How Resilmesh Supports the NIS2 Directive

A Policy Brief for National and EU Decision-Makers

March 2026

Executive Summary

Resilmesh[1] is an EU-funded research initiative developing a next-generation Security Operations and Analytics Platform Architecture (SOAPA) for heterogeneous, distributed digital infrastructures. This brief sets out how the Resilmesh technology portfolio directly supports the objectives and specific obligations of Directive (EU) 2022/2555 — the NIS2 Directive — which entered into force on 18 October 2024.

The NIS2 Directive establishes a high common level of cybersecurity across the EU, imposing obligations on essential and important entities in critical sectors and on the Member States that supervise them. Meeting these obligations requires not only organisational policies but functioning technical infrastructure. Resilmesh provides precisely this: a suite of interoperable components that enable entities to detect, respond to, and recover from incidents; to share threat intelligence; and to do so over resilient, standards-aligned communication infrastructure.

These brief maps five Resilmesh components to specific NIS2 provisions, set within the overarching Cybersecurity Mesh Architecture (CSMA) and Open XDR Architecture (OXA) frameworks that underpin their standards alignment:

Resilmesh Component	Role	Primary NIS2 Hook
Resilmesh SOAPA	Operational cybersecurity capabilities for essential and important entities	Article 21(2)(a)(b) (*Art. 21-Cybersecurity Risk Management Measures*)
CSMA[2] + Open XDR[3] Architecture	Architectural and standards framework justifying state-of-the-art and interoperability claims	Article 21(1), Article 25(1) (*Art. 25 Standardisation)*

[1] https://resilmesh.eu
[2] https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity-mesh-architecture-csma/
[3] https://github.com/opencybersecurityalliance/oxa

Resilmesh Component	Role	Primary NIS2 Hook
X-MESH (Interworking Mesh)	Open standards interoperability layer: CACAO, OpenC2, STIX 2.1, OCSF; Open Call 2 project; subset of Open XDR	Article 21(2)(b), Article 25(1), Article 29 (*Art. 29 Cybersecurity information-sharing arrangements)*
IoB[4] CTI Infrastructure	CTI sharing using OCA IoB STIX objects; Resilmesh implements a subset of the OCA IoB framework	Article 29, Article 30, Article 11(3)(a)(b) *(Art. 30 Voluntary notification of relevant information)*
CHAMELEON	Resilient NATS-based service mesh for inter-Security Operation Centre (SOC) communication; Open Call 2 project	Article 10(3), Article 11(1)(a) (Art. 10 CSIRTs) (Art. 11 Requirements and tasks of CSIRTS)

