OSCRAT
Open-Source Cyber Resilience Act Tools

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT Use Cases And Best Practices Final Report (D4.1.)

27 August 2026
DIH Trakia

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre

Abstract

This report turns twelve OSCRAT product packages into a single, practical guide to preparing for the EU Cyber Resilience Act (Regulation (EU) 2024/2847). Written for readers who are not yet confident with the CRA, it walks through twelve worked examples — from a flawless self-assessment to a product blocked at the EU border — and shows how evidence about a product is converted into a defensible compliance decision. Each example covers intake, classification, SBOM and security-scan analysis, compliance scoring, and the green, amber or red outcome that follows, with checklists and a repeatable workflow that can be reproduced on the open-source OSCRAT platform at oscrat.eu.

At the time these assessment cases were developed, the final OSCRAT platform was still being completed. The cases therefore do not represent full post-launch user journeys carried out by external SMEs. Instead, this report presents 12 representative CRA assessment scenarios developed within the OSCRAT project and informed, as far as applicable, by WP4 stakeholder-engagement activities, including feedback gathered during workshops, training sessions, stakeholder consultations and testing activities. Their purpose is to demonstrate how different types of products can be assessed against the Cyber Resilience Act, derive practical best practices for manufacturers and SMEs, and illustrate how the OSCRAT tool supports the assessment process.

Keywords

Cyber Resilience Act; CRA; Regulation (EU) 2024/2847; OSCRAT; SBOM; CycloneDX; OpenSCAP; Annex I; Annex VII; declaration of conformity; Module A; conformity assessment; market surveillance; vulnerability handling; product with digital elements; CE marking; open source.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

DISCLAIMER

Table of content

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

1. Executive Summary

This report turns twelve real OSCRAT product packages into a single, practical guide to preparing for the EU Cyber Resilience Act (CRA), Regulation (EU) 2024/2847. It is written for people who are not yet confident with the CRA and simply need a credible way to begin. Rather than restating the legal text, it walks through twelve worked examples — from a flawless self-assessment to a product that must be blocked at the EU border — and shows, step by step, how evidence about a product is turned into a defensible compliance decision.

The CRA entered into force on 10 December 2024. Its main obligations apply from 11 December 2027, while the vulnerability- and incident-reporting obligations under Article 14 apply earlier, from 11 September 2026. Most products will follow manufacturer self-assessment (Module A), but products in the important and critical categories of Annex III and Annex IV face stricter conformity routes. The twelve examples here deliberately span the full operating range so that a reader can recognise their own product somewhere on the spectrum.

The portfolio is strong for learning because it covers every outcome a manufacturer might face: clearly compliant self-assessment cases, substantially compliant cases with bounded remediation, conditional or annotated declarations, and hard-stop surveillance cases ending in an import block or a withdrawal recommendation. It also exercises every major CRA workflow in practice — intake, classification, SBOM ingestion, security-scan import, compliance scoring, decision support, declaration generation and market-surveillance escalation. Across the reviewed packages the OpenSCAP baseline scores range from 18.18 to 91, with a portfolio median of 75.

Two honest caveats run through the whole document. First, several packages were assembled before the CRA's main application date, so they are best read as rehearsal, retrospective or forward-aligned material rather than evidence of live enforcement. Second, some packages use draft-era article numbers; this report normalises every reference to the final CRA structure — Article 28 and Annex V for the declaration of conformity, Article 31 and Annex VII for technical documentation, and Article 32 and Annex VIII for the conformity-assessment route. A normalisation step like this should be the first thing any team does before locking a route decision.

The recommended learning order moves from the happy path to the hard cases: PEX, SCBL, IPTCAMA04FC, then ZUC, FCR, LAR, then ANS, EVC, GSB, SBM, and finally IFG and VTN. That sequence minimises cognitive load, shows what good looks like first, then introduces ambiguity, and only then tests the decision logic under stress. Everything in this report can be reproduced on the open-source OSCRAT platform at oscrat.eu, and project team is available to help organisations that want support getting started.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

2. Introduction — what this report is and who it is for

If you make, import or distribute a product that contains software — anything from a smart sensor to an industrial gateway — the Cyber Resilience Act now applies to you. For many teams the first reaction is uncertainty: the Regulation is long, the annexes are dense, and it is not obvious where to start. This report exists to remove that uncertainty by showing the work, not just describing it.

It is written in the spirit of sharing experience with the community. The twelve examples are drawn from genuine OSCRAT assessment packages and are presented exactly as a practitioner would walk a colleague through them: here is the product, here is what we found, here is the decision we reached and why, and here is what the manufacturer should do next. By the end you should be able to look at your own product and know which of the twelve it most resembles, and therefore what your own first steps look like.

2.1 The EU Cyber Resilience Act in one page

The CRA is the EU's horizontal cybersecurity law for products with digital elements. It places obligations on manufacturers across the whole product lifecycle: perform and maintain a documented cybersecurity risk assessment; design and ship the product so that it is secure by default; provide free security updates without undue delay for a defined support period that is normally at least five years; handle vulnerabilities responsibly with a coordinated-disclosure policy and a contact point; and keep technical documentation that lets an authority verify all of this. When the product meets these requirements, the manufacturer draws up an EU declaration of conformity and affixes the CE marking.

The essential requirements live in Annex I. Part I covers the product's own security properties — no known exploitable vulnerabilities at release, secure defaults, the ability to be updated, access control, protection of data, a minimised attack surface, resilience, logging and secure data deletion. Part II covers the manufacturer's ongoing obligations — maintaining an SBOM, remediating without delay, testing, disclosing fixed vulnerabilities, running a coordinated-vulnerability-disclosure policy, distributing secure updates and providing free security updates. Annex II turns these into user-facing information. The reader does not need to memorise the annexes; the worked examples show how each one is satisfied in practice.

2.2 Why we built twelve examples

A single example teaches one path. Twelve examples chosen to span the full range teach judgement. The set was assembled so that each major decision — is this product in scope, which Annex category does it fall in, is the evidence trustworthy, is the outcome a clean declaration or something more constrained — appears in more than one product and under more than one set of conditions.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

That repetition is deliberate: it is how a reader builds an instinct for the CRA rather than a checklist they can only follow blindly.

The examples also cover different product worlds: consumer IoT, professional surveillance, retail point-of-sale and fiscal devices, electric-vehicle charging, agricultural and building-management OT, robotics, medical-adjacent wearables and AI edge analytics. Whatever sector you work in, at least one of the twelve will feel familiar.

2.3 How to read this report

Sections 2 and 3 set up the platform and the legal backbone. Section 4 gives a portfolio overview with summary tables you can scan in a minute. Section 5 is the heart of the document: twelve product reports, each a self-contained story. Section 6 is the repeatable workflow you can run yourself. Section 7 distils the lessons and gives you checklists. Section 8 explains how to start your own preparation with OSCRAT, and Section 9 concludes. The annexes provide a glossary, an evidence index and the decision vocabulary used throughout.

Throughout, a simple colour idea is used to describe outcomes: a green path means a clean self-assessment, an amber path means conformity is achievable but conditional on remediation or update reach, and a red path means no declaration is possible and the product must be remediated, blocked or withdrawn. Those three words — green, amber, red — carry most of the meaning.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

3. The OSCRAT platform and the open-source approach

OSCRAT — Open-Source Cyber Resilience Act Tools — is a platform for organising Cyber Resilience Act (CRA) evidence and turning it into a decision. It is developed under OSCRAT project, funded under the European Cybersecurity Competence Centre programme (Grant Agreement No. 101190180) and is available as open source at oscrat.eu.

OSCRAT project is committed to enhance cybersecurity resilience among European SMEs through the development of an open-source, completely free, tool dedicated to supporting compliance with the Cyber Resilience Act (CRA).

The goal is to equip small and medium-sized European enterprises, policy & decision makers, Digital Innovation Hubs and industrial associations with all the necessary resources to enhance cybersecurity practices in the modern digital landscape.

As it is open source, a manufacturer can adopt it without licence cost, inspect exactly how it reaches a conclusion, and adapt it to their own process. That transparency matters for a compliance tool: the reasoning behind a declaration of conformity should never be a black box.

The OSCRAT Tool :

- SBOM Generation: integration into the security pipeline to track the build process, enhance security and the risk of data corruption;
- Vulnerability Assessment: utilizes the Open Vulnerability and Assessment Language (OVAL) for publicly accessible security information, covering various operating systems with available public OVAL streams;
- Incident Response: The OpenSSF OSS-SIRT Special Interest Group guides SMEs on incident management according to international standards and reports incidents to ENISA, EU CyCLONe, and others;
- Identifying and evaluating vulnerabilities continuously, allocating and overseeing corrective measures. This helps to provide resilient compliance management, which will include the inclusion of compliance and risk into the development pipeline, and the management of compliance and risk treatment actions. It also provides an overall action management to track actions from all other modules;
- Documentation Centralization: OSCRAT tool creates a centralized repository for digital product documentation, including Conformity Assessment Reports, SBOM reports, Vulnerability Disclosure Policies, Incident Reports, and Certifications of Conformity. This comprehensive approach enhances transparency and facilitates compliance for SMEs
- Self-Assessment and Third-Party Audits: SMEs are able to do self-assessments and give auditors access to collected evidence from OSCRAT tools. This can lead to a conformity certificate, BUT the platform does not replace legal judgement or a notified body where one is required. What it does is make the evidence trail explicit and repeatable, so that the same

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

product assessed by two people reaches the same place, and so that an authority asking 'show me why' receives a clear answer.

