

Cyber Resilience Act

Presentation description



11.03.2025

© ifm • Level of confidentiality: internal • Autor: Daniel Bitzer

Profile

- Daniel Bitzer B.Sc.
- 36 years old, married and one son
- Director Security Engineering @ ifm worldwide (6years)
- 12 years + experience in different IT areas
- Workgrouplead for ICS @ OI4

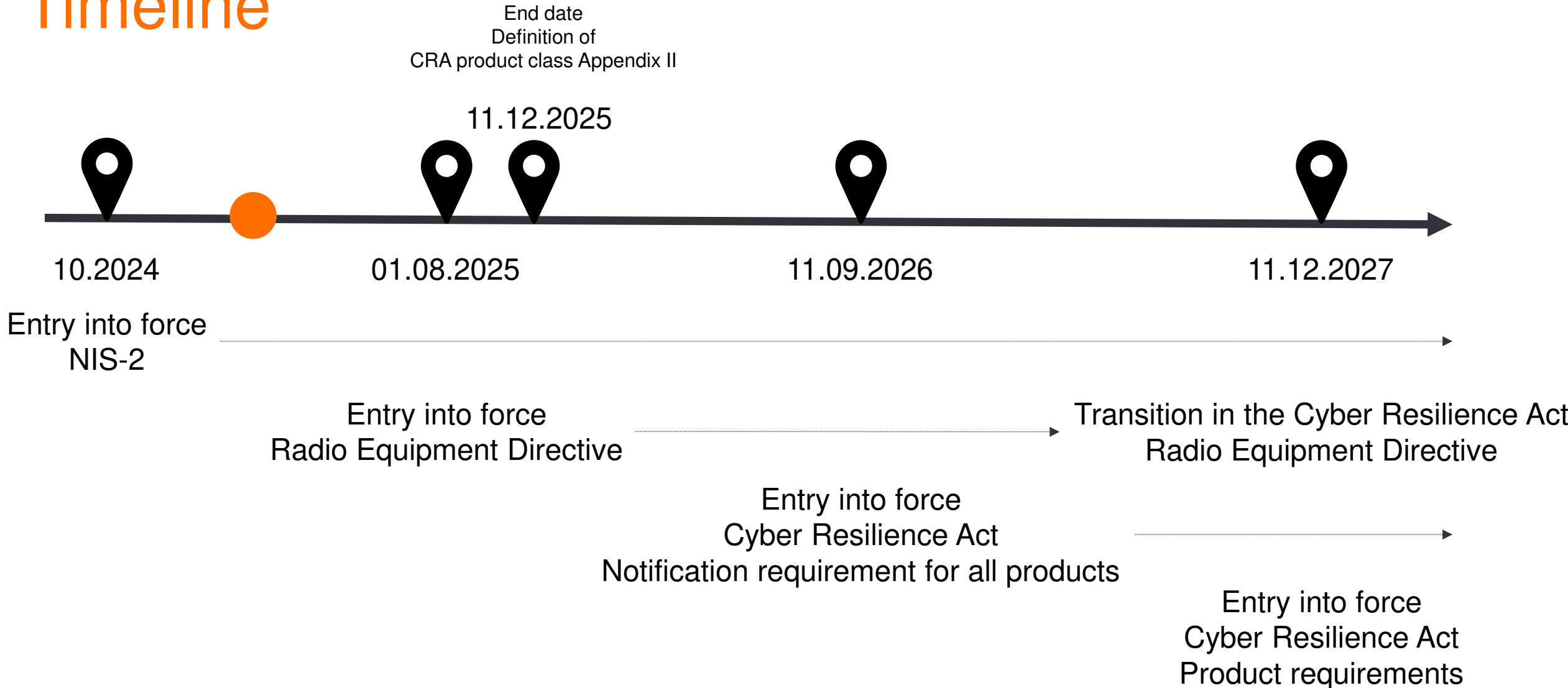


Cyber Resilience Act

Legal (EU) requirements



Cyber Resilience Act Timeline



General

- Devices with digital elements shall only be made available on the market if
 - a) they meet the essential cybersecurity requirements set out in Part I of Annex I and on condition that they are properly installed, maintained and used for their intended purpose or under reasonably foreseeable circumstances and, where applicable, the necessary security updates have been installed; and
 - b) the procedures established by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.

