

Meeting EU Cyber Resilience Act requirements with DefectDojo

Regulation (EU) 2024/2847 makes vulnerability handling a legal duty for anyone selling products with digital elements in the EU. Here are the CRA obligations that run through a vulnerability management program, each paired with the DefectDojo capability that answers it.

IN FORCE
Dec 10, 2024
The CRA entered into force, starting the transition clock.

IN EFFECT NOW
Sep 11, 2026
Article 14 reporting applies, including to products already on the market.

FULL APPLICATION
Dec 11, 2027
Annex I requirements, SBOMs, and technical documentation apply.

PENALTIES
€15M or 2.5%
Of worldwide annual turnover, whichever is higher, for the most serious breaches.

☒ **Covered:** DefectDojo does this work

☐ **Supports:** your process, enforced and recorded

Sensei is a DefectDojo Pro capability in beta that requires its own license entitlement.

SECTION 1 · ANNEX I, PART II · APPLIES DEC 11, 2027

Vulnerability handling

CRA REQUIREMENT	HOW DEFECTDOJO CHECKS THE BOX	EDITION
☒ ANNEX I, PART II (1) Identify and document the vulnerabilities and components in your product, including an SBOM of at least top-level dependencies in a machine-readable format.	Import the CycloneDX and SPDX SBOMs your builds already produce, per product or up to 25 files at once, into a dependency inventory that every new advisory is matched against. Findings from 360+ security tools in Community Edition (500+ in Pro), CycloneDX included, land on the same product, deduplicated.	COMMUNITY EDITION PRO
☒ ANNEX I, PART II (2) Address and remediate vulnerabilities without delay, including by providing security updates.	Per-product SLAs put a remediation deadline on every finding, by severity or (in Pro) by risk, and notify owners on breach. Findings push to Jira with bidirectional sync, so closing the ticket closes the finding. Sensei opens pull requests that fix findings in your repositories.	COMMUNITY EDITION PRO SENSEI (BETA)
☒ ANNEX I, PART II (3) Apply effective and regular tests and reviews to the security of the product.	Reimport each recurring scan into the same Test from CI/CD or the API. DefectDojo records what every run created, closed, left untouched, and reactivated, so the record shows whether a fix held from one release to the next.	COMMUNITY EDITION PRO
☒ ANNEX I, PART II (4) Once a security update is available, publicly disclose the fixed vulnerability: what it is, which products it affects, its impact and severity, and how to remediate it.	Write, review, and publish your own security advisories. Publishing requires every reviewer's approval, an approval goes stale if the text changes after it, and each publish is snapshotted exactly as sent. When upstream facts move, such as a CVSS revision or a new KEV listing, the advisory is flagged for revision.	PRO
☐ ANNEX I, PART II (5) Put in place and enforce a policy on coordinated vulnerability disclosure.	You write the policy and DefectDojo enforces its mechanics. An embargo date blocks publication until it passes, preflight blocks publishing while sign-offs or blocking comments are open, and PSIRT cases carry an SLA clock on the triage obligation.	PRO
☐ ANNEX I, PART II (6) Facilitate the sharing of information about potential vulnerabilities, including reports from third parties, and provide a contact address for reporting them.	Bring HackerOne and Bugcrowd reports in as findings, so researcher submissions get the same SLA, triage, and history as scanner output. Pro adds a HackerOne connector that pulls reports over the API. The published contact address remains yours to run.	COMMUNITY EDITION PRO
☐ ANNEX I, PART II (7) AND (8) Distribute security updates securely and without delay, free of charge, with advisory messages that tell users what to do.	Your release pipeline ships the update, and DefectDojo ships the message. Advisory recipients are derived from confirmed matches on your products, publishing can be scheduled, and delivery status reports what was actually sent, including what was not.	PRO

