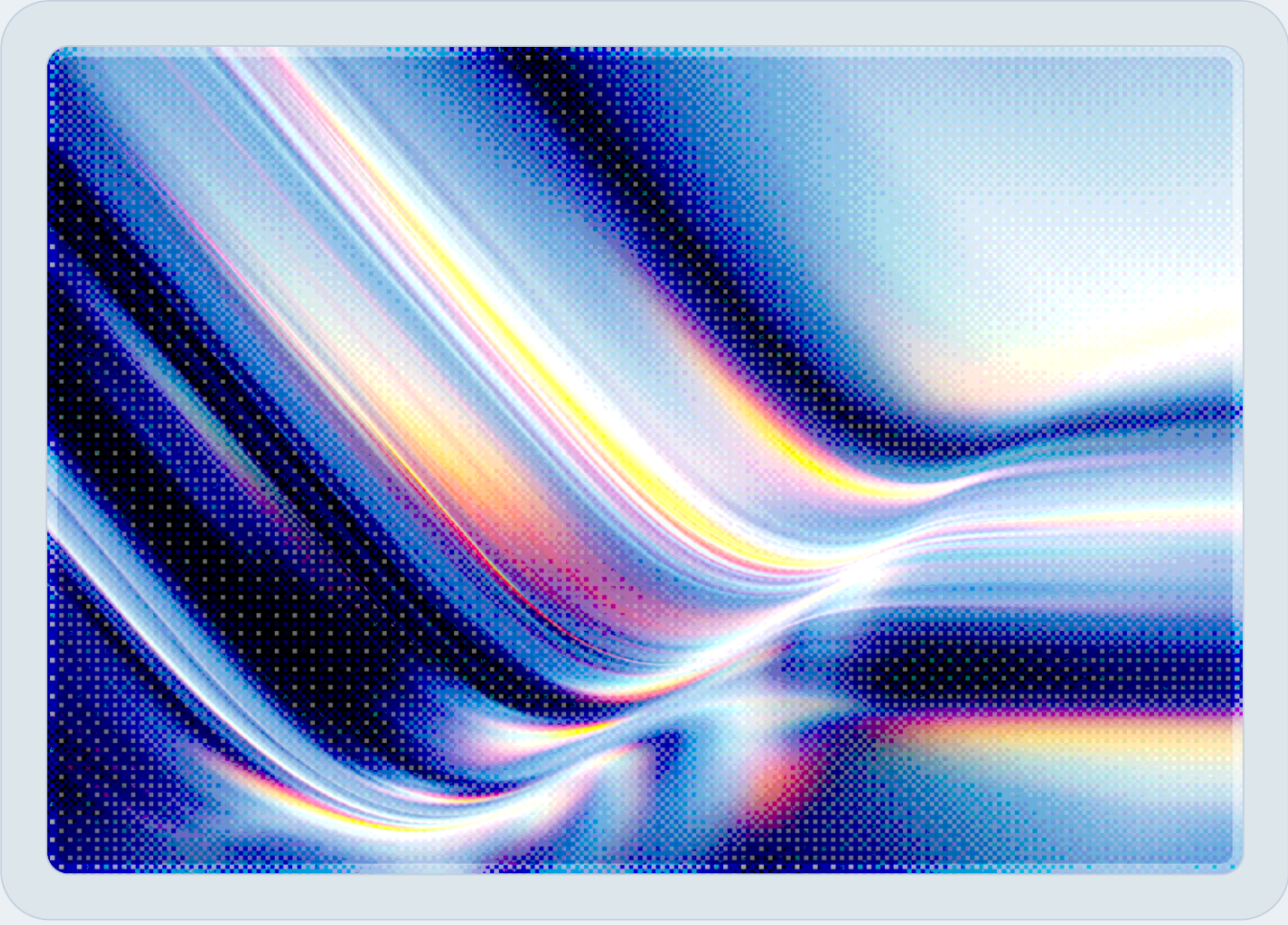
CSAI Foundation | Cloud Security Alliance

ENISA's CRA Reporting Platform: What Security Teams Must Do

2026-09-18

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

The European Union Agency for Cybersecurity (ENISA) switched on the Cyber Resilience Act (CRA) Single Reporting Platform on September 11, 2026, the same day the CRA's reporting obligations became legally binding on manufacturers of products with digital elements sold in the EU [1][2]. Any organization placing such a product on the EU market must now report actively exploited vulnerabilities and severe incidents through a single web portal at portal.cra-srp.enisa.europa.eu, which routes each submission to a designated national Computer Security Incident Response Team (CSIRT) for validation and onward distribution to other affected member states [2][3]. The reporting clock is strict: an early warning is due within 24 hours of a manufacturer becoming aware of an issue, a fuller notification with an initial assessment within 72 hours, and a final report within 14 days of a corrective measure becoming available, or within one month of the 72-hour notification for severe incidents [1][4]. Failure to meet these obligations can trigger administrative fines of up to €15 million or 2.5 percent of an organization's global annual turnover, whichever is higher, although micro- and small enterprises are shielded from penalties tied specifically to the 24-hour deadline [5]. The platform was released only one day ahead of its own legal deadline, having still been described as "not yet operational" as recently as late June 2026, and it launched supporting only manual web-form submissions [4]; ENISA added support for nine EU languages within days of launch, though API access and automated workflows remain unscheduled [6]. CSA's own recent analysis of ENISA's SME maturity survey found that awareness of the CRA already outpaced organizations' practical ability to execute on it, a gap this launch appears unlikely to close and may in fact widen for smaller manufacturers without dedicated compliance staff [7].