[Regulation - 2024/2847 - EN - EUR-Lex](#) -> Current version in different languages



Basic cybersecurity requirements

Part I Cybersecurity requirements related to the characteristics of products with digital elements (Annex 1)

Products with digital elements are designed, developed and manufactured in such a way that they ensure an appropriate level of cybersecurity in view of the risks, and ...

- *For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users. (Article 13, Sec. 2)*

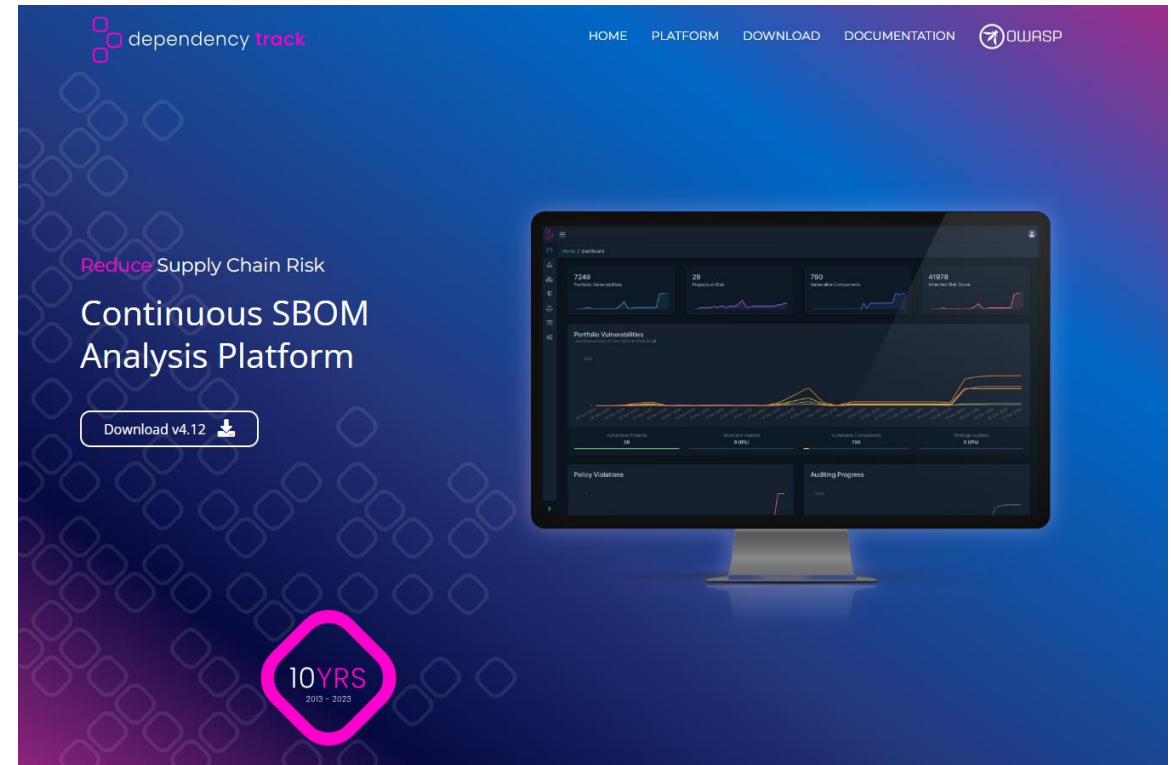
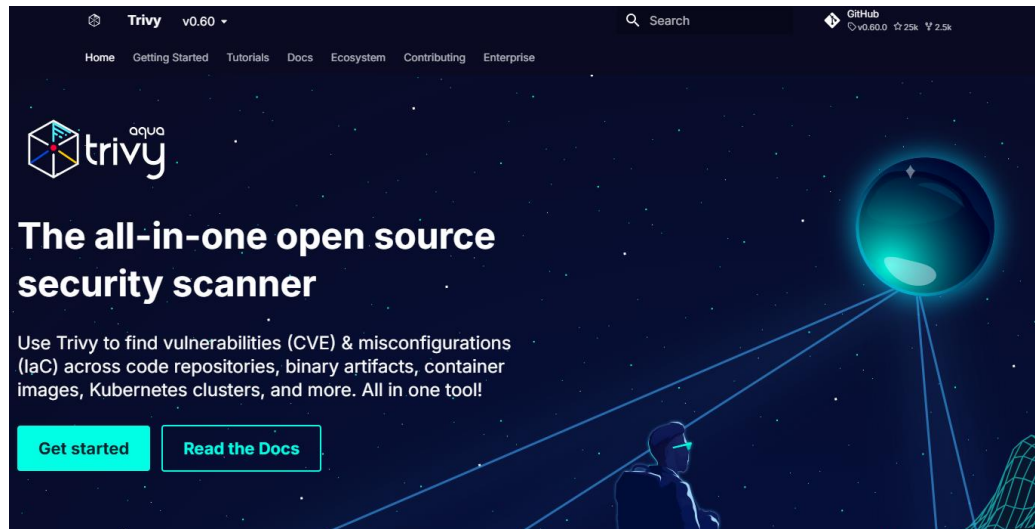
- [OWASP Threat Dragon | OWASP Foundation](#)

