CERTIFY by OmniTrust

DATA SHEET

Automate Threat Modeling and Compliance Readiness for Connected Products

Generate Threat Models 20× Faster - and Keep Them Accurate Over Time

Continuous Threat & Risk Process Challenges

Connected products now face continuous cybersecurity risk. New vulnerabilities emerge daily. Software updates change system behavior. Complex supply chains introduce new dependencies and vulnerabilities. And regulators increasingly demand **lifecycle cybersecurity governance**.

Examples include:

- EU Cyber Resilience Act (CRA)
- UNECE vehicle regulations
- NIST secure frameworks
- ISO / IEC security standards
- FDA cybersecurity guidance

Security teams must repeatedly answer difficult questions:

- How do we produce high-quality TARAs quickly?
- How do we keep threat models accurate as systems evolve?
- How do teams coordinate across engineering, security, and compliance?
- How do we maintain lifecycle evidence for regulators and auditors?

Most organizations still rely on **manual brainstorming and spreadsheets**, or outdated tools which are slow, inconsistent, and difficult to maintain over time.

The OmniTrust Certify Solution

Certify automates threat modeling and TARA development workflows for individuals and teams.
Using Certify's automated threat and risk modeling engine, organizations can:

- ✓ Generate structured threat models and TARAs **20× faster**
- ✓ Eliminate manual brainstorming and repetitive threat analysis
- ✓ Produce consistent, repeatable risk assessments
- ✓ Coordinate security workflows across teams
- ✓ Maintain lifecycle records for compliance and audit readiness

Certify transforms threat modeling from a **manual exercise** into a **repeatable engineering process, and the solution is offered in 3 Modes as follows:**

CERTIFY | Standard TARA Generator

Automated TARA Generator - Certify Standard automates the creation of threat models and TARA reports, reducing the time required from weeks to hours.
Using Certify's threat and risk modeling engine, teams can quickly generate structured security analyses from product descriptions and supporting documentation.

Key capabilities

- Automated threat and risk modeling
- Structured TARA generation and reporting
- Automated system architecture and data flow diagrams
- Standardized risk assessment outputs
- Exportable documentation for engineering teams

Certify Standard eliminates repetitive manual brainstorming and enables teams to generate consistent security analyses faster than historically possible using intelligent automation.

→

CERTIFY | Lifecycle Pro

Continuous Product Security - Lifecycle Pro transforms threat modeling from a one-time exercise into a **continuous lifecycle security capability**. Instead of generating isolated documents, Lifecycle Pro maintains a persistent security profile for each product, supporting ongoing risk management as systems evolve.

Key capabilities

- Persistent product security profiles
- Collaborative human review and validation workflows
- Lifecycle event tracking and security updates
- Portfolio visibility across product families
- Audit-ready lifecycle security history

Lifecycle Pro enables organizations to maintain living threat models that evolve with the product over time.

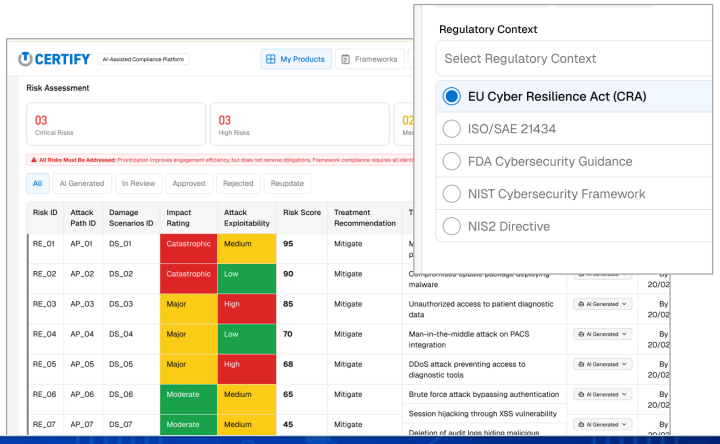
CERTIFY | White Glove (WG)

Expert-Led Threat Modeling and Compliance Support - Certify White Glove provides organizations with **expert-led threat modeling and regulatory preparation**, delivered by OmniTrust cybersecurity specialists using the Certify platform.

Key capabilities

- Expert-led threat modeling and TARA development
- Security architecture review and validation
- Regulatory preparation support (CRA, UNECE, NIST, ISO, FDA)
- Audit-ready documentation packages
- Portfolio-level security assessments

White Glove engagements combine Certify automation with experienced security practitioners to deliver **high-confidence, audit-ready security analyses.**



BEYOND STATIC THREAT MODELS

Traditional threat modeling tools produce **static documents** that quickly become outdated.

Certify enables **continuous lifecycle security management**.
Instead of rebuilding threat models from scratch each time systems change, Certify maintains a structured security record that can be updated as new information emerges.

This dramatically reduces the ongoing cost and complexity of managing product cybersecurity programs.

Preparing for Emerging Cybersecurity Regulations

Global regulations are shifting toward **continuous cybersecurity governance** rather than one-time documentation. Certify helps organizations prepare for regulatory environments such as: EU CRA), UNECE vehicle regs, NIST frameworks, ISO standards and FDA cybersecurity for med devices

These regulations increasingly require organizations to demonstrate lifecycle cybersecurity governance.

- Generate documentation faster
- Maintain lifecycle evidence and decision records
- Coordinate security responses across teams
- Prepare both pre-market and post-market regulatory submissions

OmniTrust (formerly ISS) secures the connected world, from silicon to cloud systems and AI - by delivering verifiable, enforceable trust across the entire device and software lifecycle. As the leader in Trust Lifecycle Management (TLM), OmniTrust ensures security from design and provisioning through operation, update, and retirement, protecting more than 2 billion devices and 3 billion software updates annually. Through Certify, OmniTrust extends security from threat modeling to lifecycle enforcement, enabling organizations to move from identifying risk to enforcing trust across devices and software, throughout the entire product lifecycle.

OmniTrust www.OmniTrust.com