Resilmesh: Architecture and Components at a Glance

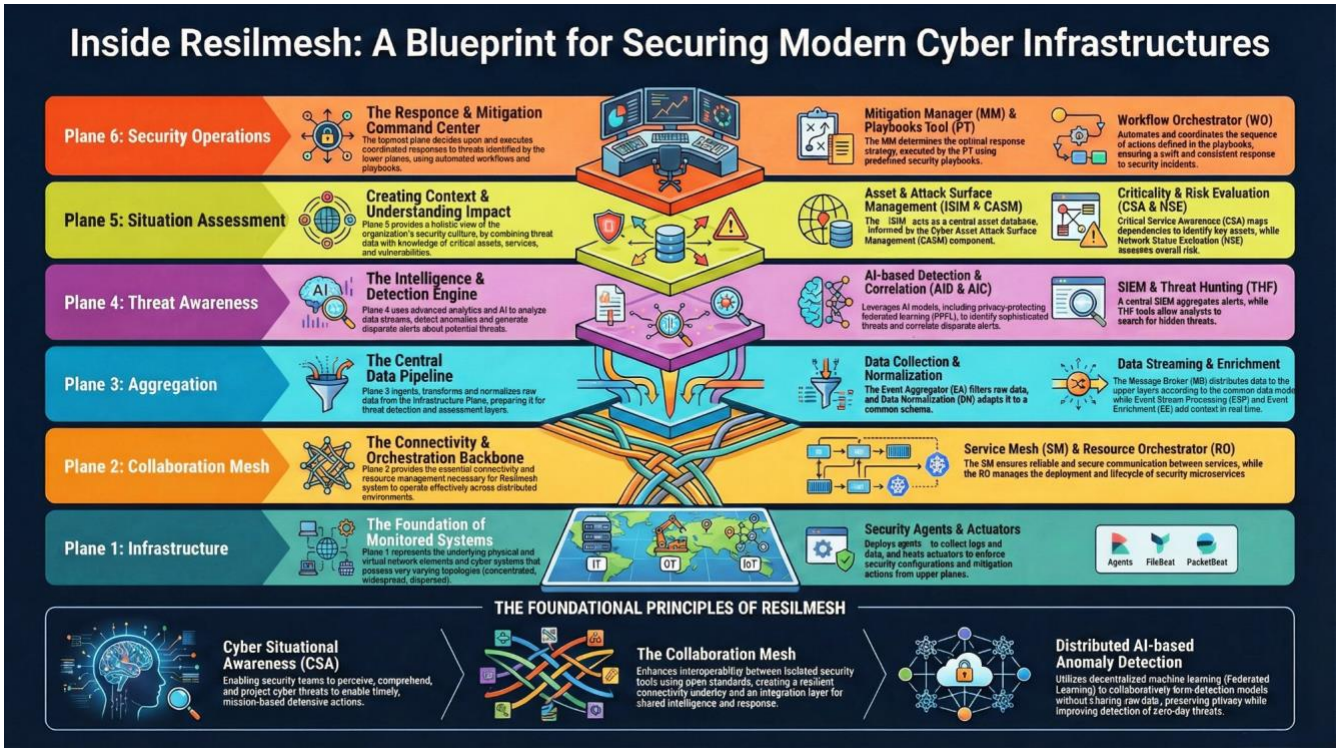
The following table provides a compact orientation for readers unfamiliar with the Resilmesh platform. Subsequent sections address each component in detail.

Component	What it is	Origin and Status
Resilmesh SOAPA	A modular Security Orchestration and Analytics Platform Architecture (SOAPA) organised across five planes: Security Operations, Situation Assessment, Threat Awareness, Aggregation, and Infrastructure.	Core Resilmesh project; EU-funded. See https://resilmesh.eu
CSMA (Cybersecurity Mesh Architecture)	An architectural framework for composable, distributed security in which controls, analytics, intelligence, and policy management operate through open interfaces. Adopted by Resilmesh as its foundational architectural model through the provision of defined Integration Reference Points and use of standardized protocols through the Resilmesh “Interworking Mesh” concept.	Industry framework articulated by Gartner; referenced in EU cybersecurity strategy discussions and Resilmesh architecture documentation.
Open XDR Architecture (OXA)	A standards framework maintained by the Open Cybersecurity Alliance (OCA) that operationalises CSMA principles through a defined stack: CACAO v2, STIX 2.1, OpenC2, OCSF/ECS, and Meshroom.	OCA open standard. See opencybersecurityalliance.org/open-xdr/

[4] opencybersecurityalliance.org/iob/

Component	What it is	Origin and Status
X-MESH	Expands the core Resilmesh Interworking Mesh through addition of a CACAO-native SOAR environment (SOARCA + CACAO Roaster), Meshroom declarative onboarding. Builds on OpenC2 enforcement, and STIX/TAXII CTI integration and provides an AI-assisted connector generator. Bridges Resilmesh internal planes with external tools (OpenCTI, DFIR IRIS, Cisco). A subset of Open XDR, not the full architecture.	Developed under Resilmesh Open Call 2 by Cyentific AS. All playbooks, Meshroom templates, and connectors released as open-source to OCA/OXA and OASIS communities.
Indicators of Behavior (IoB) CTI Infrastructure	A structured CTI sharing platform implementing OCA Indicator of Behaviour (IoB) STIX 2.1 objects over TAXII and MISP. Enables machine-readable sharing of behavioural threat intelligence within defined entity communities.	Based on OCA IoB specification; Resilmesh implements a subset of the full OCA IoB framework suited to SOC-to-SOC sharing. See opencybersecurityalliance.org/iob/
CHAMELEON	A NATS-based sidecar-less service mesh extending Resilmesh's Connectivity and Interoperability Resilience Plane (CIRP). Implements Chameleon Pod Defense (CPD): Moving Target Defense via randomised pod recycling, NATS queue group redundancy, honeytoken intrusion detection, and zero-downtime rerouting.	Developed under Resilmesh Open Call 2 by Sunesis d.o.o. Technology is generically applicable beyond Resilmesh to any Kubernetes-based inter-SOC or CSIRT communication infrastructure. Grounded in NIST SP 800-160 Vol. 2 resilience engineering principles.

