German OWASP Day 2025

Cyber Resilience Act: Wie OWASP für Hersteller eine entscheidende Rolle spielen kann

Dominik ’bitkeks’ Pataky

2025-11-26

Intro & Disclaimer

- Who am I? – Dominik Pataky, OWASP Frankfurt am Main. Builder of SaaS for CRA processes & DevSecOps 👨‍💻
- Talk in German, slides in English, everybody welcome 👋
- Disclaimer: This talk is not legal advice. CRA is still a moving target. Complex interdependencies. 🤯

Motivation – What's the goal of this talk?

1. Understand the CRA requirements
2. Know what OWASP has to offer
3. Map the requirements to OWASP projects

The Cyber Resilience Act

aka CRA
aka Regulation (EU) 2024/2847

What does the CRA want from us?

- Cyber Resilience Act = EU regulation = immediate effect
- Goal: Raise the level of **cyber security in digital products**
- Starts partly in Sept 2026, **full effect in Dec 2027**
- Manufacturers need to conform and apply CE marking

Details of the requirements

1. **Secure software development lifecycle** as base level
2. **Documentation**! (For customers and for MSA)
3. Continuous **monitoring for vulnerabilities** in products
4. **Patching** own products during their support window
5. **Reporting of vulnerabilities** to central platform (ENISA)

Software security finally a legal issue!

Have you previously lobbied for more software security?

Then the **CRA is your friend**!

„Regulation creates budgets“ – Get ready!

Relevant context

- New Legislative Framework (**NLF**) with the „Blue Guide“
- **NIS2** and **DORA**: Supply Chain Management
- **BSI TR-03183**: „Cyber-Resilienz-Anforderungen“
- Radio Equipment Directive (**RED**), **IEC 62443** for OT

Product with digital Elements (PdE)

Definition: ***'product with digital elements'*** *means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;*

Product with digital Elements (PdE)

Definition: ***'product with digital elements'*** *means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;*

☝ Important: The CRA regulates **commercial products**

❌ Not how Open Source Software is developed (*)

❌ Not how companies manage themselves (NIS2, DORA)

* OSS plays key role in commercial products

Important and critical Products

- Annex III and IV: „important“ and „critical“ products
- **More conformity requirements**
- Conformity assessment through third party
- Some allow self-assessment with **harmonized standards**
  - Created by CEN/CENELEC and ETSI
  - 15 horizontal standards (e.g. „generic security requirements“)
  - 26 vertical standards (e.g. „browsers“, „firewalls“, „hypervisors“)

What's all the fuzz about OSS?

- 💎 Open Source Software essential in CRA
- 🌈 Commercial products use OSS components (libraries)
- 🤦 But: OSS maintainers are NOT manufacturers
- 😱 Huge gap in patching responsibility!

What's all the fuzz about OSS?

💎 Open Source Software essential in CRA

🌈 Commercial products use OSS components (libraries)

🤦 But: OSS maintainers are NOT manufacturers

😱 Huge gap in patching responsibility!

- First drafts of the CRA missed this
- OSS and free software community lobbied for changes
- Solution: OSS excempt, **Stewards** are born

SBOMs: Software Bills of Materials

- Contains a **list of all used software components**
- German translation: „Software-Stückliste“

⚠ Transparency for the **Open Source** Supply Chain!

SBOMs: Software Bills of Materials

- Contains a **list of all used software components**
- German translation: „Software-Stückliste“
- ⚠ Transparency for the **Open Source** Supply Chain!
- Different „levels“ of depth and detail
  → BSI TR-03183, CISA „Minimum Elements for SBOM“
- Two de-facto standards: **CycloneDX** and **SPDX**

OWASP enters the stage

What's in OWASP that is relevant for CRA?

- OWASP Software Assurance Maturity Model (SAMM)
- Threat Modeling with OWASP Threat Dragon and pytm
- OWASP Top 10 and Cheat Sheet series
- CycloneDX SBOM standard, now in v1.7
- Dependency-Track for vulnerability tracking

And OWASP DefectDojo, Dependency-Check, SecureCodeBox, DevGuard, ...

Processes before tools!

