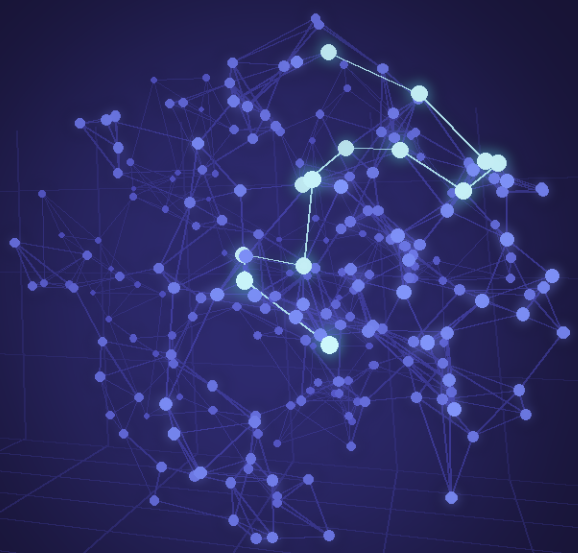
ThreatModeler

REGULATORY BRIEF · EU CYBER RESILIENCE ACT

Threat modeling as the foundation for CRA compliance

The Cyber Resilience Act's "secure by design and by default" requirement is a codification of design-time security assurance. That is precisely what threat modeling delivers.



THREATMODELER® NEXUS™

01 · WHY NOW

A compliance deadline, not a suggestion.

Regulation (EU) 2024/2847 entered into force in December 2024. Reporting duties are active now, and full application, including the essential requirements and conformity assessment, arrives at the end of 2027. Manufacturers of products with digital elements sold in the EU are the ones on the clock.

1

IN FORCE

10 Dec 2024

The Regulation entered into force.

2

ACTIVE NOW

11 Sept 2026

Reporting duties for actively exploited vulnerabilities and severe incidents apply.

3

UPCOMING

11 Dec 2027

Full application, including the essential requirements and conformity assessment.

What Annex I asks for

The Regulation requires manufacturers to maintain a documented risk assessment mapped to the essential requirements, and to report actively exploited vulnerabilities to ENISA within 24 hours, with follow-up reporting triggered at 72 hours and 14 days. Meeting Annex I means establishing three things before a product ships.

01

A structured attack surface

A documented understanding of the product's architecture, data flows, and trust boundaries, established before the product ships, not reconstructed after.

02

A repeatable design process

An auditable way to find and mitigate design-level weaknesses during design, rather than relying on scanning after the product is already built.

03

Technical documentation

Evidence that risk identification and security controls were part of the design decisions themselves, and available for regulatory review.

WHERE MOST TEAMS FALL SHORT

Post-build scanning validates what has already shipped. It cannot produce the design-phase risk assessment Article 13 expects, because by the time it runs, the design decisions are already made.

Design-time assurance, by requirement.

ThreatModeler Nexus gives security teams a continuous view of architectural risk instead of a snapshot from run-time scanning. It maps identified risk to the corresponding regulatory language and keeps a living system of record for every control applied, so the thinking behind secure design stays auditable.

CRA REQUIREMENT AREA	THREATMODELER NEXUS ALIGNMENT
Design-time risk assessment Art. 13(2)–(3) · Annex VII(3)	Threat models are generated directly from system architecture and stay current as the design evolves, producing the documented risk assessment the Regulation expects from the design phase onward.
Secure-by-design properties Annex I, Part I(1)	Threats and mitigations from MITRE ATT&CK, CAPEC, and OWASP are mapped automatically to identified components, making attack surface and trust boundaries explicit before code is written.
Documentation & standards evidence Annex VII(2)(a), (5) · Art. 13(13)	Modeling produces architectural evidence as a byproduct, mapped to CRA, NIST, ISO 27001, and IEC 62443, and retained in the platform for as long as the Regulation requires.
Vulnerability handling & continuous testing Annex I, Part II(1) & (3)	The ThreatModeler Nexus MCP Server exposes threat modeling context in IDEs, pull requests, and CI/CD pipelines, so review runs continuously rather than on a fixed schedule.
Consistent governance as products change Art. 13(1), (14)	Security policy is enforced automatically across every project, and models update as architecture, threats, and frameworks change, so conformity holds across the portfolio.

Illustrative mapping only. Not a substitute for the official text of the Regulation or for legal advice on conformity assessment.

03 · PURPOSE BUILT

Built for CRA compliance.

ThreatModeler Nexus helps organizations operationalize the CRA's secure-by-design expectations inside a governed environment.

VISIBILITY

Architectural documentation

Living threat models generated directly from system architecture produce structured, auditable evidence for Annex VII technical documentation.

THREAT INTELLIGENCE

A curated threat & control library

Threats and mitigations sourced from MITRE ATT&CK, CAPEC, OWASP, and other recognized bodies, mapped automatically to identified components.

STANDARDS

Built-in compliance mappings

Mappings to frameworks including NIST, ISO 27001, and IEC 62443, with a compliance library covering the CRA's Articles and Annexes.

180+
compliance frameworks mapped

2,500+
security requirements in the library

13
granted patents

Illustrative mapping only; not legal advice and not a substitute for the official text of the Regulation. This document is marketing material, does not form the basis of any contract, and creates no warranty or guarantee of regulatory compliance.

Achieve the design-time assurance the CRA requires.

Book a personalized demo with a solutions architect to see how ThreatModeler Nexus helps security and governance teams meet CRA requirements.

BOOK A DEMO

ThreatModeler