The Impact of CSA on CSIRTs in Europe – A high-level look

A CORAL project deliverable

Co-financed by the Connecting Europe Facility of the European Union

Document working group

Name	Affiliation	Role
Jean Lancrenon	ILNAS	Contributor
Gabriela Gheorghe	LHC	Contributor

Document history

Version	Date	Changes from previous
0.1	18/09/2023	Creation of document.
0.12	31/10/2023	Near-finalization of draft.

European Union funding

The CORAL project - of which this deliverable is a part - is Action no. 2020-LU-IA-0209, benefitting from European Union funding under the 2020 CEF Telecom Call[1].

The contents of this publication are the sole responsibility of ILNAS and the LHC and do not necessarily reflect the opinion of the European Union.

Acronyms

Acronym	Full meaning
ANEC GIE	*Groupement d'Intérêt Economique Agence pour la Normalisation et l'Economie de la Connaissance*
CB	Certification Body
CORAL	cybersecurity Certification based On Risk evALuation and treatment
CSA	Cybersecurity Act
CSP	Cloud Service Provider
CSIRT	Computer Security Incident Response TEam
ENISA	European Union Agency for Cybersecurity
EUCC	Common Criteria based European cybersecurity certification scheme
EUCS	European Union Cybersecurity Certification Scheme for Cloud Services
ILNAS	*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*
ISO	International Organization for Standardization
IT	Information Technology
ITSESF	IT Security Evaluation Facility
NCCA	National Cybersecurity Certification Authority
NIS2	Directive on measures for a high common level of cybersecurity across the Union

[1] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

Contents

1. Introduction

The CORAL project

The *cybersecurity Certification based On Risk evALuation and treatment* (CORAL) project (Action no. 2020-LU-IA-0209, benefitting from EU funding under the 2020 CEF Telecom Call[2]) aims to elaborate a toolkit and methodology to support the certification process in line with the Regulation (EU) 2019/881 (Cybersecurity Act - CSA)[3] in what concerns the self-certification and the basic level of assurance, as well as to enhance the exchange of good practices, collaboration and information sharing related to performing evaluations in line with this act. In particular, this project develops a light, efficient and straightforward evaluation method in line with the technical objectives of Article 51 of the CSA and based on risk assessments, to help SMEs achieve a 'basic' assurance level in the cybersecurity of their ICT product, process or service. This method can also be used for conformity self-assessments, also possible with the entry into force of the CSA.

The project partners are:

- The Luxembourg House of Cybersecurity[4] (LHC);
- The *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services* (ILNAS)[5] ; and
- The *Agence pour la normalisation et l'économie de la connaissance* (ANEC GIE)[6].

More information on the CORAL project and its partners can be found on the project website: https://coral-project.org/

Purpose and scope of this CORAL deliverable

Computer Security Incident Response Teams (CSIRTs) are, loosely-speaking, groups of cybersecurity experts that investigate and respond to computer security events – usually unexpected or anomalous - that may or may not be cybersecurity *incidents*, that is, capable of doing harm in one way or another to the affected ICT system or systems. Note that a computer security incident may or may not be malicious. This is generally referred to as security incident management.

CSIRTs may also play more proactive roles, such as providing assistance and advice in identifying threats and vulnerabilities in such a way as to close avenues of future incidents, including attacks. The specific

[2] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity
[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/eli/reg/2019/881/oj
[4] https://lhc.lu/
[5] https://portail-qualite.public.lu/fr/acteurs/ilnas.html
[6] https://portail-qualite.public.lu/fr/acteurs/gie-anec.html

technical knowledge that CSIRTs have can greatly increase the overall quality management of an IT system[7].

This CORAL deliverable simply shows where in the CSA certification framework CSIRTs have a role to play, taking into account the NIS2 Directive and CSIRTs' activities explicitly listed in CSA certification schemes.

Important disclaimer

The authors stress that in no way does this deliverable affirm that the CSA will for certain affect CSIRTs in a given manner. The objective is simply to show from a high-level perspective some ways in which CSA and CSIRT activities can be related. How EU legislation evolves and how roles of CSIRTs ultimately take shape in the evolving regulatory context are out of the CORAL project's objectives.

2. Requirements on CSIRTs and their roles

General CSIRT activities

Taking as a reference Carnegie Mellon University's "CSIRT Services" white paper[8], one sees that in general CSIRTS can:

- Respond and treat incidents;
- Handle vulnerabilities;
- Perform security audits;
- Support in the configuration of systems and security tools; and
- Provide security consulting and security evaluation and certification.