Project Partners include:

PMF Research is an Italian SME based in Sicily

Unicis.Tech OÜ, based in Estonia

Digital Innovation Hub "Trakia, based in Bulgaria

Enersec company, based in Romania

Oves Enterprise, based in Romania

Łukasiewicz Research Network – Institute of Artificial Intelligence and Cybersecurity (Łukasiewicz – AI), based in Poland

3.1 The six-stage evidence pipeline

Every one of the twelve packages follows the same six-stage structure on disk, and the report uses it as the backbone for each product story. Stage one captures product information and CRA applicability. Stage two holds the software bill of materials. Stage three holds the security-scan results. Stage four is the compliance assessment against the CRA requirements. Stage five is the conformity-assessment report. Stage six is the declaration of conformity. Reading a package therefore means walking those six folders in order.

Stage	Folder	What it contains	CRA anchor
1	01-product-info	Product description, intended use, CRA applicability result	Article 13
2	02-sbom	CycloneDX software bill of materials	Annex I Part II
3	03-security-scans	OpenSCAP / XCCDF baseline and vulnerability notes	Annex I Part I
4	04-compliance-assessment	Product, procedures and 41-item documentation checklist	Annex I, II; Annex VII
5	05-conformity-report	Conformity-assessment report and scorecard	Article 32 / Annex VIII

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Stage	Folder	What it contains	CRA anchor
6	06-declaration-of-conformity	EU declaration of conformity (or its absence)	Article 28 / Annex V

Table 1 — The OSCRAT six-stage evidence pipeline used by every package.

3.2 Roles in a CRA assessment

A good assessment is a team exercise. The product owner supplies the package and confirms the intended use, support period and release state. A security assessor validates the SBOM, the scan results and the exploitability of any findings. A compliance lead normalises the legal references, validates the classification and route, and checks the declaration and documentation anchors. A documentation lead verifies completeness and traceability. A legal or authorised representative confirms whether the output is internal-only, issuable, conditional or blocked. In the red-path scenarios an importer, distributor or market-surveillance observer also takes part. Section 6 lists the minimum input each role brings.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

4. CRA reference model and OSCRAT normalisation rules

For learning and for reliability, every package should be measured against the same legal backbone. This section states that backbone in plain terms and then gives the normalisation rules that keep route decisions trustworthy.

4.1 The legal backbone

Manufacturers must perform and maintain a documented cybersecurity risk assessment over the product lifecycle; determine and disclose a support period that is normally at least five years; include that analysis in the technical documentation; and ensure that the product and its vulnerability-handling processes meet Annex I. Annex I Part I covers secure-by-design and secure-by-default properties. Annex I Part II covers SBOM practice, remediation without delay, testing, public disclosure of fixed vulnerabilities, a coordinated-vulnerability-disclosure policy, a contact address, secure update distribution and free security updates. Annex II governs the information given to users. Article 28 and Annex V govern the EU declaration of conformity. Article 31 and Annex VII govern technical documentation. Article 32 and Annex VIII govern the conformity-assessment route.

4.2 Reporting and market surveillance

From 11 September 2026, manufacturers must file an early warning within twenty-four hours and a fuller notification within seventy-two hours for actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements. Market-surveillance authorities may evaluate products that present a significant cybersecurity risk, require corrective action, withdraw or recall non-compliant products, and escalate to Union safeguard procedures. The two red-path examples in this report — IFG and VTN — are precisely where this machinery is exercised.

4.3 Normalisation rules

Two rules keep a pilot honest. First, a package identifier is not always the product-version identifier: a folder may read 1.0.0 while the assessed firmware is 2.1.0, as in the SBM case. Always separate the two so the folder name cannot silently override reality. Second, legal references must be canonicalised automatically: several packages carry outdated numbering, so the platform should map legacy labels to the final CRA structure before any dashboard or route suggestion is shown. A third practical rule earns its place from the SBM

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

case: quarantine malformed evidence and rely on the stated score only until the file is repaired.

4.4 The normalisation mapping table

The table below is the single reference a team can pin to the wall: for each CRA anchor it states what OSCRAT should check and why it matters.

Normalised CRA anchor	What to check	Why it matters
Article 13	Risk assessment, support period, lifecycle handling, third-party due diligence	Establishes the manufacturer's core obligations
Annex I Part I	Product security properties	Core 'ship secure' requirements
Annex I Part II	SBOM, CVD, update mechanisms, remediation, disclosure, monitoring	Core 'stay secure' requirements
Annex II	User information, support-period disclosure, update and contact instructions	Converts compliance into user-facing duties
Article 28 / Annex V	Declaration-of-conformity content and traceability	Needed for CE-mark-backed claims
Article 31 / Annex VII	Technical-documentation set incl. SBOM, CVD, update design, support rationale	Needed for auditability and authority access
Article 32 / Annex VIII	Route selection: Module A, B+C, H or certification	Determines whether self-assessment is enough
Articles 54–55	Corrective action, withdrawal, recall, safeguard	Required for surveillance and import-block cases

Table 2 — OSCRAT normalisation map from CRA anchors to assessment checks.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5. Portfolio overview

The twelve products split naturally into four lanes. The first lane is clean standard-PDE cases that pass self-assessment with only documentation polish. The second is standard-PDE cases with bounded remediation — strong packages that still contain fixable findings. The third is conditional or lifecycle cases, where conformity depends on remediation reach, constrained updates or a borderline classification. The fourth is surveillance cases that end in an import block or a withdrawal recommendation. Reading the portfolio in that order is the fastest way to build judgement.

5.1 Product summary table

Code	Product	OSCRAT class	Snapshot	Scan	Outcome
ANS	AgroNode Solar Pro IoT Hub	Standard PDE	10/14 product; 8/8 proc; 33/41 docs	71	DoC with long-lifecycle exception
EVC	ChargePoint AC Wallbox 7kW	Standard PDE	11/14; 8/8; 36/41	72	Conditional DoC
FCR	FCR PRO-2000 Fiscal Register	Standard PDE	48/49 overall; 41/41 docs	75	Substantially compliant; fix in v1.0.1
GSB	GlucoSense BLE Pro CGM	Standard PDE	10/14; 8/8; 33/41	65	DoC for patched state, annotated
IFG	InduFlow IIoT Gateway GW-200	Annex III-I	0/14; 0/8; 3/41	22	No DoC; import block
IPT	Comelit IP Turret Camera 4MP	Standard PDE	14/14; 8/8; 41/41	75	Compliant; 3 remediable findings
LAR	LogiBot AMR-500 Robot	Standard PDE	57/63; 6 partial; 0 NC	88.1	DoC issued
PEX	Percepta Edge X1 AI Platform	Standard PDE	13/14; 8/8; 39/41	91	DoC issued
SBM	Schneider EcoStruxure Edge Box	Annex III-I	10C/3P/1NC; 7C/1P; 34/41	76	DoC issuable with conditions
SCBL	SmartClean BG LiDAR	Standard PDE	14/14; 8/8; 41/41	75	Green-path standard-PDE case
VTN	VisionTech 8-Channel NVR	Annex III-I	0/14; 0/8; 5/41	18.18	Import block and withdrawal
ZUC	Zucchetti All-in-One POS	Standard PDE	13/14; 8/8; 38/41	78	Substantially compliant; v1.1.0

Table 3 — Portfolio summary across the twelve products.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.2 Annexes exercised and conformity routes

The next table separates the OSCRAT pilot classification from the final-law validation note. That distinction matters because the Article 32 route depends on whether a product truly falls within Annex III or Annex IV. Default-category products may use internal control under Module A; important and critical products may require stricter routes.

Code	Pilot class	CRA annexes exercised	Pilot route	Final-law validation note
ANS	Standard PDE	I, II, VII, V	Module A	Strong fit for default category
EVC	Standard PDE	I, II, VII, V	Module A intent	Strong fit; package uses legacy references
FCR	Standard PDE	I, II, VII, V	Module A	Strong fit for default category
GSB	Standard PDE	I, II, VII, V	Self assessment	Recheck Annex III-I item 19 (health wearable)
IFG	Annex III-I	I, II, VII, surveillance	No valid route	Recheck category; Article 32(2) discipline critical
IPT	Standard PDE	I, II, VII, V	Module A	Recheck only if sold as consumer smart-home camera
LAR	Standard PDE	I, II, VII, V	Article 32 self-assessment	Default plausible; high-risk AI would change it
PEX	Standard PDE	I, II, VII, V	Module A	Default plausible; high-risk AI would change it
SBM	Annex III-I	I, II, VII, V	Module A	Network-management fit defensible; revalidate 32(2)
SCBL	Standard PDE	I, II, VII, V	Module A	Strong fit for default category
VTN	Annex III-I	I, II, VII, surveillance	No valid route	Category arguable; surveillance path correct regardless
ZUC	Standard PDE	I, II, VII, V	Module A	Strong fit for default category

Table 4 — Annexes exercised and conformity routes, with final-law validation notes.

5.3 Score and outcome distribution

The OpenSCAP baseline scores cluster around the portfolio median of 75, with two clear outliers at the bottom — IFG at 22 and VTN at 18.18 — that correspond exactly to the two surveillance cases, and a clear top performer in PEX at 91. The simple lesson is that the baseline score alone already separates the green and amber cases from the red ones, even before the detailed compliance assessment begins.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Outcome category	Count	Products
DoC issued or clearly issuable	5	PEX, SCBL, LAR, ANS, IPTCAMA04FC
Conditional or annotated DoC	3	EVC, GSB, SBM
Substantial compliance with scheduled clean-up	2	ZUC, FCR
Import block or no DoC	2	IFG, VTN

Table 5 — Outcome distribution for the pilot portfolio.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6. Product Use cases — twelve worked examples

Each example below is self-contained. It opens with a fact table, tells the product's story in plain language, lists the findings and their severity in context, states the decision and why it was reached, gives the remediation actions, and ends with the single lesson worth carrying away. The order runs from the cleanest green-path case to the two red-path surveillance cases, which is also the order we recommend for a stakeholder pilot.

