

EU Cyber Resilience Act für Softwarehersteller in der Praxis

Dr. Stephan Hutterer
sh@complyd.io
https://complyd.io

Dr. Stephan Hutterer, CISSP

Education

Dipl.-Ing. (FH) Automation Engineering, Dr. Informatics

Professional

15+ Years in Industry | 10+ Years Critical Infrastructure

2014–2024: Head of Product Management & Product Security – Industrial Electronics

Since 2024: CyberUp GmbH | Since 2025: COMPLYD GmbH



CyberUp

COMPLYD

Certifications / Auditor

CISSP | NIS-Auditor | ISO 27001 & IEC 62443 Auditor (CIS Cert, B-Sec)

Cybersecure Products – Are You Ready?

EU Cyber Resilience Act Enforces Security

(Business) Customers Demand For Security

Compliance Necessary 12/2027: Lots Of Work To Do

Fail To Comply:

- Lose Customers
- Pay EU Penalties

Summary – CRA

What: Cybersecurity requirements for all **Products with Digital Elements**

Where: Applies to the **EU Market**, not just to European manufacturers

How: Requirements apply to:

- **The product itself** (technical characteristics)
- **Process and documentation**, including **CE marking**
- **Vulnerability management** and remediation
- **Reporting obligations** for vulnerabilities and incidents

When:

For all products placed on the market from **11. December 2027**

For all products, including those already on the market, from **11. September 2026**

Sanctions: Up to **15 million EUR or 2.5% of annual turnover**

CLASSIFICATION: PUBLIC

CRA Requirements

Essential Requirements (Annex 1)

Product Design & Development

Design Fundamentals

- Risk-based secure design
- Data integrity & confidentiality
- User access control
- Limit attack-surface, secure-by-default
- Minimization of data use
- Secure removal / restoration
- No known exploitable vulnerabilities

Incident Readiness & Resilience

- Logging
- SBOM (where applicable)
- Incident impact limitation / reduction
- Exploitation mitigation measures
- Availability of essential functions

Maintenance

Vulnerability & Incident Management

- Advisory & disclosure process; for exploited vulnerabilities and severe incidents
- CSIRT/PSIRT
- Security updates
- Security tests & reviews

Documentation & Product Management (Annex 2,7)

Public / User

User Documentation

- Intended purpose & functionality
- Security environment & properties
- Foreseeable misuse
- Security-related handling (hardening measures, decommissioning, update installation, etc.)
- Support period

Documentation w.r.t conformity

Technical / process documentation

- Risk assessment / model
- Product description, intended use & environment
- Product design information (architecture, dependencies, etc.)
- Test reports w.r.t conformity
- Support period

EU declaration of conformity (Annex 5,6,8)

CE

+ Assessment scheme based on product class (Internal control, quality assurance, type-examination, certification)

CLASSIFICATION: PUBLIC

CRA Requirements

Essential Requirements (Annex 1)

Product Design & Development

Design Fundamentals
- Risk-based secure design
- Data integrity & confidentiality
- User access control
- Limit attack-surface, secure-by-default
- Minimization of data use
- Secure removal / restoration
- No known exploitable vulnerabilities

Incident Readiness & Resilience
- Logging
- SBOM (where applicable)
- Incident impact limitation / reduction
- Exploitation mitigation measures
- Availability of essential functions

Maintenance

Vulnerability & Incident Management
- Advisory & disclosure process; for exploited vulnerabilities and severe incidents
- CSIRT/PSIRT
- Security updates
- Security tests & reviews

Documentation & Product (Annex 2,7)

Public / User

User Documentation
- Intended purpose & functionality
- Cybersecurity features
- Foreseeable misuse
- Security-related handling (haredening measures, decommissioning, update installation, etc.)
- Support period

Documentation w.r.t conformity

Technical / process documentation
- Risk assessment / model
- Product description, intended use & environment
- Product design information (architecture, dependencies, etc.)
- Test reports w.r.t conformity
- Support period

- **Know what you ship. The software, the risks, the security.**
- **Be able to maintain security and handle issues.**
- **Document. Everything – and even more. For you & your customers.**

EU declaration of conformity Annex 5,6,8)

