 2.1, Forum of Incident Response Teams, https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

ENISA, Information Sharing and Analysis Centers (ISACs), http://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

NIS 2 Directive, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

SOC Definitions:

Wikipedia: The job of a Security Operation Center is the protection of an organization against cyber threats by establishing visibility into the operation of its IT systems, monitoring for signs of intrusions and following up on any such hints. This can include full Incident Response capabilities. It comprises both people, processes, and technology.

Mitre (2014): A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Mitre (2022): A SOC is a team, primarily composed of cybersecurity specialists, organized to prevent, detect, analyze, respond to, and report on cybersecurity incidents.

SANS (2018): A combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects.

SANS (2020): The core functions of a SOC are: collection, detection, triage, investigation, incident response.

McAfee (2013): The SOC is responsible for monitoring, detecting, and isolating incidents and the management of the organization's security products, network devices, end-user devices, and systems.

Trellix: Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Information Security Asia: A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents and threats. It serves as the nerve center for an organization's cybersecurity operations, providing real-time monitoring, incident response, and threat intelligence gathering.

FIRST (2023): SOCs typically handle many different facets of security operations and focus on information security event management (i.e., event monitoring and detection). A SOC monitors the networks and systems of its parent organization or constituency for unusual,

anomalous, or suspicious activity using some type of software or hardware (…). Some SOCs may also perform response activities using automated or predefined use cases or playbooks; they escalate any issues that do not align with those cases/playbooks to established contacts, or they promptly alert victim organizations. SOCs may provide information security incident management services and vulnerability management services independently or rely on other teams for support.