Key takeaway and OSCRAT support for each of the 12 assessment cases is clearly stated at the end of the description of the use cases.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.1 PEX — Percepta Edge X1 AI Analytics Platform

What security-by-design actually looks like.

Lane	Green path
Manufacturer	Percepta AI Systems S.r.l. (Italy)
Assessed version	1.0.0
CRA classification	Standard PDE (Other) — not Annex III/IV
Conformity route	Module A — Internal Production Control (self-assessment)
OpenSCAP baseline	91/100
Product requirements	13/14 (1 partial)
Manufacturer procedures	8/8
Technical documentation	39/41
Outcome	DoC issued — strongest green-path exemplar in the set
Reference	DOC-PEX-1.0.0-20260604

6.1.1. The story

The Percepta Edge X1 is the aspirational CRA product. Where most packages reveal a manufacturer retrofitting security — adding encryption here, patching a vulnerability there, writing a coordinated-vulnerability-disclosure policy after the fact — this Italian AI startup built GDPR and CRA security into the architecture from day one, before either regulation required it. The result is a device where privacy and security are structural properties rather than policy controls.

The headline design property is that no video ever leaves the device. Not because a privacy notice forbids it, but because there is no write path from the video pipeline to any network interface. An attacker could rewrite the configuration, compromise the operating system and disable the firewall, and video still would not leave the device, because the software architecture makes exfiltration structurally impossible. The claim was verified with seventy-two hours of network-traffic analysis showing zero video bytes on any interface.

Zero-trust is applied everywhere. Every internal service authenticates to every other service with a device-bound mTLS certificate, so there are no implicit trust relationships and a foothold in one process cannot reach another without a valid certificate. The AI itself is protected: proprietary model weights never leave a hardware-backed secure enclave, and Ed25519-signed model updates defend against supply-chain attacks aimed at the model — a threat vector most device makers have not yet considered.

6.1.2. Findings in context

Finding	Severity	Notes
CVE-2023-4863 (OpenCV, WebP heap overflow)	Contextual / informational	Present in a linked library and caught by automated SBOM scanning. SAST analysis proved the vulnerable code

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Finding	Severity	Notes
		path is unreachable from the analytics engine. Documented, quantified, and scheduled for upgrade in v1.0.1.
Standalone SCA report not yet attached	Documentation	Software-composition-analysis evidence to be packaged as a standalone artefact in the technical file.
Homomorphic-encryption preview feature under-documented	Documentation	A preview capability needs fuller description in the technical documentation.

6.1.3. Decision and remediation

Outcome: DoC issued — strongest green-path exemplar in the set.

The remediation actions are:

- Upgrade OpenCV to a fixed release and re-run the SCA in v1.0.1.
- Attach a standalone software-composition-analysis report to the technical file.
- Document the homomorphic-encryption preview feature in full.

6.1.4. Key takeaway and OSCRAT support

PEX shows that the cleanest CRA outcome is reached by making security a structural property of the architecture, so that the only open items are documentation polish rather than design defects. It is the reference for what excellent looks like for an AI edge device, and the natural first case to run in any pilot.

For an SME manufacturer in this position, OSCRAT is where an exemplary package is kept current rather than frozen in a PDF. Linking the version to its repository generates the SBOM with Syft and scans it with Grype, so a component finding such as CVE-2023-4863 is raised automatically, traced to the OpenCV component that introduced it and shown with its fixed-in version. The finding is recorded as a vulnerability on the version, the analysis proving the vulnerable path is unreachable is attached to that record as evidence, and the upgrade is scheduled as a task against v1.0.1 instead of living in a spreadsheet. The two documentation gaps appear directly in the Technical Documentation Checklist next to their Annex VII references, and each non-compliant entry produces a prefilled remediation task in one click. Once the checklist is closed, OSCRAT generates the Conformity Assessment Report from the completed assessment and unlocks the Declaration of Conformity wizard for the version.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.2 SCBL — SmartClean BG LiDAR Robot Vacuum

A textbook consumer-IoT self-assessment.

Lane	Green path
Manufacturer	Startdust Fine Edition Ltd. (Sofia, Bulgaria)
Assessed version	1.0.0
CRA classification	Standard PDE (Other) — not Annex III/IV
Conformity route	Module A — Internal Production Control (self-assessment)
OpenSCAP baseline	75/100 (9 of 12 rules pass)
Product requirements	14/14
Manufacturer procedures	8/8
Technical documentation	41/41
Outcome	Green-path standard-PDE case — 49/49 requirements compliant
Reference	DoC issuable

6.2.1. The story

The SmartClean BG LiDAR is a consumer robot vacuum cleaner with LiDAR navigation, MQTT-over-TLS cloud control and over-the-air updates. It is a clean example of a mass-market connected device that a manufacturer can take through Module A self-assessment without a notified body. Its SBOM lists ten components in CycloneDX 1.4 form, including FreeRTOS 10.5.1, lwIP 2.2.0, Mbed TLS 3.5.2, Eclipse Paho MQTT, ESP-IDF Wi-Fi, the RPLIDAR SDK, cJSON, MCUboot and two proprietary modules.

Every product-security question and every procedure question passed, and all forty-one technical-documentation checklist items were present. The OpenSCAP baseline returned seventy-five out of one hundred, with three medium-or-low findings that already have funded remediation planned for the v1.1.0 release. This is exactly the profile a pilot should show first: a strong package whose residual findings are bounded, scheduled and honestly disclosed.

6.2.2. Findings in context

Finding	Severity	Notes
Predictable setup access-point password	Medium	The temporary Wi-Fi setup password is derived from the device MAC address and is therefore guessable during commissioning.
Unencrypted room-map storage	Medium	The LiDAR room map is stored at rest without encryption, exposing floor-plan data if the device is physically accessed.
Limited security logging	Low	Security events are logged but cannot be exported, limiting forensic value.

6.2.3. Decision and remediation

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Outcome: Green-path standard-PDE case — 49/49 requirements compliant.

The remediation actions are:

- Replace the MAC-derived setup password with a random per-device secret.
- Encrypt the stored room-map data at rest.
- Add exportable security logging, including failed-association logging.

6.2.4. Key takeaway and OSCRAT support

SCBL demonstrates that a high-quality consumer-IoT package can be fully compliant on paper while still carrying a small set of fixable hardening items. It shows how OSCRAT keeps bounded residual issues visible, scheduled and linked to the rule that produced them, without blocking a declaration of conformity.

For an SME manufacturer of a consumer device like this, the configuration scan is the entry point. The OpenSCAP artefact is uploaded in ARF, XCCDF or OVAL form and rendered into a read-only report with per-rule results, CCE identifiers, severities and pass/fail counts, and each of the three failed rules offers a one-click remediation task prefilled with the rule reference and its severity. Those tasks carry owners and due dates, so the v1.1.0 hardening work is visible next to the requirements it affects, and the report links back to the task instead of offering a duplicate. Because the fourteen product-security requirements and the forty-one checklist items are all recorded as fully compliant with their evidence attached, the Declaration of Conformity can be issued for v1.0.0 while the residual tasks stay open; re-uploading a fresh scan after the fixes updates the report and closes them.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.3 IPTCAMA04FC — Comelit IP Turret Camera 4MP ColorUP AI

A complete package on a large network attack surface.

Lane	Green path / minor remediation
Manufacturer	Comelit Group S.p.A. (Rovetta, Italy)
Assessed version	Firmware 5.1.4.1_59514
CRA classification	Standard PDE (Other) — professional CCTV, not Annex III/IV
Conformity route	Module A — Internal Production Control (self-assessment)
OpenSCAP baseline	75/100 (9 of 12 rules pass)
Product requirements	14/14
Manufacturer procedures	8/8
Technical documentation	41/41
Outcome	Compliant path with three remediable findings
Reference	DoC issuable

6.3.1. The story

The Comelit IPTCAMA04FC is an AI-enabled professional IP surveillance camera with an unusually broad network protocol surface — more than thirty network protocols and on-device AI video analytics. Despite that surface, the package is complete: all fourteen product-security questions, all eight procedure questions and all forty-one technical-documentation items are satisfied, and the manufacturer is a named EU company with a genuine vulnerability-handling process.

The OpenSCAP baseline is seventy-five out of one hundred. Three medium findings remain, each with a target remediation quarter, plus one informational observation that the firmware still links OpenSSL 1.1.1w, which reached end of life. Classification should only be revisited if the device were ever marketed as a consumer smart-home camera rather than professional CCTV, which would change the Annex analysis.

6.3.2. Findings in context

Finding	Severity	Notes
Data-at-rest encryption absent	Medium	SD-card recordings and the configuration database are not encrypted. Target: Q4 2026.
Excess default-enabled network services	Medium	Several services are enabled by default, enlarging the attack surface. Target: Q3 2026.
Incomplete secure-boot chain	Medium	The cryptographic secure-boot verification chain is not fully closed. Target: Q1 2027.
OpenSSL 1.1.1w end-of-life	Observation	Migration to the OpenSSL 3.x line is recommended.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.3.3. Decision and remediation

Outcome: Compliant path with three remediable findings.

The remediation actions are:

- Encrypt SD-card and configuration data at rest.
- Minimise default-enabled network services.
- Complete the cryptographic secure-boot chain.
- Migrate away from OpenSSL 1.1.1w to a supported branch.

