SECURE CODE WARRIOR

SCW: CRA-Aligned Learning Pathways

Building Secure by Design Skills for the Cyber Resilience Act

The Cyber Resilience Act 2024 (CRA) is an EU regulation that introduces mandatory cybersecurity requirements for most products with a digital component sold in the EU. The CRA enhances cybersecurity standards of such products, which in turn requires manufacturers, importers, distributors, and retailers to ensure cybersecurity throughout the lifecycle of these products. Secure Code Warrior supports CRA readiness with CRA-aligned Quests and conceptual learning collections that help development teams build the Secure by Design, SDLC, and secure coding skills aligned with the CRA's secure development principles.

Understanding the Cyber Resilience Act 2024 (CRA)

The CRA ensures that products with a digital component placed on the EU market remain secure throughout their lifecycle, reinforcing the need for secure architecture, secure development practices, and robust vulnerability management across teams. Key CRA compliance dates include September 2026 (vulnerability reporting obligations take effect) and December 2027 (full compliance required for all in-scope products), making it important for organizations to start building readiness now.

Does the CRA apply to you?

- ✓ Manufacturers of products with a digital component
- ✓ Importers, distributors and retailers placing products on the EU market
- ✓ Critical infrastructure operators sourcing CRA-compliant products
- ✓ Essential service providers relying on secure digital components

Products likely in scope:

- Software applications and operating systems
- IoT and connected devices
- Embedded and smart home systems
- Network equipment and industrial control systems

Values and Benefits

CRA-Aligned Learning

Structured, easy-to-assign content mapped to CRA expectations.

Secure by Design Skills

Conceptual and practical knowledge developers need to build resilient software.

Simple to Deploy

CRA content is ready to add to your annual learning program.

How SCW Supports CRA Readiness

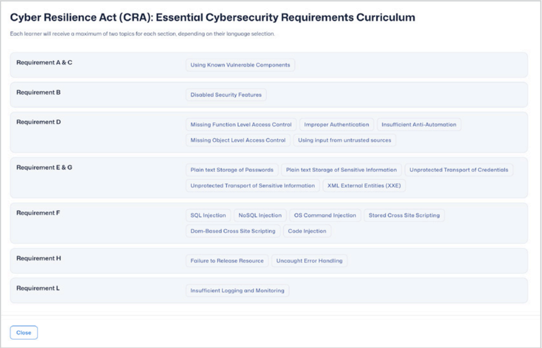
Secure Code Warrior provides practical capability building aligned to the Secure by Design and SDLC principles referenced in the CRA. CRA-aligned Quests and conceptual learning collections help teams strengthen secure coding habits, improve architecture and design awareness, and handle vulnerabilities more effectively. SCW does not certify compliance, but supports CRA readiness by providing structured learning and measurable capability improvement.

What SCW Delivers to Support CRA

Secure Code Warrior offers a blended learning approach that matches the CRA's focus on process-driven security. Teams gain both conceptual knowledge and practical experience fixing real vulnerabilities in code.

CRA Standard in Quests

Deploy the CRA Standard Quest to deliver a structured CRA-aligned pathway that combines secure-by-design concepts with high-priority vulnerability topics. Each learner will receive up to two language-specific vulnerability topics per section, selected by them, to ensure relevance. This mapping focuses specifically on the technical, language-level vulnerability requirements outlined in Annex I, Part I of the Act.



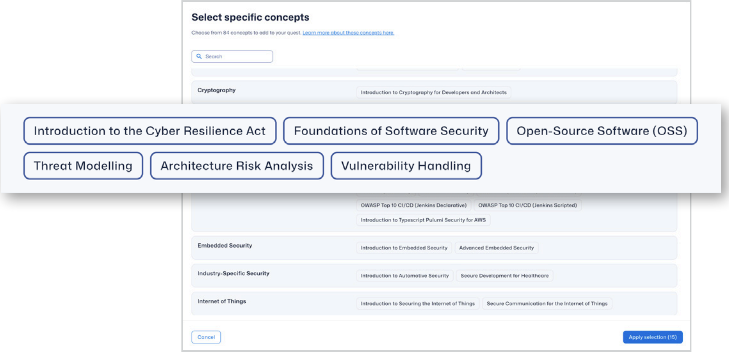
Cyber Resilience Act (CRA): Essential Cybersecurity Requirements Curriculum

Each learner will receive a maximum of two topics for each section, depending on their language selection.