CE

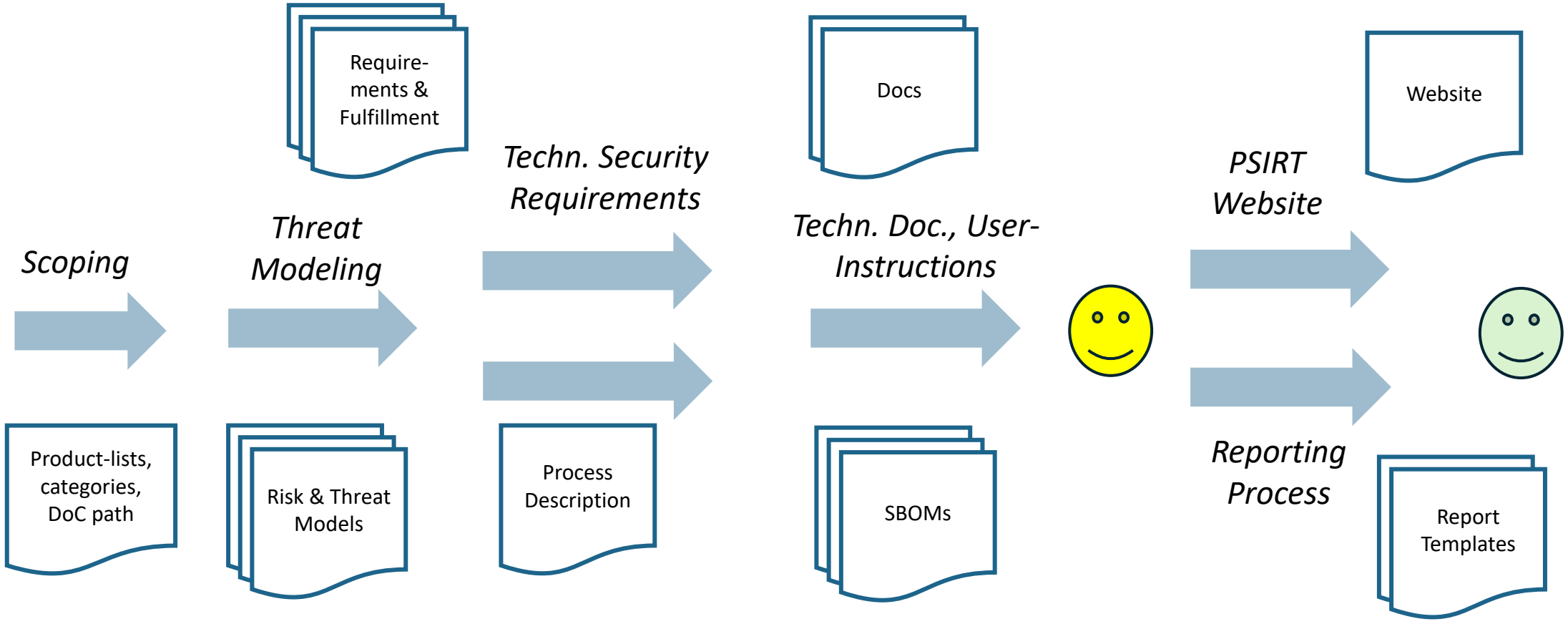
+ Assessment scheme based on product class (Internal control, quality assurance, type-examination, certification)

CLASSIFICATION: PUBLIC

Choose your CRA path. There are many bad ones.