Background

The Cyber Resilience Act, formally Regulation (EU) 2024/2847, establishes EU-wide cybersecurity requirements for hardware and software products with digital elements, covering everything from consumer IoT devices to enterprise software components, and it phases in obligations across several dates between its entry into force in December 2024 and full applicability on December 11, 2027 [4][7]. September 11, 2026 marked a major operational milestone in that phase-in: the date on which manufacturers, importers, and distributors became legally required to report actively exploited vulnerabilities in their products and any severe incidents affecting the security of those products, under the reporting obligations set out in the CRA's Article 14 [1][7]. Rather than requiring separate

notifications to each member state where a product circulates, the CRA calls for a single EU-level reporting mechanism, and ENISA was designated to build and operate that mechanism as the Single Reporting Platform, or SRP [2].

The SRP's core design goal is to let a manufacturer report once and have the platform handle downstream coordination. A reporting organization selects a national CSIRT, typically based on the location of its main EU establishment or, for non-EU manufacturers, their EU-based authorized representative, and that CSIRT becomes the coordinator that validates the manufacturer's account and disseminates notifications to other member states' authorities where the affected product is also sold [1] [2]. Access to the platform runs through EU Login with mandatory multi-factor authentication, and each manufacturer designates one primary representative and up to twenty secondary representatives authorized to file reports on the organization's behalf [1]. ENISA's Executive Director framed the platform's purpose directly at launch, noting that vulnerabilities in digital products are frequently exploited by threat actors to compromise critical services, and that a coordinated, EU-wide information-sharing mechanism strengthens the resilience of the Digital Single Market as a whole [2].

The platform's launch followed a compressed timeline. As late as June 29, 2026, industry trackers were reporting that the SRP remained non-operational even though the September reporting deadline was already fixed in law, and manufacturers were advised in the interim to prepare their internal processes independently of the tool's availability rather than wait for it [6]. ENISA published the list of coordinating CSIRTs for all 27 member states on September 4, 2026, and released the platform's address and user documentation on September 10, one day before the obligations took effect [6]. The platform ultimately launched on schedule, but the compressed runway between documentation availability and legal enforceability likely left many manufacturers with little time to test their reporting workflows against the live system before their first reporting clock could start [4][6]. Open-source software stewards are not yet subject to these obligations; their equivalent reporting duties begin on December 11, 2027, alongside the CRA's broader entry into full applicability [1][2].

Security Analysis

Among the most consequential operational details in the SRP's initial release is what it does not yet do. ENISA has confirmed that the platform launched without API functionality, meaning every report, at every stage of the 24-hour, 72-hour, and 14-day cycle, must be entered through a web interface rather than submitted programmatically from a manufacturer's existing incident-response or vulnerability-management tooling [1]. For organizations with multi-step internal escalation processes, this could create a manual bottleneck at a stage where speed matters most: a 24-hour early-warning window leaves comparatively little room to detect an alert, route it to an approver, and manually transcribe technical

detail into a web form before the deadline lapses. ENISA has indicated that automated workflows and API support are planned for future phases, but no committed date has been published, so manufacturers should treat manual entry as the operating reality for the foreseeable near term rather than a temporary inconvenience [1][4].

The platform's reliance on a single designated CSIRT per manufacturer also introduces a structural dependency that security teams should map before they need it under pressure. A report's onward distribution to other member states depends on the coordinating CSIRT correctly identifying every jurisdiction where the affected product is available and forwarding the notification accordingly; a manufacturer that has not accurately registered its product footprint, or that selects the wrong coordinating CSIRT because its EU establishment or authorized representative relationship is ambiguous, risks a report that satisfies the letter of the 24-hour deadline but fails to reach the authorities in a market where the vulnerability is actually being exploited. This is compounded by the account structure itself: with only one primary representative and up to twenty secondary representatives per manufacturer, larger organizations with distributed product-security functions across business units or subsidiaries need to decide in advance who holds reporting authority, since resolving that access-management question during an active 24-hour countdown leaves little margin for error.

The gap between the CRA's legal effective date and the platform's practical readiness is itself a governance signal worth internalizing beyond this single launch. A regulation's obligations became enforceable, complete with fines reaching 2.5 percent of global turnover, before the government-provided tool for meeting them had been available for more than a day of testing [4][5][6]. Manufacturers that assumed the platform would be stable and fully featured well ahead of the deadline, and that deferred building an internal detection-to-notification pipeline until the tool existed, would likely have entered the compliance window with little margin for error. This pattern echoes a broader dynamic documented in CSA's review of ENISA's SME Cyber Resilience Maturity Assessment Model, which found that a large share of European manufacturers, particularly smaller ones, are aware the CRA exists but lack the internal processes, staffing, or resourcing to act on that awareness before deadlines arrive [7]. The SRP's compressed rollout suggests that even well-resourced organizations, and the regulator itself, are operating with less preparation time than the regulation's own calendar implies.