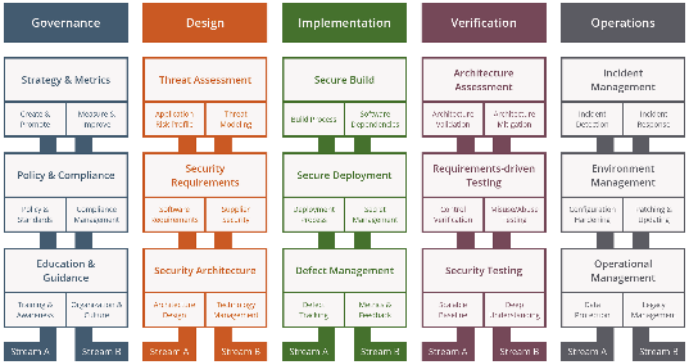
⚠️ ⚠️ ⚠️

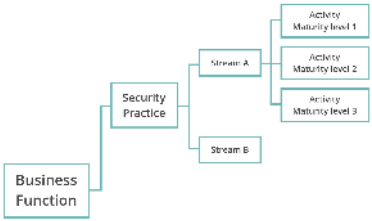
When entering CRA territory,
sharpen your **processes first**.
Then deploy appropriate tools.

Complex CI/CD cannot by itself
create CRA compliant products.

OWASP Software Assurance Maturity Model

„SAMM provides an effective and measurable way for all types of organizations to analyze and improve their software security posture.“





Source: `https://owasp.org/www-project-samm/`

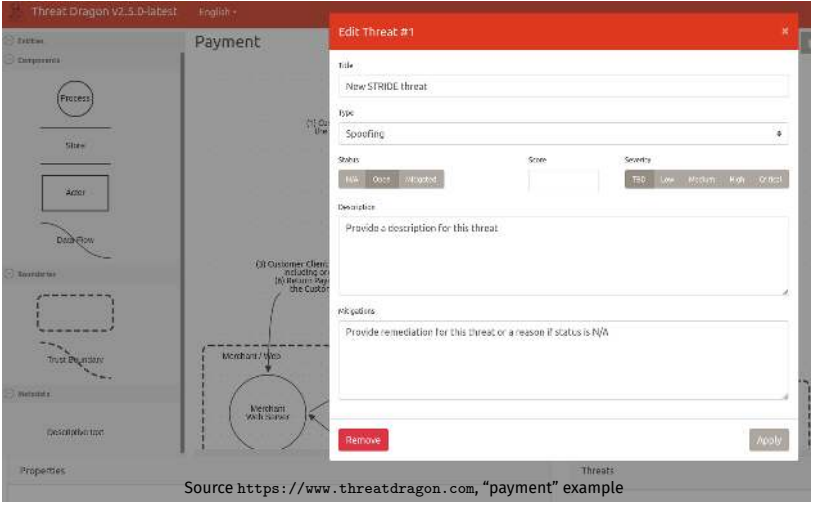
Threat modeling (1): Overview

- Workflow to identify weaknesses in Infrastructure
- Frameworks: STRIDE, PASTA, LINDDUN, (MITRE ATT&CK), ..
- Start with data flow diagrams (DFD), draw boundaries
- Identify threats and mitigations

cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

Threat modeling (2): OWASP Threat Dragon

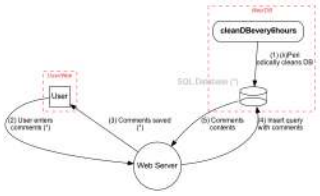
- GUI for DFDs, threats, mitigations and report creation



Source `https://www.threatdragon.com`, "payment" example

Threat modeling (3): OWASP pytm

- Infrastructure modeling in code
- Relationships and data flows as Python objects
- Graphs via `dot` et al




```python
from pytm.pytm import TM, Server, Datastore, Dataflow,

tm = TM("my test tm")
tm.description = "another test tm"
tm.isOrdered = True

User_Web = Boundary("User/Web")
Web_DB = Boundary("Web/DB")

user = Actor("User")
user.inBoundary = User_Web

web = Server("Web Server")
web.OS = "CloudOS"
web.isHardened = True
web.sourceCode = "server/web.cc"

db = Datastore("SQL Database (*)")
db.OS = "CentOS"
db.isHardened = False
db.inBoundary = Web_DB
db.isSql = True
db.inScope = False
db.sourceCode = "model/schema.sql"
```

Source `https://github.com/OWASP/pytm`

CycloneDX SBOM standard (1): ECMA and TC54

- CycloneDX v1.6 is an ECMA standard, ECMA-424
- ECMA hosts the Technical Committee TC54
  led by Steve Springett and Alyssa Wright

  TC54-TG1 Transparency exchange API (TEA) 