The CRA Path



Product-Lifecycle Definitions

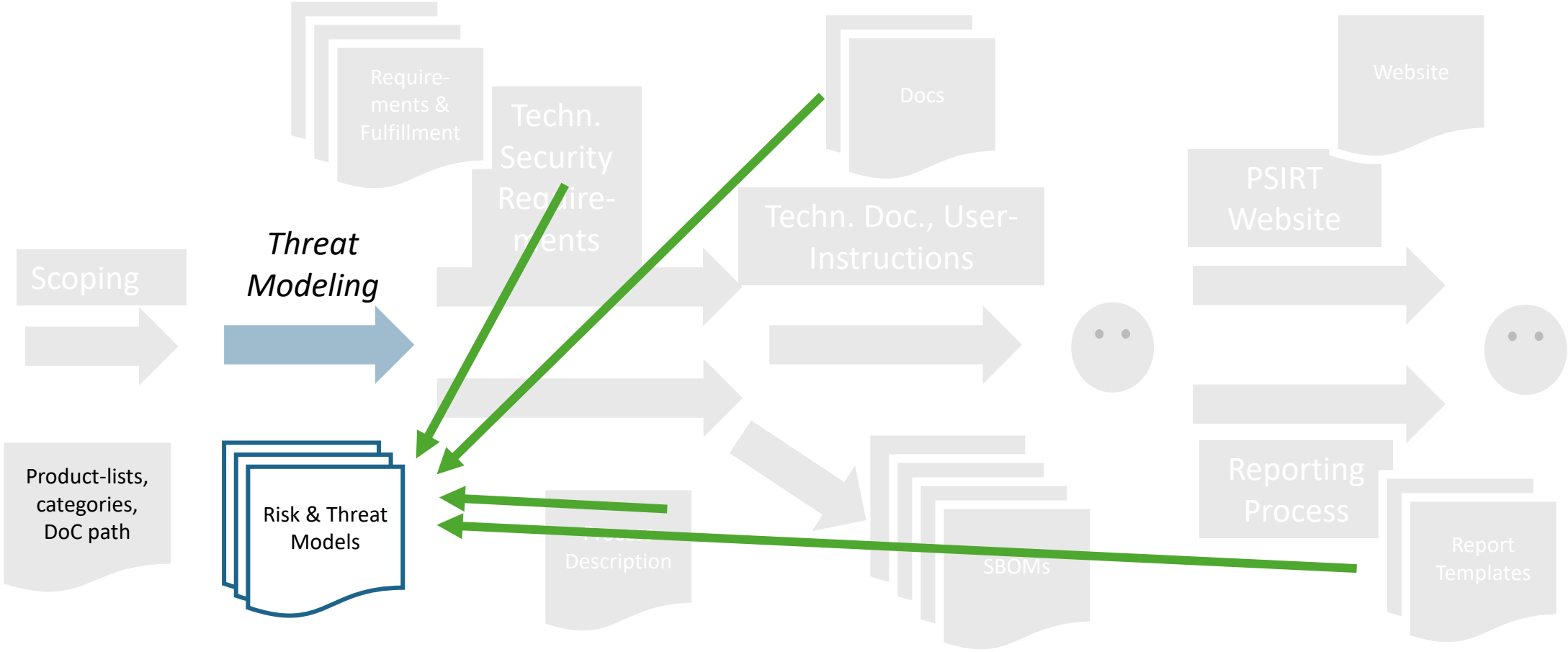
Techn. Implementations

DevSecOps

SSDLC Intro, SupplyChain, etc.…

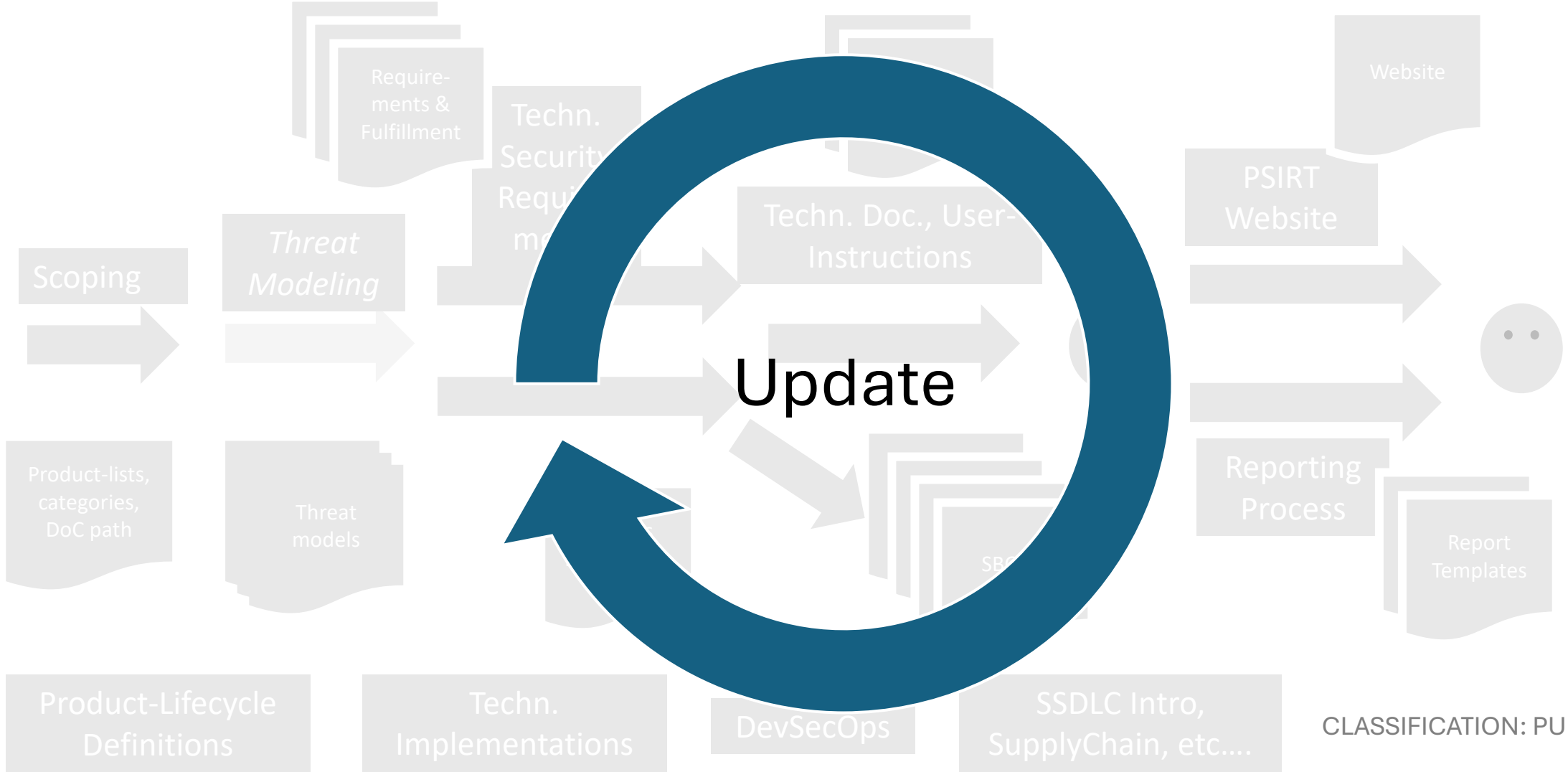