Recommendations

Immediate Actions

Manufacturers of products with digital elements sold in the EU should immediately confirm which national CSIRT they must designate as their coordinator, based on the location of their main EU establishment or their EU-based authorized representative if they are established outside the Union, and register their primary and secondary representatives on the SRP through EU Login without waiting for an active incident to force the issue [1][2]. Security and product teams should walk through a tabletop exercise using the platform's actual web interface now, before a real vulnerability or incident starts the clock, so that the people responsible for filing a report are not encountering the form's fields and required content for the first time under a 24-hour deadline. Organizations should also confirm internally who has authority to determine when a vulnerability is "actively exploited" or an incident is "severe" under the CRA's definitions, since that determination is what starts the reporting clock; ambiguity about who makes that call is a plausible source of missed deadlines in comparable EU incident-reporting regimes such as NIS2, based on the same readiness gaps CSA has documented for CRA reporting [7].

Short-Term Mitigations

Because the SRP currently supports only manual web-form submission, organizations should build a documented internal escalation path that gets a qualifying vulnerability or incident from initial detection to a completed SRP submission well inside the 24-hour window, accounting for the manual transcription step the platform's lack of API access currently requires [1]. This escalation path should specify backup representatives who can file if the primary representative is unavailable, given that only one primary and up to twenty secondary representatives can be registered per organization. Product-security and legal teams should also jointly review which of the organization's product lines and EU markets are covered by their registered CSIRT relationship, since the platform's coordination model depends on that mapping being accurate at the time of filing rather than reconstructed after the fact.

Strategic Considerations

The SRP's compressed and imperfect rollout is a preview of how CRA compliance is likely to unfold through the remaining phase-in period leading to full applicability on December 11, 2027, and organizations should not assume that subsequent milestones, including the essential cybersecurity requirements and conformity-assessment obligations still to come, will arrive with more operational lead time than this one did [4][7]. Manufacturers should treat CRA vulnerability and incident reporting as an

extension of existing product-security and vulnerability-disclosure programs rather than a standalone compliance task bolted onto product security after the fact, integrating the 24/72-hour/14-day reporting rhythm into the same processes that already govern patch development and customer notification. Given that penalties for reporting failures are already in force and independent of the platform's own feature completeness, organizations should not wait for ENISA to add API support or additional languages before building durable internal readiness; the obligation, and its financial exposure, exists today regardless of the tool's maturity [1][5].

CSA Resource Alignment

CSA's ENISA's SME Maturity Model Exposes a CRA Readiness Gap [7] is the most directly relevant prior CSA analysis: published in July 2026 from a survey of 194 organizations across 31 countries, it found that awareness of the CRA already outpaced organizations' practical readiness to execute on its obligations, with incident-response and vulnerability-handling processes identified as among the weakest areas, particularly for microenterprises. The SRP's compressed launch and its current lack of API support echo that same readiness gap, this time manifesting in the regulator's own tooling rather than only at the level of individual manufacturers, and organizations that scored poorly on ENISA's self-check in that earlier assessment should treat this note's recommendations as the concrete next step. CSA's analysis of NIS2 maturity gaps documents a structurally similar problem in a companion EU regime, showing that NIS2's 24-hour early-warning and 72-hour update requirements create the same compressed-notification dynamic now facing CRA reporters, and organizations already building NIS2 incident-reporting playbooks should extend that same internal escalation infrastructure to cover CRA-qualifying vulnerabilities and incidents rather than building a parallel process. For manufacturers whose CRA-covered products incorporate AI components, this reporting obligation also intersects with the Threat and Vulnerability Management domain of the CSA AI Controls Matrix (AICM) v1.1 [8], which sets analogous expectations for timely vulnerability identification, triage, and disclosure.

References

[1] Help Net Security. "ENISA launched the CRA Single Reporting Platform for actively exploited vulnerabilities." Help Net Security, September 14, 2026.

[2] ENISA. "The CRA Single Reporting Platform is launched." European Union Agency for Cybersecurity, September 2026.

[3] ENISA. "Single Reporting Platform (SRP)." European Union Agency for Cybersecurity, 2026.

[4] European Commission. "Cyber Resilience Act - Reporting obligations." Shaping Europe's Digital Future, 2026.

[5] White & Case LLP. "Cyber Resilience Act: The clock is ticking for compliance." White & Case, 2026.

[6] cyberresilienceact.eu. "With Reporting Due on 11 September 2026, ENISA's Single Reporting Platform Was Still Not Live." cyberresilienceact.eu, 2026.

[7] Cloud Security Alliance. "ENISA's SME Maturity Model Exposes a CRA Readiness Gap." Cloud Security Alliance, July 2026.

[8] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.