Figure 1: The Resilmesh SOAPA — six-plane architecture and foundational principles



Source: Resilmesh project (resilmesh.eu). The six planes — Infrastructure, Collaboration Mesh, Aggregation, Threat Awareness, Situation Assessment, and Security Operations form the SOAPA referenced throughout this brief.

1. The NIS2 Compliance Challenge

The NIS2 Directive represents a fundamental step-change in EU cybersecurity regulation. It extends mandatory cybersecurity obligations to a significantly larger set of entities across eleven sectors of high criticality (Annex I) and seven other critical sectors (Annex II), imposing binding requirements on risk management, incident reporting, governance, and information sharing.

The core tension for essential and important entities is that NIS2 defines what must be achieved in terms of policies, procedures and outcomes, but leaves the choice of technical implementation largely to entities themselves. **Article 21(1)** requires measures that ensure a level of security appropriate to the risks posed, taking account of the state of the art. Recitals 4 and 5 identify fragmentation in cybersecurity implementations across Member States as the central problem the directive is designed to address. This creates a practical need for reference architectures and implementations that entities and supervisors can point to as evidence of compliance.

Resilmesh addresses this need. Its technology portfolio is grounded in two widely recognised open frameworks — the Cybersecurity Mesh Architecture and the Open XDR Architecture — that directly address the state-of-the-art and standardisation requirements of the directive. The following sections examine how this plays out across the Resilmesh component set.

2. Architectural Foundations: CSMA, Open XDR, and NIS2

2.1 Cybersecurity Mesh Architecture (CSMA)

The Cybersecurity Mesh Architecture (CSMA), adopted as the foundational architectural framework of Resilmesh, posits that cybersecurity should be composable and distributed rather than monolithic. Security controls, analytics, intelligence, and policy management operate as an integrated mesh through open interfaces, rather than as a collection of siloed point products.

CSMA is directly relevant to NIS2 at two levels:

- **State of the art (Article 21(1)):** CSMA is a recognised industry architectural model. Entities implementing a CSMA-aligned security architecture can credibly claim to be adopting a state-of-the-art approach to the security of their network and information systems, as required when assessing the proportionality of risk-management measures under Article 21(1).
- **Addressing fragmentation (Article 25(1) and Recitals 4–5):** The fragmentation problem that NIS2 is designed to solve — divergent cybersecurity implementations creating inconsistency and undermining cross-border cooperation — is precisely the problem that CSMA addresses architecturally. A CSMA-aligned platform provides an architectural response to the structural problem that Article 25 and the recitals identify.

2.2 Open XDR Architecture (OXA)

The Open XDR Architecture (OXA), developed by the Open Cybersecurity Alliance (OCA), provides the standards framework through which CSMA principles are operationalised for detection and response. OXA defines a specific stack of open protocols and formats:

- CACAO v2[5] — machine-readable playbooks for automated security orchestration and response
- STIX 2.1[6] — structured representation of cyber threat intelligence
- OpenC2[7] — machine-readable commands for execution against security controls
- OCSF / ECS [8]— normalised telemetry and event data schemas
- Meshroom [9]— declarative capability onboarding and tool integration (part of the OXA framework)

Open XDR translates CSMA's architectural philosophy into a concrete, vendor-neutral standards stack. For NIS2 purposes, OXA is the mechanism through which the Article 25(1) encouragement of European and international standards is given practical content. Entities and Member States adopting OXA-aligned tools are implementing a defined, open, internationally recognised set of standards rather than proprietary vendor approaches.