CLASSIFICATION: PUBLIC

Threat Models – The Ultimate Anchor



CLASSIFICATION: PUBLIC

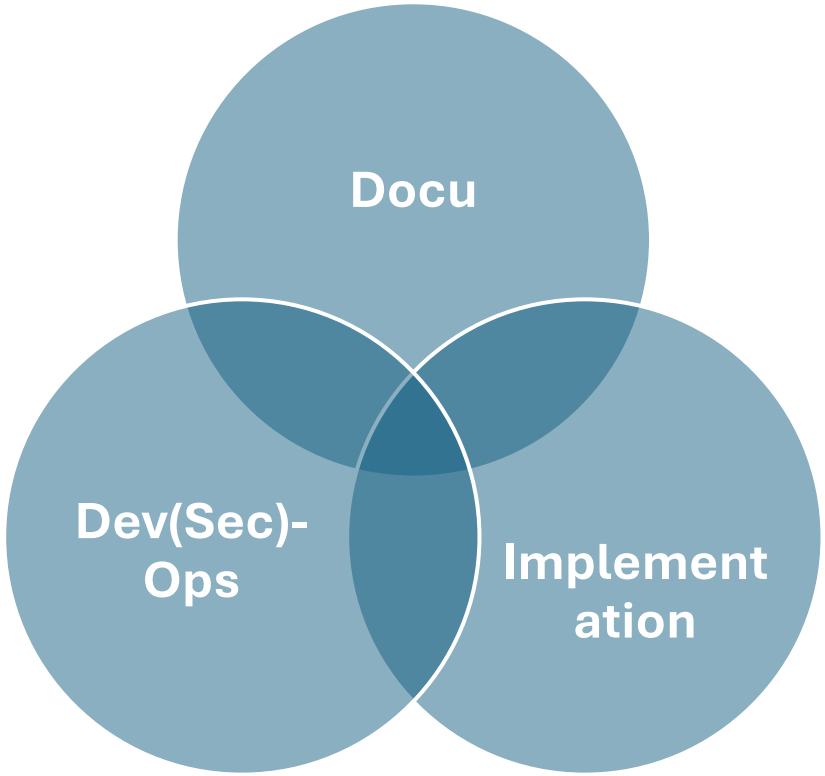
And now? Keep everything up-to-date



CLASSIFICATION: PUBLIC

Tool-Support?