6.3.4. Key takeaway and OSCRAT support

IPTCAMA04FC shows that a wide protocol surface does not by itself prevent a green outcome when documentation and procedures are complete. It is the ideal case for teaching evidence-to-control traceability on a complex product.

Evidence-to-control traceability on a wide protocol surface is exactly what the assessment structure provides. Every requirement carries its CRA reference, and individual questions can require an uploaded file as evidence, so a device with more than thirty protocols is answered against regulatory anchors rather than general assurances, with the Technical Documentation Checklist deep-linking the CRA annexes on EUR-Lex for each of its forty-one entries. The three medium findings become tasks whose due dates match the stated remediation quarters, and ISO-mapped cybersecurity controls can be attached to each task so the fix is tied to the control it satisfies, with its own audit trail. The end-of-life OpenSSL observation comes out of the SBOM scan itself, which shows the component, the version in use and the fixed-in version together, and the generated Conformity Assessment Report reproduces the whole requirement-by-requirement picture for an auditor.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.4 ZUC — Zucchetti All-in-One POS for Retail

A strong commercial platform with bounded clean-up.

Lane	Minor remediation
Manufacturer	Zucchetti S.p.A. (EU rep: Startdust Fine Edition Ltd., Sofia)
Assessed version	1.0.0 (clean-up planned for v1.1.0)
CRA classification	Standard PDE (Other) — not Annex III/IV
Conformity route	Module A — Internal Production Control (self-assessment)
OpenSCAP baseline	78/100 (9 of 12 rules pass)
Product requirements	13/14 (1 partial)
Manufacturer procedures	8/8
Technical documentation	38/41 (92.7%)
Outcome	Substantially compliant; v1.1.0 clean-up planned
Reference	DoC issuable

6.4.1. The story

The Zucchetti All-in-One POS runs Windows 10 IoT Enterprise LTSC 2021 with the TCPOS Retail Suite, a SQLite database, BitLocker full-disk encryption, Secure Boot, and a Wazuh-based monitoring agent branded as SecureMonitor. It is a mature commercial product that already implements most CRA expectations out of the box, which is why thirteen of fourteen product questions and all eight procedure questions pass and the technical file is ninety-three per cent complete.

The three open items are clearly bounded: application data in SQLite is stored in plaintext, there is no USB device allow-listing policy, and the management interface lacks a security.txt contact file. None of these is a design flaw; each has a straightforward route to a cleaner v1.1.0 state.

6.4.2. Findings in context

Finding	Severity	Notes
Plaintext SQLite application storage	Medium	Application data is stored unencrypted at the database layer despite full-disk encryption being enabled.
No USB device allow-list	Medium	The terminal accepts arbitrary USB devices; an allow-list would reduce the physical attack surface of a retail device.
Missing security.txt	Low	The device-management interface does not publish a security.txt contact point.

6.4.3. Decision and remediation

Outcome: Substantially compliant; v1.1.0 clean-up planned.

The remediation actions are:

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- Move SQLite storage to SQLCipher or an equivalent encrypted store.
- Add USB device allow-listing.
- Publish security.txt on the management interface.

6.4.4. Key takeaway and OSCRAT support

ZUC teaches the green-to-amber transition: a near-complete package whose residual items are scheduled rather than blocking, and where conformity is retained while remediation proceeds.

OSCRAT is built for exactly this half-way state. A requirement can be recorded as Partially compliant rather than forced into a pass or a fail, so the single partial product requirement and the three open technical-documentation items are stated honestly and still counted in the result. Each open item becomes a prefilled task with a default thirty-day due date, and that work can be grouped against a v1.1.0 version created in draft while v1.0.0 stays in supported status with a valid declaration behind it. The generated Conformity Assessment Report records which requirement is partial, what was answered and what evidence was attached, so the internal team, the EU representative and a market surveillance authority all read the same picture, and the audit log shows when each status changed and who changed it.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.5 FCR — FCR PRO-2000 Fiscal Cash Register

A minimal-attack-surface embedded device done right.

Lane	Minor remediation
Manufacturer	Stardust Fine Edition (assessor: Yasen Tanev, AI2 Institute)
Assessed version	1.0.0 (remediate in v1.0.1)
CRA classification	Standard PDE (Other) — not Annex III/IV
Conformity route	Module A — Internal Production Control (Article 32(3), Annex VIII)
OpenSCAP baseline	75/100
Product requirements	48/49 fully compliant (1 partial)
Manufacturer procedures	included in 48/49
Technical documentation	41/41
Outcome	Substantially compliant (98%); v1.0.1 closes the gap
Reference	CAR-FCR-2026-001

6.5.1. The story

The FCR PRO-2000 is a retail fiscal cash register built on FreeRTOS with a deliberately minimal attack surface and segmented fiscal and management interfaces. The internal conformity assessment, performed under Article 32(3) using Module A, evaluated forty-nine requirements across product compliance, procedures and the forty-one-item Annex VII checklist, and reported a ninety-eight per cent conformity rate.

Forty-eight of forty-nine requirements were fully compliant and one was partial. The partial finding bundles two concrete technical items for the v1.0.1 release: default passwords are not forced to change at first boot, and data at rest is encrypted with AES-128 rather than AES-256. Both are scheduled and neither reflects a fundamental design deficiency. The package usefully exercises mixed artefact formats — PDF, DOCX, XML and TXT — which is why it is a good case for testing parser hygiene at intake.

6.5.2. Findings in context

Finding	Severity	Notes
Default passwords not forced at first boot	Medium	First-boot password change is not mandatory, leaving a window of default credentials.
Data-at-rest encryption at AES-128	Low/Medium	Stored data uses AES-128 rather than the stronger AES-256.

6.5.3. Decision and remediation

Outcome: Substantially compliant (98%); v1.0.1 closes the gap.

The remediation actions are:

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- Enforce a mandatory first-boot password change.
- Upgrade data-at-rest encryption from AES-128 to AES-256.

6.5.4. Key takeaway and OSCRAT support

FCR shows that a small, well-segmented embedded device can reach near-complete conformity, and that bundling two technical fixes under a single partial finding is an acceptable, transparent way to schedule remediation.

The practical support here is intake and evidence hygiene. Mixed artefacts in PDF, DOCX, XML and TXT are handled by the unified attachment system with type and size validation, while SBOM files follow a dedicated import path so the scanning pipeline is not disturbed by them. The single partial finding is entered once, with both technical items described and their evidence attached, and the follow-up work sits on a task pointed at v1.0.1 with an owner and a due date. Every status change is written to the audit log inside the same transaction as the change itself, with the previous value next to the new one, so the ninety-eight per cent result can be reconstructed months later. The Conformity Assessment Report is generated from the completed version assessment and is the prerequisite that the Declaration of Conformity wizard checks before it will run.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.6 LAR — LogiBot Autonomous Mobile Robot AMR-500

When a cyberattack becomes a physical-safety event.

Lane	Minor remediation / dual-regulation edge case
Manufacturer	LogiBot Robotics B.V. (Amsterdam, Netherlands)
Assessed version	1.0.0
CRA classification	Standard PDE (Other); also references Machinery Directive 2006/42/EC and RED 2014/53/EU
Conformity route	Article 32 self-assessment (Module A intent)
OpenSCAP baseline	88.1/100
Product requirements	57/63 compliant; 6 partial; 0 non-compliant
Manufacturer procedures	covered within 63 tracked items
Technical documentation	Annex VII set complete
Outcome	DoC issued (~92% compliant)
Reference	DoC issued 2026-06-04

6.6.1. The story

The LogiBot AMR-500 is a five-hundred-kilogram autonomous mobile robot running ROS 2, with behavioural anomaly detection and safety-and-cybersecurity co-design. It is the portfolio's clearest dual-regulation case: it must satisfy the Machinery Directive for physical safety and the Cyber Resilience Act for cybersecurity at the same time. That convergence changes the threat model fundamentally — a cyberattack on a smart television is a privacy problem, while a cyberattack on a heavy robot moving beside human workers can be a physical-safety incident.

LogiBot engineered for that reality. A hardware emergency-stop that software cannot override bounds the worst case by physics rather than code; an on-board machine-learning model watches navigation commands for replay-like flooding and path deviations; every robot carries a unique X.509 certificate so a compromised unit can be revoked and isolated within an hour; and the robot can run air-gapped on cryptographically signed mission plans.

The package is notable for its honesty. The OpenSCAP scan produced two failures, the most interesting being a ROS 2 DDS discovery misconfiguration risk. DDS participant discovery is multicast-based and, if SROS2 enforcement were accidentally disabled, would provide no authentication for joining the robot's communication graph. LogiBot deploys SROS2 with mandatory enforcement, but rather than paper over the residual configuration risk it documents it and plans a v1.1.0 watchdog that continuously verifies enforcement and suspends the mission if it is disabled.

6.6.2. Findings in context

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Finding	Severity	Notes
CVE-2023-7248 (Open3D PCD parser, CVSS 5.5)	Low in context	The vulnerable parser is only reached when loading signed, pre-commissioned map files via the authenticated maintenance port after RSA-4096 signature verification; live LiDAR does not exercise it. Fix planned with Open3D 0.18.x in Q3 2026.
ROS 2 DDS / SROS2 discovery pattern	Medium (configuration-dependent)	Mitigated operationally by mandatory SROS2 enforcement; a watchdog is planned for v1.1.0.

6.6.3. Decision and remediation

Outcome: DoC issued (~92% compliant).