The OXA standards stack maps directly to substantive NIS2 obligations:

- **Article 21(2)(b) — Incident handling:** CACAO v2 playbooks enable automated, machine-readable incident response that is both documented and reproducible.
- **Article 29(1) — CTI sharing:** STIX 2.1 and TAXII provide the structured, interoperable format for the categories of threat intelligence that Article 29(1) identifies as shareable.
- **Article 25(1) — Standardisation:** The OXA stack constitutes precisely the kind of international technical specification that Article 25(1) encourages Member States to promote.

2.3 Open XDR as Interworking Mesh

Resilmesh's Interworking Mesh in an implementation of OXA and is partly implemented in the core project and partly by the X-MESH product. It is a subset of Open XDR — not the full architecture — specifically the interoperability and integration layer connecting Resilmesh's internal security planes with external tools and third-party systems.

The Interworking Mesh introduces:

- A CACAO-native SOAR environment combining SOARCA (execution engine) and CACAO Roaster (playbook editor), providing open, standards-compliant orchestration within the Security Operations Plane
- Meshroom as the declarative onboarding mechanism, enabling Resilmesh components and external products to publish their available actions and data flows

[5] https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html
[6] https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html
[7] https://openc2.org/
[8] https://schema.ocsf.io/
[9] https://github.com/opencybersecurityalliance/meshroom

through YAML and Python descriptors — establishing a plug-and-play integration fabric

- OpenC2 actuator profiles for command execution against network and endpoint controls, enabling machine-readable mitigation enforcement (demonstrated against Cisco devices)
- STIX/TAXII integration with OpenCTI for CTI exchange, OCA STIX 2.1 IoB extensions, and DFIR IRIS for incident case management
- An AI-assisted integration generator that automatically parses OpenAPI specifications to create and maintain CACAO-compliant connectors, reducing integration time from days to minutes

The NIS2 significance of the Interworking Mesh operates at two levels. First, it is a working implementation: it demonstrates that the OXA standards stack can be deployed against real tools in operational environments — the kind of practical reference material that competent authorities and ENISA need when developing supervisory guidance under Articles 21(5) and 25(2). Second, it is an open contribution: all CACAO playbooks, Meshroom templates, and integration connectors are released as open-source artefacts to the OCA/OXA and OASIS communities, creating reusable assets for national SOCs and CSIRTs across the EU.

> *The relationship between CSMA, Open XDR, and Interworking Mesh forms a coherent standards hierarchy: CSMA provides the architectural philosophy justifying Resilmesh as a state-of-the-art approach (Article 21(1)); Open XDR provides the standards stack implementing that philosophy (Article 25(1)); and the Interworking Mesh provides the working implementation validating those standards in operational practice — directly relevant to Articles 21(2)(b) and 29.*

3. Resilmesh SOAPA: Supporting Article 21

3.1 The Regulatory Requirement

Article 21(2) requires essential and important entities to implement an all-hazards approach to cybersecurity risk management. The Resilmesh SOAPA provides operational capability relevant to two of these measures in particular: policies on risk analysis and information system security (Article 21(2)(a)) and incident handling (Article 21(2)(b)).

It is important to be precise here: Article 21(2) defines policy obligations. Entities must have such policies in place. What the Resilmesh SOAPA provides is the operational infrastructure through which those policies can be enacted and made demonstrable to supervisory authorities.

3.2 How the SOAPA Platform Supports Compliance

Article 21(2)(a) — Risk analysis: The Situation Assessment Plane, incorporating the Cyber Asset Attack Surface Management (CASM) and Infrastructure and Services Information Model (ISIM) components, provides continuous analysis of the entity's network and information system exposure. This supports the enactment of a risk analysis policy by providing the real-time asset and threat visibility on which meaningful risk analysis depends.

Article 21(2)(b) — Incident handling: The Security Operations Plane — including the AI-based Detector, SIEM, Threat Hunting and Forensics (THF), and the Workflow Orchestrator with Playbooks Tool — provides end-to-end incident detection, triage, and response capability. Through X-MESH, incident response is further automated via CACAO playbooks and OpenC2 commands, making the incident handling process both documented and machine-executable.