Not all CSIRTs will have all of these services; but they are all in the realm of CSIRT competence, and thus are all able to be weighed against the various tasks that the CSA ecosystem may yield in terms of certification.

The NIS2 Directive

In the European Union (EU), a specific framework is in place to create and manage a network of national CSIRTs. Indeed, the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)[9] lays down obligations for Member States with respect to CSIRTs. Specifically:

- Article 10 requires that each MS appoint at least one national CSIRT in order to be able to perform services in specific sectors (deemed 'essential' or 'important') designated by the Directive[10];
- Article 11 lists the requirements, technical capabilities and tasks that those CSIRTs shall have;

[7] See for instance https://insights.sei.cmu.edu/library/csirt-services/
[8] https://insights.sei.cmu.edu/library/csirt-services/
[9] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[10] In the language of the Directive, essential and important entities, among others. One can consult Annexes I and II of the Directive

- Article 12 indicates that at least one of these CSIRTs shall be responsible for coordinated vulnerability disclosure, cooperating with other EU CSIRTs appointed to also hold that role in their respective Member States, and in particular contributing to a European vulnerability database; and
- Article 15 establishes the create of the CSIRTs Network, a pan-European network of national CSIRTs designed to facilitate coordination at the EU level on matters of knowledge sharing, in particular vulnerabilities, threats, best practices, and support in capacity building.

The table below shows how the points of NIS2's Article 11 map to the broad categories of general CSIRT services.

General CSIRT service	Article 11 point
Handle incidents, Perform security audits	(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;
Handle vulnerabilities	(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;
Handle incidents	(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;
Provide security consulting and security evaluation and certification	(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
Perform security audits, Provide security consulting and security evaluation and certification	(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;
Support in the configuration of systems and security tools	(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;
Handle vulnerabilities	(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);
Support in the configuration of systems and security tools	(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

Note however that the NIS2 Directive does not frame all entities that may consider themselves CSIRTs in the EU.

We shall see further in the deliverable how CSIRT activities can serve the CSA.

3. ENISA's role in relation to CSIRTs

Part of the CSA's content – see Title II – entails in establishing ENISA as the European Union's permanent agency for cybersecurity. Accordingly, ENISA's roles and responsibilities are also described, and some of these are directly in relation to the activity of the CSIRTs in the CSIRTs Network created by the NIS2 Directive. We summarize these points below:

- CSA Recital 25: ENISA should assist Member States in setting up their CSIRTs;

- CSA Recital 31: ENISA should support in aggregating and disseminating CSIRT information for the purpose of coordinated and harmonized information sharing, in particular in the NIS2 CSIRTs network;
- CSA Recital 46: ENISA should, in its capacity of secretariat of the NIS2 CSIRTs Network, facilitate cooperation and coordination among the CSIRTs, in particular in handling of incidents involving at least two such CSIRTs. Note that this covers the case of cross-border incidents;
- CSA Article 6.1., points (d) and (g): ENISA supports the development and harmonization of national CSIRTs in the context of the NIS2 Directive;
- CSA article 7.3: ENISA is the secretariat for the NIS2 Directive CSIRTs Network; and
- CSA Article 7.4: ENISA supports NIS2 Directive CSIRTs' operational cooperation.

The NIS2 Directive also explicitly mentions how the CSIRTs of the CSIRTs Network should interact with ENISA:

- NIS2 recital 43: ENISA should assist Member States in setting up their CSIRTs;
- NIS2 Recital 62 and Article 12.2, and more precisely also point (c): ENISA shall develop and maintain a European vulnerability database. Vulnerabilities listed in the database shall include either availability of patches, which can be developed by CSIRTs, or guidance on how vulnerable ICT products or services can mitigate the risk resulting from the vulnerabilities. This guidance may also come from CSIRTs; and
- NIS2 Article 15.2: ENISA shall provide the secretariat for the CSIRTs Network and provide active assistance to CSIRTs in that network.

Thus, one sees from these that ENISA plays on one hand an extremely active role in essentially

- Coordinating;
- Aiding in capacity building to have a common harmonized baseline of capabilities; and
- Supporting information sharing;

in the CSIRTs network.

On the other hand, ENISA shall put in place a very concrete tool to be placed at the disposition of the CSIRTs network, and other CSIRTs operating in the EU: a European vulnerability database to be populated by information from the CSIRTs.