The remediation actions are:

- Upgrade Open3D when 0.18.x is available.
- Harden the DDS watchdog and discovery controls (v1.1.0).
- Continue certificate rotation and quarterly scans.

6.6.4. Key takeaway and OSCRAT support

LAR teaches that operational context can legitimately downgrade a CVSS base score, and that the right CRA posture for safety-critical robotics is transparent documentation of residual risk with a concrete engineering fix — not a checkbox that hides findings.

Operational context is not a footnote in OSCRAT, it is a record. The risk assessment task type takes the asset, the threat, the affected security categories, the likelihood and the impact, computes exposure from the risk matrix, and then, in a second stage that unlocks only once the first is saved, records the treatment decision, the mitigation measures, the residual exposure and the responsible party. That is where a CVSS 5.5 base score is documented as low in this deployment, with the reasoning visible rather than the score quietly rewritten. The Open3D upgrade and the planned SROS2 enforcement watchdog are tasks against v1.1.0, certificate rotation and quarterly scanning sit in the same task list with recurring due dates, and the safety and cybersecurity co-design narrative that the Machinery Directive interface depends on lives in the documentation module as a versioned document linked to the tasks that implement it.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.7ANS — AgroNode Solar Pro Agricultural IoT Hub

What does 'without undue delay' mean over a 0.3 kbps radio link?

Lane	Conditional / lifecycle
Manufacturer	AgroNode Technologies ApS (Aarhus, Denmark); EU rep Startdust Fine Edition Ltd.
Assessed version	1.0.0 (support until 2036-12-31)
CRA classification	Standard PDE (Other)
Conformity route	Module A — Internal Production Control
OpenSCAP baseline	71/100
Product requirements	10/14 (3 partial, 1 documented long-lifecycle exception)
Manufacturer procedures	8/8
Technical documentation	33/41
Outcome	DoC issued with explicit long-lifecycle / constrained-update narrative
Reference	DoC issued

6.7.1. The story

A solar-powered AgroNode sensor can sit in a Danish vineyard for a decade with no human ever touching it. Its only update channel is LoRaWAN, a radio protocol with practical bandwidth of roughly 0.3 to 5 kbps and a one per cent EU duty-cycle limit, so a hundred-kilobyte firmware image can take two to six hours to deliver and a failed update could brick the device. Article 13 of the CRA requires security updates without undue delay; this product forces a precise answer to what that phrase means when the update channel is constrained by EU radio regulation itself.

AgroNode's answer is a structured exception framework: modular delta firmware targeting under thirty-two kilobytes per update, a three-stage rollout from one to ten to one hundred per cent of the fleet, rollback capability, and a binding ten-year Long-Lifecycle Security Commitment running to the end of 2036. An ATECC608B hardware secure element keeps the device identity key non-extractable even under physical attack. The known LoRaWAN replay weakness CVE-2022-39182 affects all LoRaWAN 1.0.x devices and cannot be instantly patched across a field of millions of sensors, so the documented exception is the responsible engineering position rather than an evasion.

6.7.2. Findings in context

Finding	Severity	Notes
CVE-2022-39182 (LoRaWAN 1.0.x replay pattern)	Medium (lifecycle-constrained)	Relevant to LoRaWAN 1.0.4; mitigated by documented constrained-update handling and planned migration to LoRaWAN 1.1.
Three partial product-security items	Mixed	Bounded gaps handled through the documented long-lifecycle exception narrative under Article 13.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.7.3. Decision and remediation

Outcome: DoC issued with explicit long-lifecycle / constrained-update narrative.

The remediation actions are:

- Upgrade the stack to LoRaWAN 1.1.
- Coordinate the LoRaWAN Network Server upgrade.
- Maintain the staged FUOTA rollout and documented Article 13 exception handling.

6.7.4. Key takeaway and OSCRAT support

ANS sets a precedent for interpreting 'without undue delay' for constrained IoT. It teaches that a credible, documented constrained-update plan and a long-lifecycle commitment can support a declaration of conformity even where instant patching is physically impossible.

A constrained-update plan only counts if it is written down and traceable, which is what OSCRAT stores. The version record carries the support end date, so the ten-year commitment running to the end of 2036 becomes part of the product data and of organisation-level reporting rather than a promise in a brochure. The LoRaWAN finding is tracked as a vulnerability moving through the CRA handling workflow, from pending and preparation through verification and remediation development to release and post-release, with the affected member states recorded on the finding itself. The Long-Lifecycle Security Commitment and the Article 13 exception narrative are versioned documents in the documentation module, publishable on a shareable public route and linked both ways to the tasks that implement the staged FUOTA rollout, and the three partial requirements are recorded as Partially compliant with that narrative attached as evidence rather than left unexplained.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.8 EVC — ChargePoint Smart AC Wallbox 7kW

A critical bug, handled the way the CRA intends.

Lane	Conditional
Manufacturer	ChargePoint Europe GmbH
Assessed version	1.2.1 (line); v1.2.0 units must update
CRA classification	Standard PDE (Other) — package uses legacy article references
Conformity route	Self-assessment / Module A intent
OpenSCAP baseline	72/100
Product requirements	11 compliant / 2 partial / 1 non-compliant
Manufacturer procedures	8/8
Technical documentation	36/41
Outcome	Conditionally conformant — DoC issuable with conditions
Reference	CP-SEC-2026-0042 (vulnerability ID)

6.8.1. The story

The ChargePoint Smart AC Wallbox is an EV charging station on an embedded Linux stack with an OCPP 2.0.1 communication layer, a web management portal and signed over-the-air updates. In early 2026 a security researcher reported a SQL-injection authentication bypass in the portal's /api/v1/auth/login endpoint: an unauthenticated attacker could use the classic admin'-- payload to gain full administrative access — stopping charging sessions, exfiltrating charge history, reconfiguring OCPP settings or bricking the device. The flaw scored CVSS 9.4.

The value of this case is the response. ChargePoint's PSIRT acknowledged the report within three days, confirmed the root cause as an unsanitised SQLite query in the authentication module of fw-core 1.2.0 within two weeks, developed and validated a parameterised-query patch by day twenty-one, and released v1.2.1 — adding OCPP token-entropy and rate-limiting fixes — with coordinated CVE publication by day thirty-eight. By day fifty-eight, sixty per cent of the fleet had taken the OTA update and forty per cent remained on v1.2.0. Under the CRA this is a pass with conditions: the patch exists, the product can be made conformant, the declaration is issued for the v1.2.x line with an explicit instruction that v1.2.0 devices must update and that no new units ship on the vulnerable build.

6.8.2. Findings in context

Finding	Severity	Notes
CP-SEC-2026-0042 — SQL injection auth bypass (CVSS 9.4)	Critical (patched)	Fixed in v1.2.1 via parameterised queries and input sanitisation; conditional on fleet adoption.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Finding	Severity	Notes
Weak OCPP token entropy	Medium	Addressed in v1.2.1.
Missing rate-limiting controls	Medium	Added in v1.2.1.

6.8.3. Decision and remediation

Outcome: Conditionally conformant — DoC issuable with conditions.

The remediation actions are:

- Complete fleet patching to v1.2.1.
- Publish a coordinated-vulnerability-disclosure page.
- Add a security.txt contact file.
- Confirm enforcement of OCPP SecurityProfile 2.

6.8.4. Key takeaway and OSCRAT support

EVC is the model for amber decisions: a serious but fixable flaw, a disciplined disclosure-and-patch timeline, and a declaration issued conditionally on update reach. It also illustrates why legacy legal references in a package must be normalised before locking the route.

For a manufacturer handling a disclosure like this, OSCRAT produces the timeline as a by-product of the work. The vulnerability record holds the reference, the CVSS severity, the advisory identifier, the affected vendor and the affected member states, and it moves through the CRA handling states, so acknowledgement, root-cause confirmation, patch validation and release are dated as they happen instead of being reconstructed afterwards; the remediation plan and the disclosure correspondence attach to the same record. Reporting organisations, meaning the CSIRTs and authorities with their reporting addresses, are assigned to the product in advance, so the notification path already exists when the clock starts. Versions carry the conditions: v1.2.1 stays supported while v1.2.0 is moved to deprecated or withdrawn, and the declaration is bound to the version it was issued for. The legacy article references are corrected through the CRA reference held on every requirement, which points at the current articles and annexes before the conformity route is locked.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.9 GSB — GlucoSense BLE Pro Continuous Glucose Monitor

A patch is not a fix if users cannot deploy it.

Lane	Conditional / human-factors
Manufacturer	GlucoSense Medical Devices GmbH (Cologne, Germany)
Assessed version	2.0.1 (v2.1.0 remediation assessed)
CRA classification	Standard PDE (Other); NOT an MDR medical device; recheck Annex III-I item 19
Conformity route	Self-assessment (Article 32(2))
OpenSCAP baseline	65/100
Product requirements	10 compliant / 3 partial / 1 non-compliant
Manufacturer procedures	8/8
Technical documentation	33 compliant / 5 partial / 3 non-compliant
Outcome	DoC supportable for the patched state with annotations
Reference	GSB-CR-001 (BSI coordination BSI-2024-0451)

6.9.1. The story

The GlucoSense BLE Pro is a wearable glucose-trend monitor for wellness use — explicitly not a certified medical device under the EU Medical Device Regulation — using Bluetooth Low Energy 5.2 exclusively and delivering updates through a companion smartphone application. Its primary issue is CVE-2020-15802, the BLE 'Just Works' man-in-the-middle exposure present in firmware v2.0.1 and mitigated in v2.1.0 by Numeric Comparison pairing; secondary application, database and advertisement issues are already patched.