Article 21(1) — State of the art: The SOAPA's grounding in CSMA architecture and implementation of OXA standards provides a well-founded basis for claiming that the platform reflects the state of the art. This is an architectural position grounded in recognised international frameworks, not a marketing assertion.

> *The Resilmesh SOAPA does not replace the policy obligations under Article 21(2) — entities must still adopt the relevant policies. What Resilmesh provides is the operational infrastructure that makes those policies real, measurable, and demonstrable to supervisory authorities under Chapter VII.*

4. IoB CTI Infrastructure: Supporting Article 29

4.1 The Regulatory Requirement

Article 29 — Cybersecurity information-sharing arrangements — requires Member States to ensure that entities can exchange on a voluntary basis relevant cybersecurity information, including cyber threats, near misses, vulnerabilities, indicators of compromise, adversarial tactics, techniques and procedures, and cybersecurity alerts. Article 29(2) requires such sharing within defined communities of entities. Article 29(3) specifies that sharing arrangements may use dedicated ICT platforms and automation tools.

Additional relevant provisions:

- **Article 11(3)(a):** CSIRTs shall monitor and analyse cyber threats, vulnerabilities and incidents at national level.
- **Article 11(3)(b):** CSIRTs shall provide early warnings, alerts and dissemination of information on cyber threats, vulnerabilities and incidents, if possible, in near real-time.
- **Article 30:** entities may voluntarily notify CSIRTs of cyber threats and near misses.
- **Article 7(2)(h):** national cybersecurity strategies shall include procedures and tools to support voluntary cybersecurity information sharing between entities.

4.2 How the IoB Infrastructure Supports Compliance

The Resilmesh IoB CTI sharing infrastructure implements a subset of the OCA Indicator of Behaviour (IoB) specification, using OCA IoB STIX 2.1 objects over an authenticated HTTPS REST API, deployed as a two-site testbed.

Content alignment (Article 29(1)): OCA IoB STIX objects carry behavioural threat intelligence — precisely the categories Article 29(1) identifies as shareable. Structured STIX objects enable machine-readable sharing, supporting the near real-time dissemination requirement of Article 11(3)(b).

Architecture alignment (Articles 29(2) and (3)): The authenticated REST API provides controlled-access sharing within defined entity communities, directly addressing the sensitivity requirements of Article 29(2). The dedicated platform satisfies Article 29(3)'s provision for dedicated ICT platforms.

Integration with the Interworking Mesh (Articles 29 and 21(2)(b)): The IoB infrastructure connects with Interworking Mesh through STIX/TAXII integration with OpenCTI and the MISP CTI connector, enabling received threat intelligence to feed directly into CACAO playbook execution. This closes the loop between intelligence sharing (Article 29) and automated incident response (Article 21(2)(b)) within a single open-standards framework.

> *Note on regulatory character: Article 29 frames CTI sharing as voluntary. NIS2 requires Member States to enable and facilitate such sharing — not to mandate it. The Resilmesh IoB infrastructure is therefore a technical enabler for what NIS2 encourages, providing the platform through which voluntary sharing can occur at scale with appropriate access control and structured, machine-readable payloads.*

5. CHAMELEON: Supporting Resilient Inter-SOC Communication

5.1 The Regulatory Requirement

Two NIS2 provisions directly mandate resilient communication infrastructure for CSIRTs:

- **Article 10(3):** Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders.
- **Article 11(1)(a):** CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times.

These provisions address the resilience of the communication fabric connecting CSIRTs to the entities they serve and to each other. The directive does not prescribe specific technical solutions, but the requirements — avoiding single points of failure, ensuring high availability, and maintaining resilience under adversarial conditions — are precise and demanding.

5.2 How CHAMELEON Supports Compliance

CHAMELEON is a NATS-based service mesh extending Resilmesh's Connectivity and Interoperability Resilience Plane (CIRP), implementing a Chameleon Pod Defense (CPD) framework for resilience and adaptive security in Kubernetes-native environments. Although developed within Resilmesh, the technology is generically applicable to any inter-SOC or CSIRT communication infrastructure and is grounded in NIST SP 800-160 Vol. 2 resilience engineering principles.