Reporting exploited vulnerabilities and severe incidents

CRA REQUIREMENT	HOW DEFECTDOJO CHECKS THE BOX	EDITION
 ARTICLE 14 (AWARENESS) Know when a vulnerability in your product is being actively exploited. Every reporting clock starts at awareness, not at confirmation.	EPSS and CISA KEV data enrich findings at import and daily after, and a KEV listing raises a finding's Priority and Risk. PSIRT polls advisory feeds from publishers including CISA, NVD, and EUVD, and answers "am I affected?" against your SBOM inventory.	PRO
 ARTICLE 14 (1) AND (2) Actively exploited vulnerability: early warning within 24 hours, notification within 72 hours, final report within 14 days of a corrective or mitigating measure being available.	CRA Article 14 Reporting runs a live countdown for each stage. When an exploited advisory matches a product marked in scope for the CRA, a banner flags the 24-hour deadline, and the moment it appeared is written to the audit trail. The final-report clock arms when you record that a fix is available.	PRO
 ARTICLE 14 (3) AND (4) Severe incident affecting product security: early warning within 24 hours, notification within 72 hours, final report within one month.	Start a severe incident report with no advisory attached. The final-report clock arms once the notification is recorded as submitted. Statutory clocks alert through the same SLA warning and breach notifications your team already receives.	PRO
 ARTICLES 14 AND 16 Submit each stage through ENISA's Single Reporting Platform with the content that stage requires.	Each stage lists the content its submission needs and exports the package as JSON, Markdown, or PDF. A person submits it on the platform and records the reference it returns, and DefectDojo notes the submission on every related finding and engagement. Changing the awareness time requires a written justification.	PRO

SECTION 3 · ANNEX I, PART I AND ARTICLE 13 · APPLIES DEC 11, 2027

Product security and due diligence

CRA REQUIREMENT	HOW DEFECTDOJO CHECKS THE BOX	EDITION
 ANNEX I, PART I (2)(A) Make products available on the market without known exploitable vulnerabilities.	Every CI/CD import lands on the product and engagement it came from, so open findings for a release are one filter away before it ships. In Pro, Priority and Risk weigh severity, business criticality, EPSS, and KEV, so exploitable issues sort to the top of the release review.	COMMUNITY EDITION PRO
 ARTICLE 13 (5) Exercise due diligence when integrating third-party components, including open source components.	Results from the SCA and SBOM tools you already run, such as Dependency-Track and Gripe, arrive as deduplicated findings per product. PSIRT keeps a component inventory where you add a risk rating, an authoritative CPE, and tags, then checks it against each new advisory.	COMMUNITY EDITION PRO
 ARTICLE 13 AND ANNEX VII Assess cybersecurity risk, document the decisions, and keep technical documentation available to market surveillance authorities for at least 10 years.	Risk Acceptances store the justification and supporting files, with an expiration date that returns findings to Active for review. Object History records changes to products, engagements, tests, findings, and Risk Acceptances. Pro adds an instance-wide Audit Log and a history API.	COMMUNITY EDITION PRO

COMMUNITY EDITION

The handling loop, free

Self-hosted under BSD-3. 360+ parsers including CycloneDX, deduplication, per-product SLAs with breach notifications, Risk Acceptances, Jira sync, bug bounty imports, and object history on every finding.

DEFECTDOJO PRO

Exploit-aware, audit-ready

500+ integrations, in the cloud, on-premises, or air-gapped. For the CRA, Pro adds EPSS and KEV enrichment to catch active exploitation (Article 14), risk-based SLAs to remediate without delay (Annex I), and an instance-wide Audit Log for the evidence trail (Article 13).

PSIRT MODULE (BETA)

Built for Article 14

SBOM matching against advisory feeds, your own published advisories, and CRA Article 14 Reporting with statutory clocks. Requires the PSIRT Advisory Engine entitlement; an administrator enables Article 14 Reporting per instance.

ABOUT DEFECTDOJO

DefectDojo is the open source unified vulnerability management platform that remediates at the speed of AI, enabling security teams to focus on fixing the most critical vulnerabilities first. Parse any security finding, aggregate across your stack, prioritize what matters, and report on your security posture and compliance.

BOOK A DEMO

Walk through SBOM matching, risk-based SLAs, and Article 14 reporting with our team.

Book yours at defectdojo.com/book-a-demo

This datasheet maps DefectDojo capabilities to CRA obligations for planning purposes and is not legal advice. DefectDojo tracks deadlines, builds submission packages, and records your team's determinations. It does not submit reports to ENISA's Single Reporting Platform on your behalf, distribute software updates, or decide whether you comply. Confirm your obligations, product classification, and support period with qualified counsel. Beta capabilities may change before general availability.