DRAGOS.COM

POSITIONING PAPER

DRAGOS EU CYBER RESILIENCE ACT COMPLIANCE POSITION

JUNE 2026

OT CYBERSECURITY BUILT FOR WHAT THE CRA DEMANDS

The EU Cyber Resilience Act (CRA) establishes binding requirements for any product with digital elements placed on the EU market. It demands that software and connected technologies be secure by design, resilient by default, and actively maintained throughout the product lifecycle. For organizations operating OT/ICS environments, the stakes are especially high: a rogue device or misconfigured asset is more than a data breach; it is a threat to human safety and operational integrity.

.

Dragos was built by practitioners who have responded to the most significant OT cyber-attacks on record. That operational experience is the foundation of how we architect our platform, build our threat intelligence, and support our customers. The CRA codifies what Dragos has practiced since its founding: security by design is a critical requirement, not an afterthought, in OT environments.

THE DRAGOS CRA COMPLIANCE PROGRAM

Dragos has established a dedicated, cross-functional CRA compliance program spanning our Engineering, Product, Governance, Risk, and Compliance (GRC), and Legal teams. This program addresses both our obligations as a vendor placing products on the EU market and our commitment to equipping customers with the documentation, evidence, and operational controls they need.

Our program is aligned with the IEC 62443-4-1 and IEC 62443-4-2 framework, which governs the security of industrial automation and control systems. This combined approach strengthens our Secure Development Lifecycle and the technical security posture of every product we ship.

Upcoming CE marking and conformity assessment: Dragos is assessing each in-scope product line against the CRA CE Marking tiers and will pursue the appropriate route, issue an EU Declaration of Conformity, and affix the CE marking accordingly. Because the CE marking reflects ongoing conformity rather than a one-time approval, we maintain it across the product lifecycle and reassess when changes materially alter a product's risk profile.

WHAT IS ALREADY IN PLACE

Dragos has been operationalizing CRA-aligned practices long before the Act entered into force. The following capabilities reflect existing program maturity:

- **Vulnerability disclosure and coordinated response:** Dragos maintains a formal, publicly documented Vulnerability Disclosure Policy (VDP) and a dedicated Product Security Incident Response Team (PSIRT). Dragos was designated by the CVE Program as a CVE Numbering Authority (CNA) in September 2022. As a CNA, Dragos is authorized to assign CVE IDs to newly discovered vulnerabilities and publicly disclose information about them through CVE Records. This includes vulnerabilities found in Dragos's own products as well as third-party products not covered by another CNA that Dragos discovers through its ongoing OT/ICS research. Customers and security researchers have clear channels to report vulnerabilities, and Dragos issues timely security advisories with actionable remediation guidance.
- **Software Bill of Materials (SBOM):** Dragos produces SBOMs for its platform and sensor product lines, enabling customers to maintain accurate inventories of software components and assess third-party dependency risk, consistent with the CRA's essential cybersecurity requirements (Annex I).
- **Secure Development Lifecycle (SDLC):** Dragos applies a structured SDLC to all product lines, including threat modeling, static and dynamic analysis, and mandatory security review gates prior to release.
- **Security update delivery:** Dragos provides security updates to customers throughout the supported lifecycle of each product, with a defined process for communicating update availability, impact severity, and installation guidance. In line with CRA support-period expectations, Dragos commits to a defined minimum support period as is defined in our software and hardware lifecycle support guides from the date of placing on the market and will notify customers in advance of any product reaching end of support.
- **Threat intelligence integration:** Dragos tracks 25+ named ICS threat groups. That intelligence is embedded directly into platform detections, enabling customers to identify adversary behaviors aligned with MITRE ATT&CK for ICS before they cause operational impact.
- **Incident response readiness:** Dragos maintains the only in-house OT incident response capability in the market, with practitioners who have responded to real-world attacks on critical infrastructure. IR retainer access is included in the platform, not offered as a separate engagement.

CRA COMPLIANCE ROADMAP

Milestone	Status / Target
Incident notification readiness (CRA Art. 14: 24-hr early warning / 72-hr full report, from 11 Sep 2026)	On track for September 2026 alignment
Full CRA conformity declaration	Target December 2027, subject to final Act text

PRODUCT LINES IN SCOPE

The following Dragos product families are in scope for CRA classification, conformity assessment, and certification activities. Dragos is determining each product line's CRA risk tier (default, Important, or Critical), which sets the applicable conformity-assessment route; classifications will be confirmed as harmonized standards and Commission implementing acts are finalized.

- **Platform:** Dragos Platform enterprise and cloud-managed deployment
- **Sensors:** Dragos Sensor hardware appliances and virtual sensor editions
- **Collector:** The endpoint-based collection agent deployed on OT assets
- **Services:** Includes OT Watch and other services

SUPPORTING YOUR CRA OBLIGATIONS

Customers who deploy Dragos in EU-connected environments may themselves have obligations under the CRA, depending on how products are integrated and placed into service. Dragos is committed to making compliance straightforward and to sustaining your operations throughout the product lifecycle. To support your own due diligence and conformity efforts, we provide:

- **Security documentation:** Product security specifications, architecture summaries, and security capability descriptions aligned to CRA Annex requirements.
- **SBOM access:** Component-level software inventory available for all in-scope product lines, updated with each release.
- **Security advisory distribution:** Timely disclosure of vulnerabilities affecting Dragos products, with CVSS scoring, affected version identification, and remediation steps.
- **CRA evidence packages (Planned once EU finalizes codification):** Structured documentation packages to support customer conformity assessments, audits, and regulatory submissions.
- **Direct engagement:** Our GRC and Product Security teams are available to engage directly with customer compliance, procurement, and security teams on CRA-specific questions.

OUR COMMITMENT

The Cyber Resilience Act represents an elevation of baseline security expectations for digital products, particularly those operating in or adjacent to critical infrastructure. Dragos welcomes this shift. Our platform was designed from the ground up to give OT operators the visibility, intelligence, and response capability to defend what matters most. Security by design is not an end in itself: it is

how we assist our customers in managing their operational technology cybersecurity risks. Every control we build, from coordinated vulnerability disclosure to lifecycle security updates to in-house incident response, exists to sustain safe, continuous operations through the full life of the products our customers depend on.

We are on track to meet all CRA obligations, and we will continue to provide customers with the evidence, documentation, and direct support needed to navigate their own compliance requirements. Questions about this program can be directed to our Product Security team.