Eliminating single points of failure (Article 11(1)(a)): NATS queue groups maintain multiple active replicas of each service and support automatic message rerouting on pod or service failure, directly implementing the Article 11(1)(a) requirement.

Resilient communication infrastructure (Article 10(3)): The sidecar-less NATS-native architecture eliminates known vulnerabilities of conventional service meshes — sidecar injection, mTLS misconfiguration, ingress/egress control gaps — providing a more robust communication layer. The CPD framework adds Moving Target Defense through dynamic pod regeneration with randomised Time-to-Live values, configuration jitter, and honeytoken-based intrusion detection. Unauthorised access triggers immediate pod recycling and rerouting, maintaining communication availability even under active attack.

5.3 Broader Applicability

CHAMELEON's NIS2 relevance extends beyond Resilmesh. The technology addresses a generic infrastructure problem: how to maintain resilient, secure, and available communication between distributed security components under adversarial conditions. Any Member State or essential/important entity operating Kubernetes-based security infrastructure could deploy CHAMELEON's service mesh and CPD framework as a technical measure supporting compliance with Articles 10(3) and 11(1)(a).

6. Summary: Resilmesh Components and NIS2 Provisions

Component	NIS2 Article	Provision	How Resilmesh Addresses It
CSMA	Art. 21(1)	State-of-the-art risk management	Resilmesh's CSMA grounding provides a recognised architectural basis for state-of-the-art compliance
CSMA	Art. 25(1), Recitals 4–5	Standardisation; addressing fragmentation	CSMA directly addresses the interoperability and fragmentation problems NIS2 identifies at architectural level
Open XDR (OXA)	Art. 21(2)(b)	Incident handling	CACAO v2 playbooks enable automated, documented, machine-readable incident response
Open XDR (OXA)	Art. 25(1)	European and international standards	OXA stack (CACAO, STIX 2.1, OpenC2, OCSF) constitutes the standards that Article 25 encourages Member States to promote
Open XDR (OXA)	Art. 29(1)	CTI sharing content	STIX 2.1 and TAXII provide the structured format for the threat intelligence categories Article 29(1) identifies
Interworking Mesh	Art. 21(2)(b)	Incident handling (operational)	SOARCA CACAO-native SOAR with OpenC2 enforcement provides working automated response against real targets
Interworking Mesh	Art. 25(1)	Standardisation — reference implementation	Open-source CACAO playbooks and Meshroom templates are reusable artefacts for national SOCs and CSIRTs

Component	NIS2 Article	Provision	How Resilmesh Addresses It
Interworking Mesh	Art. 29(1)(3)	CTI sharing via STIX/TAXII	STIX/TAXII with OpenCTI and OCA IoB extensions operationalises CTI sharing through automated playbook execution
Resilmesh SOAPA	Art. 21(2)(a)	Risk analysis and information system security	Situation Assessment Plane (CASM, iSIM) provides continuous asset and threat visibility supporting risk analysis policies
Resilmesh SOAPA	Art. 21(2)(b)	Incident handling	Security Operations Plane (Detector, SIEM, THF, Workflow Orchestrator) provides end-to-end detection, triage and response
IoB CTI	Art. 29(1)(2)(3)	Cybersecurity information-sharing arrangements	OCA IoB STIX subset over authenticated REST API provides structured, access-controlled CTI sharing within defined entity communities
IoB CTI	Art. 11(3)(a)(b)	CSIRT threat monitoring and early warning	Machine-readable STIX payloads support near real-time threat intelligence for CSIRT workflows
IoB CTI	Art. 30	Voluntary notification	Infrastructure enables voluntary reporting of behavioural indicators and threat data to competent authorities
IoB CTI	Art. 7(2)(h)	National strategy: information-sharing tools	IoB platform provides the dedicated ICT tool that national strategies under Article 7(2)(h) are required to promote
CHAMELEON	Art. 10(3)	Resilient CSIRT communication infrastructure	NATS-native sidecar-less service mesh eliminates single points of failure and known mesh vulnerabilities
CHAMELEON	Art. 11(1)(a)	High availability, no single points of failure	NATS queue groups with automatic rerouting on pod failure ensure zero-downtime message delivery under attack or failure