The interesting CRA lesson is human-factors. The fix exists, but the target population skews older and update adoption through a phone app is not guaranteed. GSB therefore demonstrates that update availability is not the same as update reach: a declaration of conformity is supportable for the patched state only with an explicit annotation of the patch-adoption gap and the absence of automatic updates, plus a commitment to deliver auto-update in v2.2.0 and to continue elderly-user adoption support and healthcare-channel outreach. The package also flags a classification question: under the final Annex III Class I item 19 for personal wearables with a health-monitoring purpose, the category fit should be re-examined by counsel.

6.9.2. Findings in context

Finding	Severity	Notes
CVE-2020-15802 — BLE 'Just Works' MITM	High (patched in v2.1.0)	Mitigated by Numeric Comparison pairing; deployed devices must move to v2.1.0+.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Finding	Severity	Notes
Patch-adoption / no auto-update	Medium (human-factors)	Availability does not equal reach; auto-update deferred to v2.2.0.
Three partial / non-compliant technical-doc items	Mixed	Annotated in the DoC for the patched state.

6.9.3. Decision and remediation

Outcome: DoC supportable for the patched state with annotations.

The remediation actions are:

- Push all deployed devices to v2.1.0 or later.
- Deliver automatic updates in v2.2.0.
- Continue elderly-user adoption support and healthcare-channel outreach.
- Re-check classification against Annex III Class I item 19 with counsel.

6.9.4. Key takeaway and OSCRAT support

GSB teaches that update adoption is itself a cybersecurity control. In amber cases OSCRAT carries the update-delivery plan and the adoption gap in the assessment record itself, and the applicability check provides the classification gate that borderline wearables need.

OSCRAT does not ingest device telemetry, so fleet adoption figures are entered as assessment evidence rather than measured by the platform; this is one of the clearer extension points the pilot identified. What the platform does carry is the rest of the chain. The patched state is assessed on version 2.1.0, the residual items are recorded as Partially compliant or Not compliant with the adoption gap written into the additional information on the requirement, and those annotations flow into the generated Conformity Assessment Report, so the declaration is never read without them. The automatic-update commitment for v2.2.0 is a task with an owner and a due date, the elderly-user adoption support and the healthcare-channel outreach are tracked in the same list, and the classification question is answered by re-running the public applicability check and comparing the resulting category with the one stored on the product, with the change and its author visible in the audit log.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.10 SBM — Schneider EcoStruxure Edge Box BMS Controller

Securing protocols that predate cybersecurity.

Lane	Conditional / OT-route caution
Manufacturer	Schneider Electric SE (France); EU rep Startdust Fine Edition Ltd.
Assessed version	2.1.0 (note: package folder labelled 1.0.0)
CRA classification	Annex III Class I in OSCRAT (network management / OT-IT bridge) — revalidate Article 32(2)
Conformity route	Module A in package (route to be revalidated)
OpenSCAP baseline	76/100
Product requirements	10 compliant / 3 partial / 1 non-compliant
Manufacturer procedures	7 compliant / 1 partial
Technical documentation	34/41
Outcome	DoC issuable with conditions
Reference	DoC issuable with conditions

6.10.1. The story

The Schneider EcoStruxure Edge Box bridges thirty-year-old building protocols — BACnet/IP, which has no authentication, and KNX, which has no encryption — into modern IP networks and cloud dashboards, alongside Modbus TCP, DALI and M-Bus. You cannot fix those legacy protocols, so the engineering answer is to isolate and compensate: dedicated VLANs, protocol-level firewalls, command allow-lists and one-way data diodes. The CRA challenge is how to express those compensating controls inside a conformity framework designed for secure-by-default systems.

SBOM analysis surfaced two supply-chain currency issues — OpenSSL 1.1.1w, which reached end of life in September 2023, and Wazuh 4.6.0 with a low-severity log-injection CVE — both scheduled for v2.1.1. The package is also the portfolio's ingestion caveat: its stated OpenSCAP score is usable from the summary, but the raw scan XML is malformed and should be repaired or quarantined before automated parsing. Two further normalisation notes apply: the assessed product is version 2.1.0 even though the folder is labelled 1.0.0, and the Annex III Class I classification, while defensible for a network-management device, should be revalidated against Article 32(2) route discipline.

6.10.2. Findings in context

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Finding	Severity	Notes
OpenSSL 1.1.1w end-of-life	Medium	Upgrade scheduled for v2.1.1.
Wazuh 4.6.0 log-injection CVE	Low	Upgrade scheduled for v2.1.1.
BACnet security limitations / default SNMP strings	Medium (OT)	Compensated by VLAN isolation, firewalls, allow-lists and diodes; defaults to be hardened.
Self-signed default TLS certificates; no automatic rotation	Medium	Improve default enrolment and automate certificate rotation.
Malformed OpenSCAP XML	Ingestion	Quarantine and use the stated score only until the file is repaired.

6.10.3. Decision and remediation

Outcome: DoC issuable with conditions.

The remediation actions are:

- Upgrade OpenSSL and Wazuh in v2.1.1.
- Harden SNMP defaults.
- Improve default certificate enrolment and automate rotation.
- Formalise the missing support and documentation elements.
- Repair the malformed scan XML before automated ingestion.

6.10.4. Key takeaway and OSCRAT support

SBM teaches three things at once: how to document compensating controls for legacy OT, how OSCRAT stops malformed evidence at intake instead of scoring it, and why a borderline Annex III classification needs a legal-validation gate before external reliance.

Compensating controls need somewhere to live, and in OSCRAT that is the requirement answer together with its evidence. A requirement that legacy BACnet and KNX cannot satisfy directly is recorded as Partially compliant, with the VLAN isolation, protocol firewalls, command allow-lists and data diodes described in the answer and the network design attached as a document, so the control is stated at the point where a regulator will look for it. Intake protects the record: configuration-scan uploads are XML only, the format is detected from the file header and only ARF 1.1, XCCDF 1.2 and OVAL 5.x are accepted, so a malformed artefact fails at the door instead of becoming a score nobody can trace back. The OpenSSL and Wazuh currency issues arrive from the SBOM scan with their fixed-in versions, and because the CRA classification and the conformity procedure are explicit fields on the product, revalidating a borderline Annex III Class I route is a recorded and audit-logged decision rather than an assumption.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.11 IFG — InduFlow Industrial IoT Gateway GW-200

A hard-coded root backdoor and twenty-three known CVEs.

Lane	Surveillance / import block
Manufacturer	Shenzhen InduFlow Technology Co., Ltd. (non-responsive)
Assessed version	1.0.0 (pre-import due diligence)
CRA classification	Annex III Class I in OSCRAT (recheck category fit)
Conformity route	No valid route completed
OpenSCAP baseline	22/100
Product requirements	0/14
Manufacturer procedures	0/8
Technical documentation	3/41 (7.3%)
Outcome	No DoC possible — import block recommended
Reference	CVE-2024-INDUFLOW-001 (custom ref, CVSS 10.0)

6.11.1. The story

The InduFlow GW-200 was sourced for pre-import due diligence before deployment in EU manufacturing facilities. A Grype scan and SBOM analysis uncovered a hard-coded SSH root backdoor — the account induflow_support with password Indu@2022! grants root on port 22 of any device — tracked as a custom reference with a CVSS of 10.0. The manufacturer in Shenzhen did not respond to responsible disclosure within thirty days.

Beyond the backdoor, the firmware is built on multiple end-of-life components: OpenSSH 7.4p1 from 2017, OpenSSL 1.0.2k from 2016 and PHP 7.2.34, which reached end of life in 2020, contributing to twenty-three known CVEs including four rated critical — OpenSSH CVE-2023-38408, PHP CVE-2022-31625 and BusyBox CVE-2022-28391 each at 9.8, with OpenSSL, nginx and Mosquitto high-severity issues alongside. Product compliance is zero of fourteen, procedures zero of eight and technical documentation three of forty-one. The scenario mirrors the 2021 Hikvision CVE-2021-36260 backdoor that affected more than eighty thousand EU-deployed cameras and led to import restrictions and mandatory update campaigns. No declaration of conformity is possible, and the correct output is a surveillance and import-block dossier.

6.11.2. Findings in context

Finding	Severity	Notes
CVE-2024-INDUFLOW-001 — hard-coded SSH root backdoor (CVSS 10.0)	Critical	induflow_support / Indu@2022! grants unauthenticated root on port 22.
Multiple EOL components	Critical/High	OpenSSH 7.4p1, OpenSSL 1.0.2k, PHP 7.2.34 — 23 known CVEs, 4 critical.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Finding	Severity	Notes
No manufacturer security process	Blocking	No CVD, no PSIRT, no SBOM, no update infrastructure; non-responsive vendor.

6.11.3. Decision and remediation

Outcome: No DoC possible — import block recommended.

The remediation actions are:

- Remove the backdoor and all default credentials; disable Telnet.
- Replace EOL components; implement signed OTA over HTTPS; enable full-disk encryption; add logging.
- Publish a CVD policy and stand up a PSIRT; generate a manufacturer SBOM.
- Prepare the full technical documentation and re-audit before any EU placement.

6.11.4. Key takeaway and OSCRAT support

IFG is the first red-path teaching case: it shows the no-DoC state, how third-party and researcher evidence is carried as first-class evidence in OSCRAT, and how an import-block recommendation is assembled when the manufacturer will not engage.