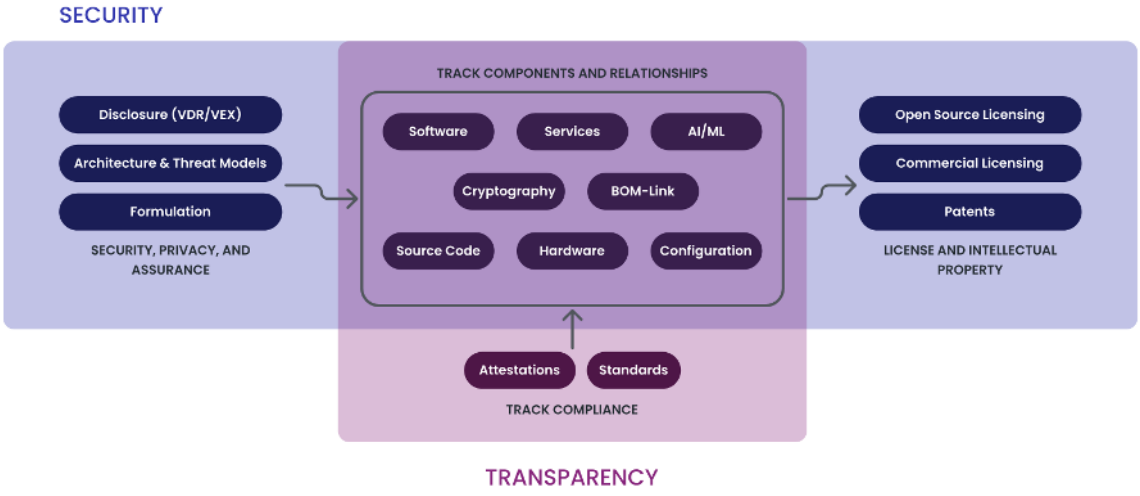
  TC54-TG2 Package URL (PURL)

  TC54-TG3 Common Lifecycle Enumeration (CLE)

  TC54-TG4 Contributing.yaml specification

German OWASP Day 2025

CycloneDX SBOM standard (2): Capabilities



Source: https://cyclonedx.org

Dependency-Track (1)

- Tracking of vulnerabilities after build
- Ingestion of SBOMs source of analysis
- Feeds in multiple streams of vulnerability reports (CVE..)
- Java monolith refactoring $\Rightarrow$ container-based **Hyades**
- Recently added CSAF capabilities

Dependency-Track (2)

Source: https://dependencytrack.org

OWASP Top 10 and Cheat Sheet series

- Top 10s: Web, API, Mobile, Kubernetes, ..
- The™ OWASP Top 10 now in 2025 version
- A lot of Cheatsheets for everything software security
  `cheatsheetseries.owasp.org`

🤓 Use them as best practices!

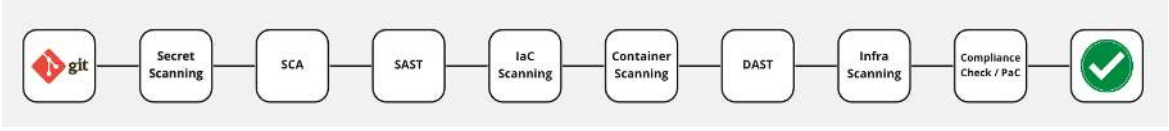
📋 Use them as checklists!

DevSecOps enforces policies

- **DevSecOps** integrates security into DevOps
- Goal: Enforce a **defined level of security and transparency** in software development process
- Perfect fit for compliant CRA processes! 🏆

DevSecOps enforces policies

- **DevSecOps** integrates security into DevOps
- Goal: Enforce a **defined level of security and transparency** in software development process
- Perfect fit for compliant CRA processes! 🏆



Source: https://owasp.org/www-project-devsecops-guideline/

Conclusion for manufacturers

- Software security posture for CRA? ⇒ **OWASP SAMM**!
- Risk analysis for infra & software? ⇒ **Threat modeling**!
- SSDLC? ⇒ **DevSecOps**! Top 10s! Cheatsheets!
- Documentation of software components? ⇒ **CycloneDX**!
- Vulnerability tracking? ⇒ **Dependency-Track**!

Thanks & good bye

Thank you all for attending this talk 🤓

Have a good travel home 🚆

📨 Feedback and questions → `dominik.pataky@owasp.org`

🔔 Feel free to ping me on LinkedIn or OWASP Slack

CRA structure (Regulation 2024/2847)

1. 130 recitals (dt. „Erwägungsgründe“)
2. 8 chapters with 71 articles
   - Art. 3: Definitions
   - Art. 13: Obligations of manufacturers
3. 8 annexes (dt. „Anhänge“)
   - Annex I: Essential cybersecurity requirements
   - Annex III: Important products with digital elements
   - Annex VII: Content of the technical documentation

Roles in the CRA (excerpt)

	German	English
1	Hersteller	**Manufacturer**
	Einführer	Importer
	Händler	Distributor
2	Verwalter quelloffener Software	Open Source **Stewards**
3	Marktüberwachungsbehörde	**Market Surveillance** Authority
4	Konformitätsbewertungsstelle	**Conformity Assessment** Body