7. Conclusions and Recommendations

For National Competent Authorities

NIS2 competent authorities are tasked with supervising essential and important entities' compliance with Article 21. When assessing whether an entity's cybersecurity posture meets the state-of-the-art standard of Article 21(1), an entity deploying a CSMA-aligned, OXA-standards-based SOAPA such as Resilmesh provides a well-grounded evidential basis for compliance. Competent authorities developing supervisory methodologies under Article 31(2) may wish to reference CSMA and Open XDR alignment as indicators of state-of-the-art compliance in guidance to supervised entities.

For Member States

Member States are required by Article 10(3) to ensure that national CSIRTs have resilient communication infrastructure. The CHAMELEON NATS-based service mesh and Chameleon Pod Defense framework represents a technically mature approach to this requirement in Kubernetes-native deployments and should be evaluated as a candidate for inter-CSIRT and entity-to-CSIRT communication resilience investment.

Member States are required by **Article 7(2)(h)** to include in their national cybersecurity strategies procedures and tools to support voluntary information sharing. The Resilmesh IoB CTI infrastructure, implementing OCA IoB STIX 2.1 over an authenticated REST API, provides a reference implementation of such a platform that Member States could adopt, adapt, or reference in their national strategies.

For the European Commission and ENISA

ENISA is tasked under **Article 25(2)** with drawing up advice and guidelines on technical areas relevant to standardisation. The Interworking Mesh implementation of the OXA Interworking Mesh — including open-source CACAO playbooks, Meshroom templates, and OpenC2 connectors contributed to the OCA and OASIS communities — represents validated technical work that ENISA could draw on when developing such guidance, particularly in relation to SOC interoperability and automated incident response.

The Commission's implementing acts under **Article 21(5)** will lay down technical and methodological requirements for managed service providers and managed security service providers. Resilmesh's technology portfolio — developed through EU-funded research, validated in operational testbeds, and grounded in CSMA and Open XDR — offers practical reference material for the development of those implementing acts.

> *Resilmesh demonstrates how EU-funded research can deliver practical, standards-aligned technical infrastructure that directly addresses the implementation challenges of the NIS2 Directive. The portfolio — spanning SOC operations grounded in CSMA, Open XDR-based automation and interoperability via X-MESH, structured CTI sharing via the IoB infrastructure, and resilient inter-SOC communication via CHAMELEON — provides a coherent and grounded technical response to the compliance challenge that thousands of essential and important entities across the EU now face.*

Annex: Quick Reference — NIS2 Articles and Resilmesh Components

NIS2 Article	Subject	Resilmesh Component(s)
Article 7(2)(h)	National strategy: information-sharing tools	IoB CTI Infrastructure
Article 10(3)	Resilient CSIRT communication infrastructure	CHAMELEON
Article 11(1)(a)	CSIRT high availability, no single points of failure	CHAMELEON

NIS2 Article	Subject	Resilmesh Component(s)
Article 11(3)(a)	CSIRT threat monitoring and analysis	IoB CTI Infrastructure
Article 11(3)(b)	CSIRT early warning dissemination	IoB CTI Infrastructure
Article 21(1)	State-of-the-art risk-management measures	CSMA; Open XDR
Article 21(2)(a)	Risk analysis and information system security	Resilmesh SOAPA — Situation Assessment Plane
Article 21(2)(b)	Incident handling	Resilmesh SOAPA — Security Operations Plane; X-MESH (CACAO/OpenC2)
Article 25(1)	Standardisation and technical specifications	CSMA; Open XDR; Interworking Mesh (reference implementation)
Article 29(1)(2)(3)	Cybersecurity information-sharing arrangements	IoB CTI Infrastructure; X-MESH (STIX/TAXII/OpenCTI)
Article 30	Voluntary notification of threats and near misses	IoB CTI Infrastructure

Resilmesh is funded by the European Union. Views and opinions expressed are those of the project consortium and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.