An importer or distributor doing pre-import due diligence is a first-class role here: OSCRAT ships separate questionnaires for importers, distributors and authorised representatives, so the assessment asks what the CRA actually asks of that role instead of a manufacturer checklist. The product can be registered and examined without any cooperation from the vendor, because an SBOM can be imported or generated and scanned with Grype, and the twenty-three findings come back traced to OpenSSH 7.4p1, OpenSSL 1.0.2k and PHP 7.2.34 with severities and fixed-in versions attached. The hard-coded backdoor is entered manually with its custom reference, its CVSS score and its date of discovery, and the researcher evidence and the failed disclosure correspondence attach to that record. With zero of fourteen product requirements and three of forty-one documentation items, no Conformity Assessment Report can be generated and the Declaration of Conformity wizard stays locked, which is the correct outcome rather than an error state. What can be exported instead is the assessment, the scan reports and the audit trail, and that is the substance of the import-block dossier.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6.12 VTN — VisionTech 8-Channel Network Video Recorder

A budget NVR shipping an unauthenticated root shell.

Lane	Surveillance / import block & withdrawal
Manufacturer	VisionTech Electronics Ltd. (no EU presence, non-responsive)
Assessed version	1.0.0
CRA classification	Annex III Class I in OSCRAT (category fit arguable; surveillance path correct regardless)
Conformity route	No valid route completed
OpenSCAP baseline	18.18/100 (lowest in portfolio)
Product requirements	0/14
Manufacturer procedures	0/8
Technical documentation	5/41
Outcome	Import block and market-withdrawal recommendation — no valid DoC
Reference	OSCRAT-2024-VTN-001 (finding VTN-2024-001)

6.12.1. The story

The VisionTech NVR-8CH represents the flood of sub-150-euro white-label network video recorders entering the EU through online marketplaces, achieving their price in part by skipping product security. It runs Android 9 on a Rockchip SoC — an OS already end-of-life before the device reached EU shelves — from a manufacturer with no EU presence, no security contact, no disclosure process and no update infrastructure: precisely the gap the CRA was written to close.

An EU researcher acquired a unit, scanned it, and found TCP port 9527 open with no banner. APK extraction revealed com.visiontech.nvr.debug.DebugApiService and an exec endpoint; a single POST to /api/debug/exec returned root with no authentication, on a device whose quick-start guide instructs users to port-forward it to the internet. Responsible disclosure failed: the security and info mailboxes bounced or went unanswered for forty days. The backdoor, tracked VTN-2024-001 at CVSS 9.8, sits alongside severe SBOM issues across OpenSSL 1.0.2u, FFmpeg, BusyBox, SQLite and an end-of-life kernel. Product compliance is zero of fourteen, procedures zero of eight, documentation five of forty-one and the OpenSCAP baseline 18.18 — the lowest in the portfolio. The package yields an import-block and market-withdrawal recommendation with no valid declaration of conformity.

6.12.2. Findings in context

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Finding	Severity	Notes
VTN-2024-001 — unauthenticated root command execution on TCP/9527 (CVSS 9.8)	Critical	Undocumented Debug API exposes a root shell from the network with no authentication.
Severe SBOM issues	Critical/High	OpenSSL 1.0.2u, FFmpeg, BusyBox, SQLite and an EOL kernel.
No manufacturer presence or process	Blocking	No EU authorised representative, no CVD, no update path; non-responsive vendor.

6.12.3. Decision and remediation

Outcome: Import block and market-withdrawal recommendation — no valid DoC.

The remediation actions are:

- Remove the Debug API / port 9527 service entirely.
- Replace OpenSSL 1.0.2u and rebuild OTA with code signing; enforce first-boot password change.
- Disclose or remove undocumented APKs; designate an EU authorised representative.
- Produce full technical documentation and a secure-development process before any re-entry.

6.12.4. Key takeaway and OSCRAT support

VTN is the portfolio's worst case and the clearest demonstration of CRA market surveillance: it exercises the no-DoC state, the import block and the withdrawal recommendation, and shows how OSCRAT supports authorities under Articles 54 and 55.

The lifecycle states are the point in this case. A version can be moved to withdrawn, the organisation dashboard counts products carrying a withdrawn version, and the incident record captures cross-border impact and a suspected unlawful act with forensic evidence attached, which is what a surveillance file needs. Reporting organisations and their contact addresses are held against the product, so the authority a notification goes to is already identified. An external reviewer can be added to the organisation as an auditor, which grants read access to the evidence without any ability to change it, and every file download, status change and record edit is written to the audit log with the actor, the timestamp and the previous value. For a distributor or importer the more useful support comes earlier: the same SBOM scan and role-based assessment, run before the purchase order, would have surfaced the open debug service, the end-of-life components and the absent manufacturer process at the point where walking away was still cheap.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

7. The end-to-end pilot workflow

A good CRA assessment is a controlled evidence-and-decision exercise, not a generic file upload. The point is not merely to ingest files; it is to demonstrate that evidence can be converted into a legally intelligible outcome. This section gives the repeatable workflow you can run on your own product.

7.1 Preconditions for every run

1. Package integrity confirmed.
2. Product/package identifier separated from the firmware/version identifier.
3. Legal-reference normalisation switched on.
4. Route-decision rules set to the final CRA text, not older drafts.
5. Outcome vocabulary fixed in advance: DoC issued, DoC issuable, conditional/annotated DoC, remediation required, no DoC, import block / surveillance package.

7.2 Roles and minimum inputs

Role	Responsibility	Minimum input
Product owner	Supplies package; confirms intended use, support period, release state	Package and named contact
Security assessor	Validates SBOM, scans, exploitability and remediation evidence	SBOM, scan, vulnerability notes
Compliance lead	Normalises references; validates classification, route, DoC and doc anchors	Profile, applicability file, report, DoC
Documentation lead	Verifies completeness, traceability and consistency	Annex-VII-equivalent set
Legal / authorised rep	Confirms internal-only, issuable, conditional or blocked	Outcome summary and rationale
Importer / MSA observer	Participates in red-path and surveillance scenarios	Origin, supply-chain facts, corrective status

Table 6 — Roles and minimum inputs for a CRA assessment.

7.3Step-by-step operating

Step	What you do	Validation checks	Output
Intake & completeness	Upload files; assign code, version, manufacturer, intended use	File presence, extension profile, duplicate detection, malformed-XML check	Intake pass/fail

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Step	What you do	Validation checks	Output
Classification & routing	Review applicability vs final CRA categories	Standard PDE vs Annex III vs IV; draft-numbering correction; AI-Act interaction	Locked class and route note
SBOM analysis	Import CycloneDX; enumerate components; identify CVEs or gaps	SBOM parses; versions match report; gaps flagged	SBOM dashboard, vuln register
Scan import	Import XCCDF / OpenSCAP baseline	Score parsed; pass/fail consistent; malformed files quarantined	Baseline-security dashboard
Compliance assessment	Link product, procedure and doc evidence to CRA anchors	Annex I, II, VII, V mapping complete	Scorecard and gap register
Decision support	Compare route, maturity, exploitation, feasibility, timing	Clear green/amber/red; no unresolved route mismatch	Outcome recommendation
DoC generation	For green/amber, produce DoC draft or validated statement	Annex V fields complete; support period; signatory	DoC-ready or DoC-with-conditions
Market surveillance	For red, prepare authority-facing case pack	Significant-risk narrative; corrective record; withdrawal rationale	Surveillance / import-block dossier

Table 7 — The eight-step OSCRAT operating report.

7.4 Which products demonstrate which sub-use-case

Sub-use-case	Best products	What to demonstrate
Import & package normalisation	FCR, GSB, SBM	Mixed formats, version mismatches, parser hygiene
CRA classification	ANS, GSB, SBM, VTN	Straightforward vs borderline category calls
SBOM analysis	PEX, IFG, VTN	Supply-chain visibility, CVE context, exploitability
Scan import	SCBL, ZUC, LAR	Baseline scoring linked to practical remediation
Compliance dashboard	IPTCAMA04FC, PEX, ZUC	Evidence-to-control traceability and scorecards
Decision support	ANS, EVC, GSB, SBM	‘Compliant’ vs ‘conditional’ vs ‘annotated’
DoC generation	PEX, SCBL, LAR, ANS	Green-path and amber-path declaration logic
Market surveillance	IFG, VTN	No-DoC state, import block, withdrawal, authority pack

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Table 8 — Sub-use-cases mapped to the best demonstrator products.

7.5 Suggested demo sequencing and schedule

Lane	Products	Why here	Stakeholder learning
Green path first	PEX, SCBL, IPTCAMA04FC	Cleanest evidence, easiest Module-A narrative	Understand the happy path first
Minor remediation	ZUC, FCR, LAR	Strong packages still contain bounded findings	How to treat fixable residual issues
Conditional / lifecycle	ANS, EVC, GSB, SBM	Exception handling, patch rollout, human factors, legacy OT	The amber path and deadline governance
Surveillance last	IFG, VTN	Hard stops shown after platform logic is clear	How OSCRAT supports authorities and import control

Table 9 — Recommended demonstration lanes

.

Session	Products	Objective	Decision target
A	PEX and SCBL	Green-path baseline	DoC-ready self-assessment
B	IPTCAMA04FC and ZUC	Green-to-amber transition	Minor remediation, retained conformity
C	FCR and LAR	Mixed-format ingest, robotics edge case	Substantial compliance with action list
D	ANS and EVC	Conditional reasoning, constrained update	Conditional / annotated output
E	GSB and SBM	Human-factor update gap, OT-route caution	Conditional output plus legal review
F	IFG and VTN	Surveillance, no-DoC, import-block logic	Authority-ready dossier

Table 10 — A six-session pilot schedule.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

8. Lessons learned and recommendations

Four lessons run through the whole portfolio. First, normalisation is not optional: without it, a platform mixes final-law anchors with draft-era references and route decisions become unreliable. Second, process maturity can legitimately outweigh the existence of bounded vulnerabilities — but only where the package proves a credible remediation path, a support-period rationale and secure update delivery. Third, human update adoption is itself a cybersecurity control: GSB shows that a patch is not enough if the target population cannot realistically deploy it. Fourth, market-surveillance cases need first-class support for third-party evidence, because IFG and VTN are driven by researcher or pre-import findings rather than a cooperative manufacturer disclosure record.