Confluence Jira Excel draw.io



Release Management

SBOM Generation

Software Supply Chain Security

Vulnerability Handling

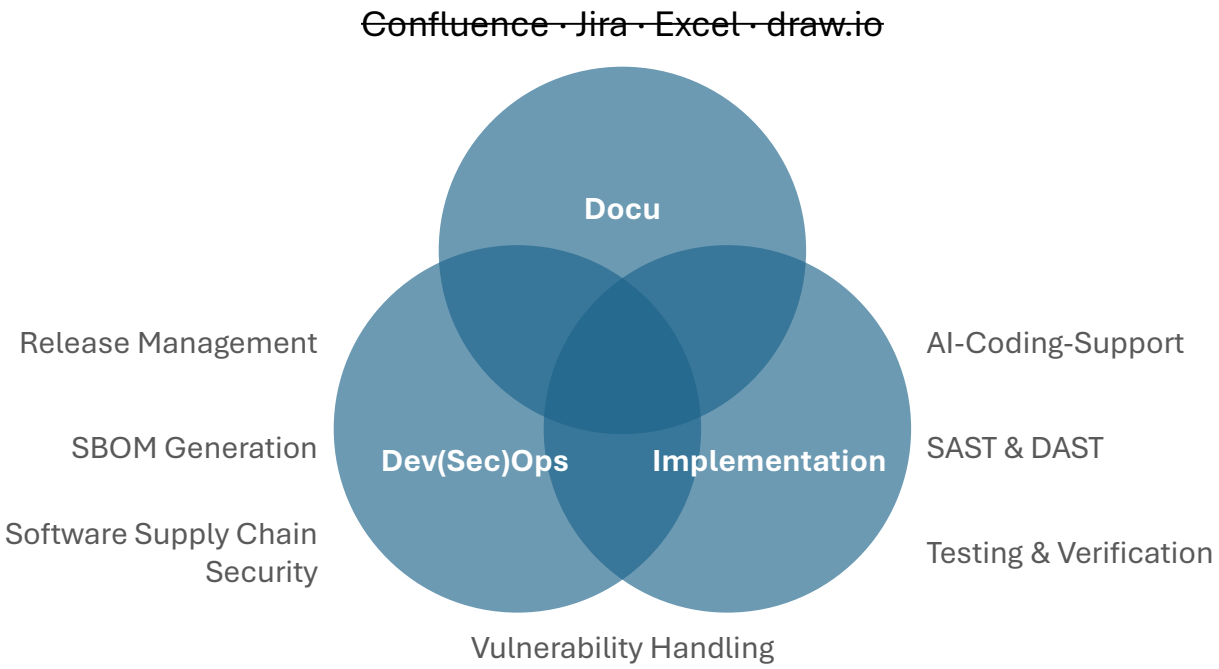
AI-Coding-Support

SAST & DAST

Testing & Verification

CLASSIFICATION: PUBLIC

Tool-Support?



What no tool keeps up to date

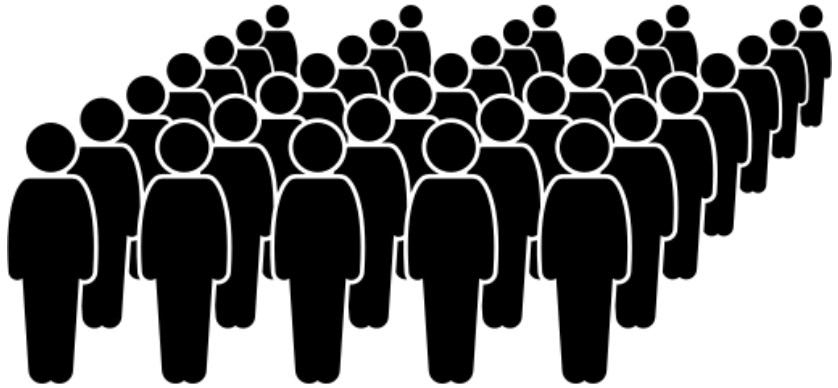
- Risk & threat models
- Security requirements & design proof
- Technical documentation
- User instructions
- SSDLC proof

Every release outdates them. The CRA expects them current.

CLASSIFICATION: PUBLIC

How to CRA?