4. CSIRT implication in the CSA certification schemes

Here we examine where CSIRTs are invited to contribute in the CSA's existing certification schemes. At the time of writing, these schemes are:

- The Common Criteria based European candidate cybersecurity certification scheme (EUCC), covering ICT products at the 'substantial' and 'high' levels of assurance, and based on the well-known Common Criteria[11] standards (also known as the ISO/IEC 15408 series on Evaluation

[11] https://www.commoncriteriaportal.org/cc/

criteria for IT security[12]), the final draft being publicly available here: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme; and

- The European Cybersecurity Certification Scheme for Cloud Services (EUCS), covering Cloud services classified according to capabilities type at the 'basic', 'substantial', and 'high' levels of assurance, the current draft being publicly available here: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

We also take a look at how CSIRTs might have their own services become the topic of certification schemes through a proposed CSA amendment.

Mentions of CSIRTs in the schemes' texts

Both certification schemes are structured in a similar way, owing essentially to the fact that the CSA (specifically, Article 51.1) specifies those elements that a given scheme shall contain, in turn leading to these elements mapping roughly to the schemes' chapters.

In particular, CSIRT activity is mentioned explicitly in both schemes' Chapter 14, which details how new vulnerabilities ought to be handled. In both cases, CSIRTs are stated as having a role to play mainly in a process known as *vulnerability disclosure*. The table below states these passages in each scheme.

EUCC (p. 53)	EUCS (p. 54)
When a correction has been brought to the certified product, the manufacturer or provider shall establish the necessary CVE with the support of the NCCA and related national CSIRT, and proceed to its publication on the relevant list, in accordance with the requirements of Article 55 of the CSA. ENISA shall be informed of the changes of status of the related certificates. NCCAs may develop their capacity to act as "coordinators" as defined in ISO/IEC 29147[13], and alternatively, designate their national CSIRT to play this role. In that case, the CSIRT shall have access to the necessary details related to the vulnerabilities and to the certificated ICT products.	When a correction has been brought to the certified cloud service, the CSP shall establish the necessary CVE with the support of the NCCA and related national CSIRT, and proceed to its publication on the relevant list, in accordance with the requirements of Article 55 of the CSA. ENISA shall be informed of the changes of status of the related certificates. NCCAs may develop their capacity to act as "coordinators" as defined in ISO/IEC 29147, and alternatively, designate their national CSIRT to play this role. In that case, the CSIRT shall have access to the necessary details related to the vulnerabilities and to the certificated cloud services.

In both cases, it appears that CSIRTs may generally only have a role to play as collectors of vulnerability information after a vulnerability has been treated by a provider or manufacturer of a certified product, or provider of a certified service. However, examining in more detail the overall content of both schemes' Chapter 14, it becomes apparent that CSIRT knowledge can, in theory at least, be handy in multiple stages.

Both schemes recommend following a vulnerability handling process structure standardized in ISO/IEC 30111 *Information technology - Security techniques - Vulnerability handling processes*[14]:

[12] https://www.iso.org/standard/72891.html
[13] ISO/IEC 29147 *Information technology Security techniques - Vulnerability disclosure*, https://www.iso.org/standard/72311.html
[14] https://www.iso.org/standard/69725.html

preparation, receipt, verification, remediation development, release, and ***post release***.

We go through these one after the other, in an effort to determine how CSIRTs could be involved, for the benefit of the provider or manufacturer (and also the certification bodies and National Cybersecurity Certification Authorities – NCCAs - involved).

Preparation

Both schemes specify that the manufacture or provider *"shall develop methods for receiving vulnerability information and make them public in accordance with Article 55.1.c) of the CSA"*[15].

It would be logical for there to be a proactive and open communication channel established with one or more CSIRTs – whether in the NIS2 CSIRTs Network or not – as these are certainly good sources of up-to-date vulnerability information. It is conceivable even that there might be an interest in CSIRTs monitoring certified equipment specifically over time.

Receipt

Upon being notified, or having been made aware of a vulnerability, providers or manufacturers have to keep the relevant certification bodies and NCCAs notified and in parallel begin conducting a vulnerability analysis in particular to determine the extent of the applicability of the vulnerability and its relevance to the certificate (in particular, if its applicability is in the scope of the declared assurance level), so as to determine if the ultimate course of action (which is part of the next step).

It would be logical - especially in the case the vulnerability is notified to the provider or manufacturer by a CSIRT, but in theory not only – for a CSIRT to assist in this vulnerability analysis. In the particular case of the EUCC, recall furthermore that the certification process will necessarily have gone not just through a certification body, but also an Information Technology Security Evaluation Facility (ITSEF) which will have conducted a vulnerability analysis commensurate to the assurance level prior to certification. It is not unreasonable to imagine a CSIRT collaborating with this ITSEF in this context as well. It is also not unreasonable to image that a CSIRT could actually be itself an ITSEF.