8.1 Lessons and mitigations

Lesson	Example products	Practical mitigation
Legacy legal references cause route drift	EVC, GSB, LAR, IPTCAMA04FC, SBM	Add a CRA canonical-reference layer before route selection
Borderline Annex III classification needs legal review	GSB, IFG, IPTCAMA04FC, SBM, VTN	Mandatory legal-validation gate for non-obvious categories
Mixed artefact formats complicate ingest	FCR, GSB, SBM	Standardise the package schema; add parser health checks
Malformed evidence can distort dashboards	SBM	Quarantine malformed XML; use stated score only until repaired
Update availability is not update reach	GSB, ANS, EVC	Track adoption telemetry; require an update-delivery plan
OT and constrained IoT need narrative exceptions	SBM, ANS	Provide compensating-controls and constrained-update templates
Surveillance needs authority-facing outputs	IFG, VTN	Add import-block and withdrawal dossiers tied to Article 54/55

Table 11 — Lessons learned and their practical mitigations.

8.2 Checklist for assessors

Assessor check	What ‘good’ looks like
Canonical legal anchors used	Article 28/Annex V, 31/Annex VII, 32/Annex VIII
Classification tested against final Annex III / IV	Borderline calls escalated, not buried
Package version separated from product version	Folder name cannot override firmware reality
SBOM parseability confirmed	CycloneDX imports cleanly or is quarantined
Scan score and narrative agree	Pass/fail counts, score and remediation text line up
Support period visible	End date and rationale present
CVD / contact / update mechanism visible	Single contact, CVD policy, secure update path

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Assessor check	What 'good' looks like
Outcome traceable	Every decision explainable in one page

Table 12 — Assessor checklist.

8.3 Checklist for manufacturers

Manufacturer check	What to have ready before the pilot
Product description	Intended use, architecture, release version, support end date
CRA applicability note	Why the product is default, important or critical
SBOM	CycloneDX in machine-readable form
Security baseline	XCCDF / OpenSCAP scan with a reproducible score
Risk assessment	Current lifecycle risk assessment and threat model
Vulnerability handling	CVD policy, disclosure contact, triage and SLA
Update evidence	Signed update path, rollback behaviour, user notification
Documentation set	Complete Annex-VII-equivalent package with change control
Outcome narrative	DoC rationale, or a candid no-DoC / remediation path

Table 13 — Manufacturer readiness checklist.

8.4 Open questions and limitations

A short list should be carried into the next iteration. The GSB classification should be reviewed against final Annex III Class I item 19 for non-MDR personal wearables with a health-monitoring purpose. IFG, IPTCAMA04FC, SBM and VTN each carry some category-fit ambiguity against the final Annex III/IV taxonomy and need an explicit legal sign-off before being used as external reference cases. PEX and LAR are strong AI-enabled products, but the archive does not establish whether either should be treated as a high-risk AI system; if that changes, Article 12 alters the conformity story. Finally, several packages carry pre-application dates and should be labelled as simulation, rehearsal or retrospective alignment rather than evidence of live enforcement.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

9. How to start your own CRA preparation

If you have read this far and recognised your own product somewhere in the twelve, the good news is that starting is straightforward. You do not need to solve the whole Regulation at once. You need to assemble evidence in the six-stage structure, run an honest assessment, and decide which colour path you are on. The platform is free and open at oscrat.eu, and the rest of this section is the shortest credible route to a first result.

9.1 A five-step start

6. Write a one-page product description: what it is, who uses it, how long you will support it, and how it receives updates.
7. Answer the CRA applicability questions to fix your category — standard PDE, Annex III important, or Annex IV critical — and escalate any borderline call to counsel.
8. Generate a CycloneDX SBOM and run an OpenSCAP baseline; these two artefacts alone already separate green from red.
9. Complete the compliance assessment against Annex I, Annex II and the forty-one-item Annex VII checklist, linking each control to evidence.
10. Decide the outcome using the fixed vocabulary, and either draft the declaration of conformity or write a candid remediation plan.

Most first-time teams find that the hardest part is not the security work but the discipline of evidence: knowing your supply chain, scanning it, understanding exploitability in context, and writing down why a finding is or is not a real risk. That discipline is exactly what the twelve examples model.

9.2 Where support fits

OSCRAT is open source, so an organisation can adopt it independently and inspect every step of its reasoning. For teams that want a faster or assured start — a borderline classification, a constrained-IoT exception narrative, an OT compensating-controls package, or a surveillance dossier — we offer hands-on support built on exactly the practices in this report. The aim is the same whether you do it alone or with help: a declaration you can defend, or an honest decision not to declare. Sharing experience and building trust is the point.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

10. Conclusion

The twelve use cases are a strong foundation for understanding the CRA in practice. Their value is not that every legal reference is already perfect; it is that, once normalised, they cover almost the entire operating envelope a manufacturer or an authority will meet. A reader who follows the green, amber and red examples in order gains something a statute cannot give on its own: the judgement to look at a real product and know what to do first.

If there is one message to carry away, it is that CRA compliance is an exercise in honesty made operational. The strongest use cases do not hide findings; they document them, quantify the real risk, and commit to a fix on a stated timeline. The weakest are weak not because they have vulnerabilities but because there is no manufacturer, no process and no willingness to engage. Everything between those poles is the work — and the platform, the workflow and these examples exist to make that work repeatable, transparent and shareable.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

11. Annexes

11.1 Annex A — Glossary of key terms

Term	Meaning in this report
CRA	Cyber Resilience Act, Regulation (EU) 2024/2847
PDE	Product with digital elements — the unit the CRA regulates
Standard PDE	Default category; eligible for Module A self-assessment
Annex III / IV	Important / critical product categories with stricter routes
Module A	Internal production control — manufacturer self-assessment
SBOM	Software bill of materials (here, CycloneDX format)
OpenSCAP / XCCDF	Security baseline scan format and its results
CVD	Coordinated vulnerability disclosure policy and contact
DoC	EU declaration of conformity (Article 28 / Annex V)
Technical documentation	The Annex VII evidence set (Article 31)
MSA	Market-surveillance authority (Articles 54–55)
Support period	The time the manufacturer supplies security updates (normally ≥ 5 years)

Table 14 — Glossary of key CRA and OSCRAT terms.

11.2 Annex B — Per-product evidence index

Each package contains the same six-stage evidence set described in Section 2. The table records the assessed manufacturer, the assessed version and the reference identifier for each product, so a reader can trace any decision back to its source package.

Code	Manufacturer	Assessed version	Reference
PEX	Percepta AI Systems S.r.l. (Italy)	1.0.0	DOC-PEX-1.0.0-20260604
SCBL	Startdust Fine Edition Ltd. (Sofia, Bulgaria)	1.0.0	DoC issuable
IPTCAMA04FC	Comelit Group S.p.A. (Rovetta, Italy)	Firmware 5.1.4.1_59514	DoC issuable
ZUC	Zucchetti S.p.A. (EU rep: Startdust Fine Edition Ltd., Sofia)	1.0.0 (clean-up planned for v1.1.0)	DoC issuable
FCR	Stardust Fine Edition (assessor: Yasen Tanev, AI2 Institute)	1.0.0 (remediate in v1.0.1)	CAR-FCR-2026-001
LAR	LogiBot Robotics B.V. (Amsterdam, Netherlands)	1.0.0	DoC issued 2026-06-04
ANS	AgroNode Technologies ApS (Aarhus, Denmark); EU rep Startdust Fine Edition Ltd.	1.0.0 (support until 2036-12-31)	DoC issued

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Code	Manufacturer	Assessed version	Reference
EVC	ChargePoint Europe GmbH	1.2.1 (line); v1.2.0 units must update	CP-SEC-2026-0042 (vulnerability ID)
GSB	GlucoSense Medical Devices GmbH (Cologne, Germany)	2.0.1 (v2.1.0 remediation assessed)	GSB-CR-001 (BSI coordination BSI-2024-0451)
SBM	Schneider Electric SE (France); EU rep Startdust Fine Edition Ltd.	2.1.0 (note: package folder labelled 1.0.0)	DoC issuable with conditions
IFG	Shenzhen InduFlow Technology Co., Ltd. (non-responsive)	1.0.0 (pre-import due diligence)	CVE-2024-INDUFLOW-001 (custom ref, CVSS 10.0)
VTN	VisionTech Electronics Ltd. (no EU presence, non-responsive)	1.0.0	OSCRAT-2024-VTN-001 (finding VTN-2024-001)

Table 15 — Per-product evidence index.

11.3 Annex C — Outcome vocabulary

Fixing the words before the assessment prevents disputes afterwards. The six outcomes used throughout this report are defined below.

Outcome	Meaning
DoC issued	Declaration drawn up; the product is conformant as assessed
DoC issuable	Declaration can be drawn up immediately on the stated evidence
Conditional / annotated DoC	Declaration valid subject to remediation, update reach or an explicit annotation
Remediation required	Bounded fixes scheduled before a clean declaration
No DoC	Declaration not possible in the current state
Import block / surveillance	Authority-facing dossier; block, withdrawal or recall recommended

Table 16 — The six-term outcome vocabulary.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

www.oscrat.eu

https://www.linkedin.com/c