Standard



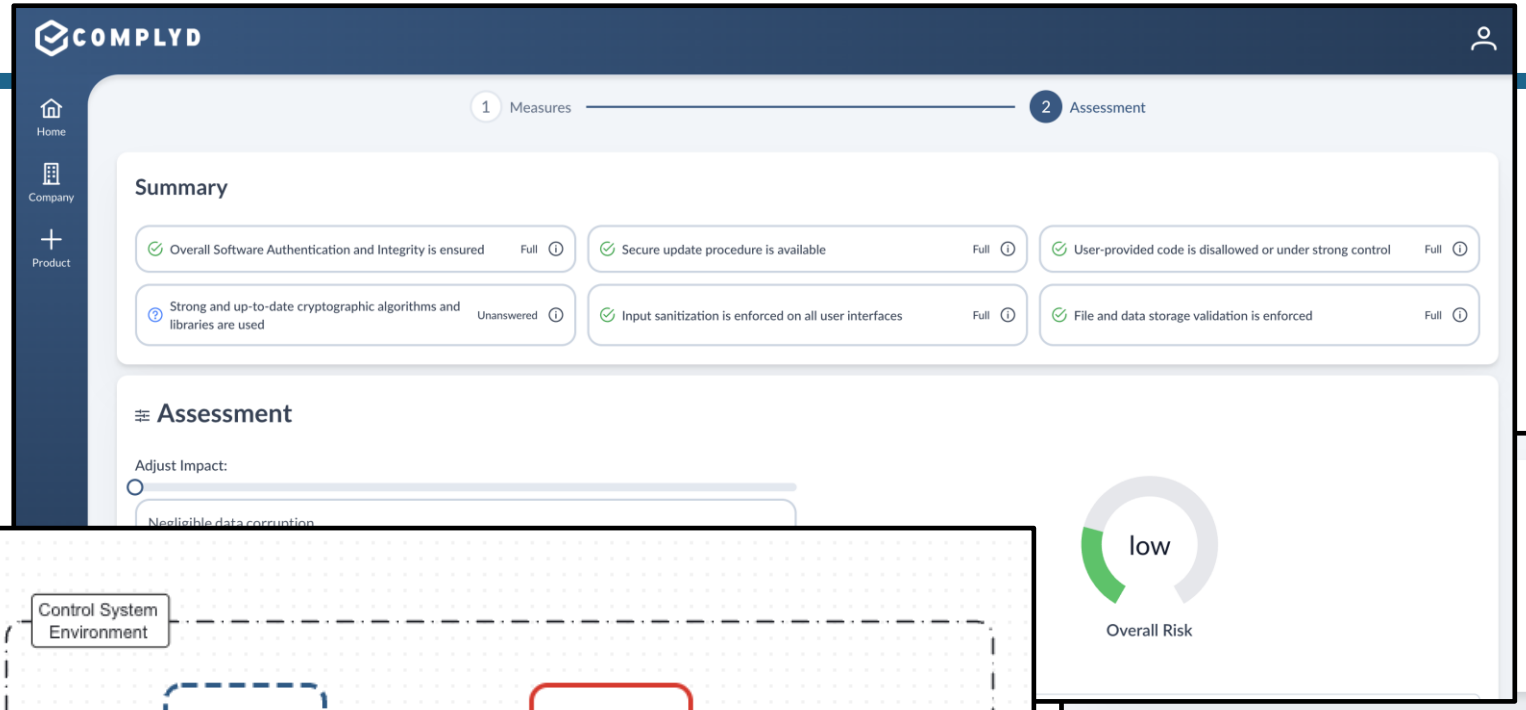
Smart

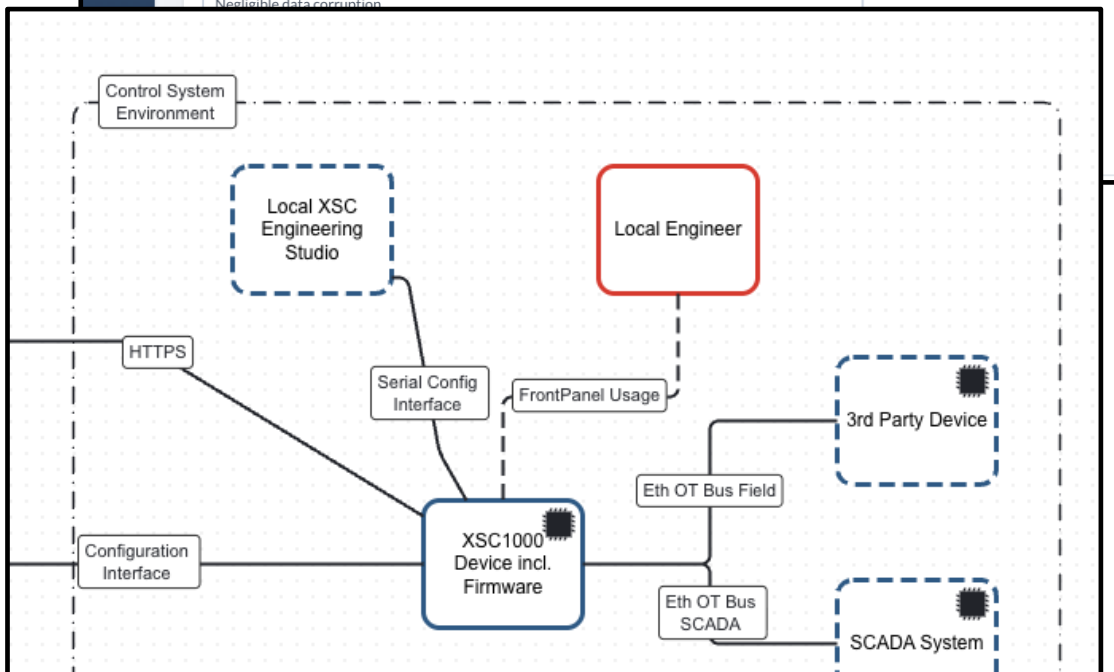


CLASSIFICATION: PUBLIC

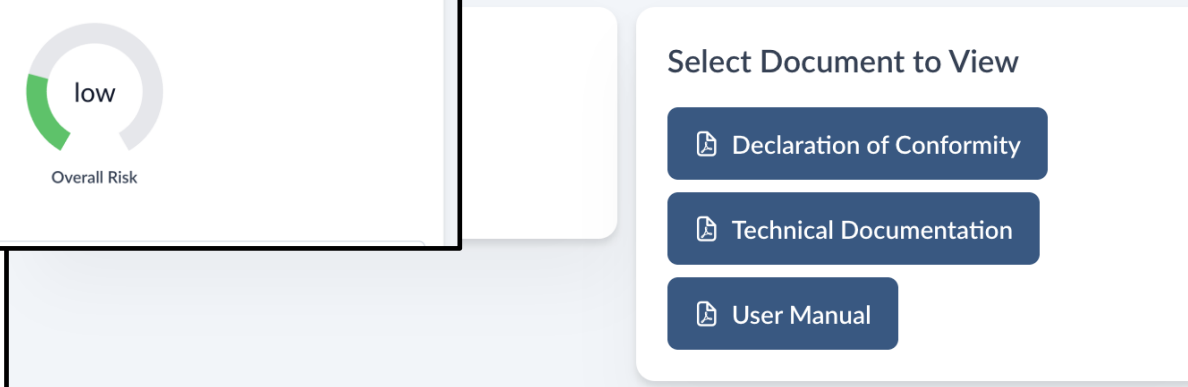
Some Impressions...

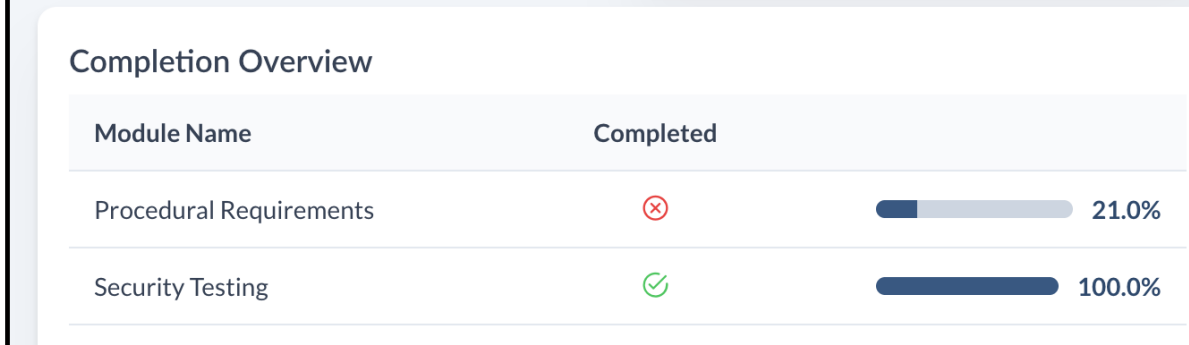
Guided graphical product risk-modelling





COMPLYD generates all documents you need for conformance declaration





COMPLYD: Your Product Security Experts



CLASSIFICATION: PUBLIC


COMPLYD.IO