Framework Foundations: EU Cybersecurity Resilience Act (CRA)

Introduction to EU CRA

The EU Cyber Resilience Act (CRA) is a landmark regulation designed to improve the cybersecurity of digital products sold or made available in the European market. Introduced by the European Commission in September 2022, the CRA applies to Products with Digital Elements (PDEs)—including hardware, software, and remote data processing solutions—but excludes software provided solely as a service, such as in-house or cloud-based systems. These are instead covered under the NIS2 Directive and other sector-specific regulations.

The EU CRA was adopted in October 2024 and entered into force in November 2024. While most obligations begin on December 11, 2027, some take effect earlier:

- June 11, 2026 – Member States must begin appointing and notifying conformity assessment bodies.
- September 11, 2026 – Manufacturers must begin meeting reporting obligations.
- December 11, 2027 – Full CRA compliance becomes mandatory for all covered products.

Objectives of EU CRA

- Strengthen cybersecurity of digital products sold in the EU.
- Reduce design-stage vulnerabilities in devices and software.
- Increase transparency of cybersecurity risks.
- Clarify liability for breaches by manufacturers and providers.
- Align EU practices with global cybersecurity standards.

Key Requirements

The CRA introduces mandatory requirements for manufacturers, importers, and distributors, including secure-by-design principles, vulnerability management, and long-term support. It also extends CE marking to digital products, signaling compliance with cybersecurity standards.

Secure by Design

Products must be built with secure default settings, access controls, and data protection features.

Risk-Based Development

Cybersecurity risk assessments are required during design, development, and maintenance.

Third-Party Component Due Diligence

Cybersecurity risk assessments are required during design, development, and maintenance.

Lifecycle Security Updates

Products must receive security updates for at least five years.

Vulnerability Management

Organizations must document vulnerabilities, disclose them responsibly, and notify authorities within 24 hours of active exploitation.

Incident Reporting

Severe incidents must be reported to EU authorities (CSIRT and ENISA) within 72 hours, with follow-up reports required.

Conformity Assessments

Products are classified by risk level. Non-critical products require self-assessment; critical ones need third-party evaluation.

CE Marking

Compliant products must display the CE mark, signaling adherence to CRA standards.

Economic Operator Duties

Importers and distributors must verify CE compliance and report risks. Open-source stewards must support secure development and disclosure practices.

How Cisco + Splunk Supports Compliance

Cisco and Splunk offer complementary capabilities that help organizations meet the cybersecurity obligations of the EU Cyber Resilience Act (CRA). Their combined strengths in secure infrastructure, observability, threat detection, and lifecycle support enable manufacturers and service providers to align with CRA requirements across product design, deployment, and incident response.

CRA Requirement	How Cisco + Splunk Supports Compliance	Relevant Products
Secure-by-Design	Promotes secure development practices, including secure boot, signed updates, and encryption	Cisco Secure Email, Cisco Umbrella, Cisco Secure Access, Cisco XDR, Cisco Secure Endpoint, Cisco Secure Firewall, Cisco Identity Services Engine (ISE), Cisco Secure Workload, Cisco Duo, Cisco Secure Client, Cisco Cyber Vision, Cisco Secure DDoS Protection, Spunk Enterprise Security (ES), Splunk SOAR, Splunk Attack Analyzer, Splunk User Behavior Analytics (UBA), Splunk Asset and Risk Intelligence (ARI)
Vulnerability Management	Supports continuous monitoring, vulnerability detection, and automated alerting	Cisco Secure Endpoint, Cisco XDR, Talos Threat Intelligence, Cisco Multicloud Defense, Cisco Secure Client, Cisco Secure Workload, Cisco Cyber Vision, Cisco Secure Equipment Access, Spunk ES, Splunk SOAR, Splunk Attack Analyzer, Splunk UBA, Splunk Asset and Risk Intelligence, Splunk Enterprise
Incident Reporting	Enables rapid detection and supporting workflows; Supports integration with incident response platforms	Cisco XDR, Cisco Secure Network Analytics (SNA), Cisco Secure Firewall, Cisco Secure Endpoint, Cisco Secure Malware Analytics, Talos Emergency Incident Response, Splunk ES, Splunk SOAR, Splunk Asset and Risk Intelligence, Splunk UBA
Lifecycle Security Updates	Long-term support for hardware and software ensures product resilience, while update tracking improves coverage and effectiveness	Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco XDR, Cisco Lifecycle Services, Splunk SOAR, Splunk Enterprise
SBOM & Technical Documentation	Supports SBOM generation and documentation tracking	Cisco Secure Firewall, Cisco AI Defense, Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco XDR, Cisco SNA, Splunk ES, Splunk SOAR, Splunk ARI, Splunk UBA
Conformity Assessment Support	Supports CRA-aligned deployments and enable audit readiness	Cisco XDR, Cisco Secure Firewall, Cisco Secure Endpoint, Cisco Malware Analytics, Cisco SNA, Cisco Duo, Cisco ISE, Talos Threat Intelligence, Cisco Cyber Vision, Splunk ES, Splunk SOAR, Splunk ARI, Splunk UBA, Splunk Enterprise

EU CRA Compliance with Cisco Security + Splunk

As organizations prepare for the EU Cyber Resilience Act (CRA), Cisco and Splunk offer a powerful combination of security, observability, and automation to support compliance and resilience. Together, they help manufacturers and service providers meet CRA obligations across the product lifecycle—from secure design and vulnerability management to incident response and audit readiness.

Cisco secures digital products at the core, while Splunk adds visibility, automation, and traceability. This enables organizations to:

- Accelerate CRA readiness through unified visibility and risk-based prioritization.
- Streamline reporting and documentation with automated workflows and audit trails.
- Enhance product resilience by detecting, responding to, and recovering from threats faster.

Together, Cisco and Splunk empower businesses to not only meet CRA requirements but also build a more secure and resilient digital ecosystem.

Resources

For more information and guidance on EU CRA compliance, please refer to the following resources:

- EU Cyber Resilience Act website
- Cisco Trustworthy Solutions
- Cisco Trustworthy Technologies Data Sheet