Requirement A & C	Using Known Vulnerable Components
Requirement B	Disabled Security Features
Requirement D	Missing Function Level Access Control Improper Authentication Insufficient Anti-Automation Missing Object Level Access Control Using input from untrusted sources
Requirement E & G	Plain text Storage of Passwords Plain text Storage of Sensitive Information Unprotected Transport of Credentials Unprotected Transport of Sensitive Information XML External Entities (XXE)
Requirement F	SQL Injection NoSQL Injection OS Command Injection Stored Cross Site Scripting Dom-Based Cross Site Scripting Code Injection
Requirement H	Failure to Release Resource Uncaught Error Handling
Requirement L	Insufficient Logging and Monitoring

CRA Secure by Design Conceptual Collection

Broader procedural requirements and other sections of the CRA are covered in our conceptual course including bite-size topics on secure architecture, SDLC fundamentals, design principles, OSS and supply chain security, threat modeling, and secure coding basics.



Select specific concepts

Choose from 84 concepts to add to your quest. Learn more about these concepts here.

Cryptography	Introduction to Cryptography for Developers and Architects
	OWASP Top 10 CI/CD (Jenkins Declarative) OWASP Top 10 CI/CD (Jenkins Scripted) Introduction to Typescript Pulumi Security for AWS
Embedded Security	Introduction to Embedded Security Advanced Embedded Security
Industry-Specific Security	Introduction to Automotive Security Secure Development for Healthcare
Internet of Things	Introduction to Securing the Internet of Things Secure Communication for the Internet of Things

Introduction to the Cyber Resilience Act
Foundations of Software Security
Open-Source Software (OSS)
Threat Modelling
Architecture Risk Analysis
Vulnerability Handling

Additional Recommended SCW Learning Topics Relevant to the CRA

Introduction to the Cyber Resilience Act 2024
Foundations of Software Security
Open-Source Software (OSS)
Threat Modeling
Architecture Risk Analysis
Vulnerability Handling
Using Known Vulnerable Components
Disabled Security Features
Missing Function Level Access Control
Improper Authentication
Insufficient Anti-Automation
Missing Object Level Access Control
Using Input from Untrusted Sources
Plain Text Storage of Passwords
Plain Text Storage of Sensitive Information
Unprotected Transport of Credentials
Unprotected Transport of Sensitive Information
XML External Entities (XXE)
SQL Injection
NoSQL Injection
OS Command Injection
Stored Cross Site Scripting
DOM-Based Cross Site Scripting
Code Injection
Failure to Release Resources
Uncaught Error Handling
Insufficient Logging and Monitoring

SCW helps organizations prepare for the Cyber Resilience Act by giving development teams the practical skills and Secure by Design foundations aligned with the regulation's secure development principles. CRA-aligned learning pathways make it simple to build consistent secure development capability across diverse teams, reduce product risk, and strengthen long-term software resilience. With SCW, organizations can confidently advance their secure development maturity in line with the secure development principles of the CRA.

To learn more, please visit How Secure Code Warrior can assist you in achieving Compliance: CRA (Cyber Resilience Act).

About Secure Code Warrior

Secure Code Warrior is a Developer Risk Management Platform enabling enterprises to measure, manage and mitigate risk. Improve security posture and reduce vulnerabilities by up to 53% with our integrated approach of organizationally benchmarking developer secure code skills, governance through quality gates, integrated during code changes and upskilling with a dynamic on-demand secure code learning platform. Trusted by over 600 enterprises to help them deliver secure software rapidly and create a culture of developer-driven security.

securecodewarrior.com | **Request a demo** |