- **Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege**



Basic cybersecurity requirements

- *be made available on the market without known exploitable vulnerabilities; (Annex 1, Part 1, 2a)*



Basic cybersecurity requirements

- *ensure that vulnerabilities can be addressed through security updates ... (Annex 1, Part 1, 2c)*



Basic cybersecurity requirements

- *be made available on the market with a secure by default configuration (Annex 1, Part 1, 2b)*



Basic cybersecurity requirements

- *ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access (Annex 1, Part 1, 2d)*



Basic cybersecurity requirements

- *protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means (Annex 1, Part 1, 2e)*
- OI4 Members: Ecos, secunet & Campus Schwarzwald

Keyfactor/ejbca-ce

KEYFACTOR

EJBCA® – Open-source public key infrastructure (PKI) and certificate authority (CA) software.

28
Contributors

8
Issues

526
Discussions

691
Stars

115
Forks



Basic cybersecurity requirements

- *provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner (Annex 1, Part 1, 2m)*



Basic cybersecurity requirements

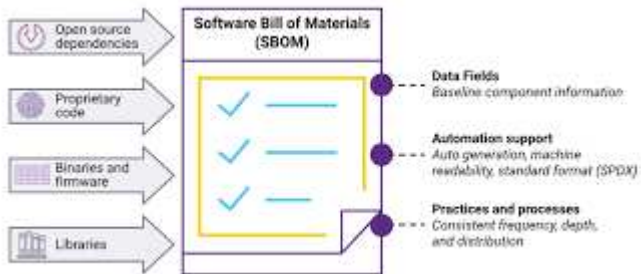
- Exception clause
- *[...] Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.*
Article 13 Section 4)



Requirements for the organization

Manufacturers of products with digital elements must,

- *identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products (Annex 1, Part 2, 1)*



Requirements for the organization

Manufacturers of products with digital elements must,

- *in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates; (Annex 1, Part 2, 2)*



Requirements for the organization

Manufacturers of products with digital elements must,

- *apply effective and regular tests and reviews of the security of the product with digital elements; (Annex 1, Part 2, 3)*



Requirements for the organization

Manufacturers of products with digital elements must,

- *once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch; (Annex 1, Part 2, 4)*