Verification and remediation development

The steps taken here involve concretely deciding whether a certificate should be suspended or even withdrawn pending remediation or patching. This is up to the certification body and provider or manufacturer. It was already mentioned that vulnerability analysis might be an area where a CSIRT could have added value; in the context of their tracking of vulnerabilities in general, CSIRTs may be interested in the remediation procedures implemented, in particular to document patches.

Release and post-release

See the beginning of the section.

[15] P. 51 in EUCC, p. 53 in EUCS

The proposed CSA amendment

In April of 2023, the European Commission proposed the Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services[16]. This is a proposed amendment to the CSA that concretely adds 'managed security services' to the list '"ICT products', 'ICT services', and 'ICT processes'" of fundamental categories of targets for CSA certification. The proposal in particular gives the definition of what a managed security service is:

> *"[…] a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy."*

(See p. 7 of the proposed text.) It is clear that CSIRTs in general - in regard to both the general tasks attributed to them and those specific to the NIS2 Directive - are squarely in the scope of the proposed amendment. This is by design, for at least two important reasons:

- Managed security service providers, and CSIRTs in particular, are themselves considered essential or important entities per the classification of the NIS2 Directive; and
- Managed security service providers, and CSIRTs in particular, are given the critical tasks of designing security to other essential and important entities.

Thus, in the near future, CSIRTs, in particular national ones involved in the NIS2 Directive CSIRTs network, may be the target of CSA certification in order to 1) gain sufficient assurance that these providers themselves are adequately protected and 2) gain sufficient assurance in their capacity to implement security effectively for other entities.

5. CSIRT overall tasks as viewed through the prism of the CSA

In this section, we aggregate the information from the sections above and make some suggestions as to how CSIRT activities can play a role in certain CSA processes.

The European vulnerability database

A key tool put into place by the NIS2 Directive is the establishment by ENISA of a European database of vulnerabilities that can serve as a baseline repository that all CSIRTs (not just those from the CSIRTs Network) can contribute to.

→ This European vulnerability database is ultimately populated in particular by CSIRT contributions and constitutes a key resource that providers or manufacturers of certified ICT products, services, or processes should monitor with respect to their certified offering.

→ The European vulnerability database is a key resource for certification bodies and ITSEFs that are tasked with checking vulnerabilities in the context of the certification process.

→ ITSEFs can also contribute to the database when doing vulnerability scanning that goes beyond simply checking for known weaknesses.

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208

NIS 2 Article 11 activities

Here, we try to showcase some avenues for CSIRTs to contribute to the CSA ecosystem through the points of the NIS2 Directive's Article 11.

(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;

→ Monitoring of essential an important entities' networks or information systems may yield vulnerabilities on components. Should those components be the subject of a certification, an analysis can be conducted to see to what extent the vulnerability is within the certification scope and whether a new component, or a patch of the current component, and a new certification are needed.

(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;

→ No particular remark.

(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;

→ Responding to incidents may yield new vulnerabilities, or new ways to exploit already known ones.

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

→ Forensic data could be of use to certification bodies or ITSEFs in the context of certificate management activities.

(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

→ See the remarks on point (a).

(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;

→ In case vulnerabilities are not yet able to be made public, they could be however circulate among CSIRTs in a limited dissemination effort.

(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);

→ Coordinated vulnerability disclosure is particularly important in the case of certified products, as there are scheme-specified response times that providers are allowed in order to respond to

vulnerability discovery. Coordination with the providers, NCCA, and related certification bodies is essential

(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

→ Secure information sharing tools can also be deployed with those bodies that are tasked with product or service evaluation in the context of certification, for them to gain access to specific vulnerability information know to the CSIRTs, but perhaps not yet public.

CSA certification schemes

→ It is clear from Section 4 that CSIRTs' knowledge is an added value to both certification, and re-certification, in particular for remediation.

→ CSIRTs may very well be the subject of CSA certificates of their own.

6. Conclusion

This high-level overview shows that there are many avenues for collaboration between CSIRTs, providers and manufacturers, and certification bodies, in particular ITSEFs. It also points to the European vulnerability database begin a cornerstone for this information sharing to be as vast and transparent as possible.

A much more refined study could entail examining what kinds of separation of duties and what specific procedures should be in place for concrete interactions between these entities.