Occtet the why, what and how

Martin von Willebrand, DoubleOpen Dr. Andreas Kotulla, Bitsea Michael Plagge, Eclipse Foundation





Occtet.eu

Open CyberSecurity Compliance Toolkit



• Problem: The Cyber Resilience Act (CRA) strengthens the cyber resilience of digital products

in the EU and places new obligations on manufacturers and retailers to ensure

product security throughout the entire life cycle. Managing open source correctly is

a complex and tedious task.

• Goal: Highly automated tools and processes to strengthen cyber security capabilities

and resources while reducing operating costs.

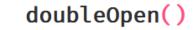
• Solution: Tool-based support to comply with CRA regulations, improve cyber security,

automate the handling of open source.

Sponsor: EU - Digital Europe Programm





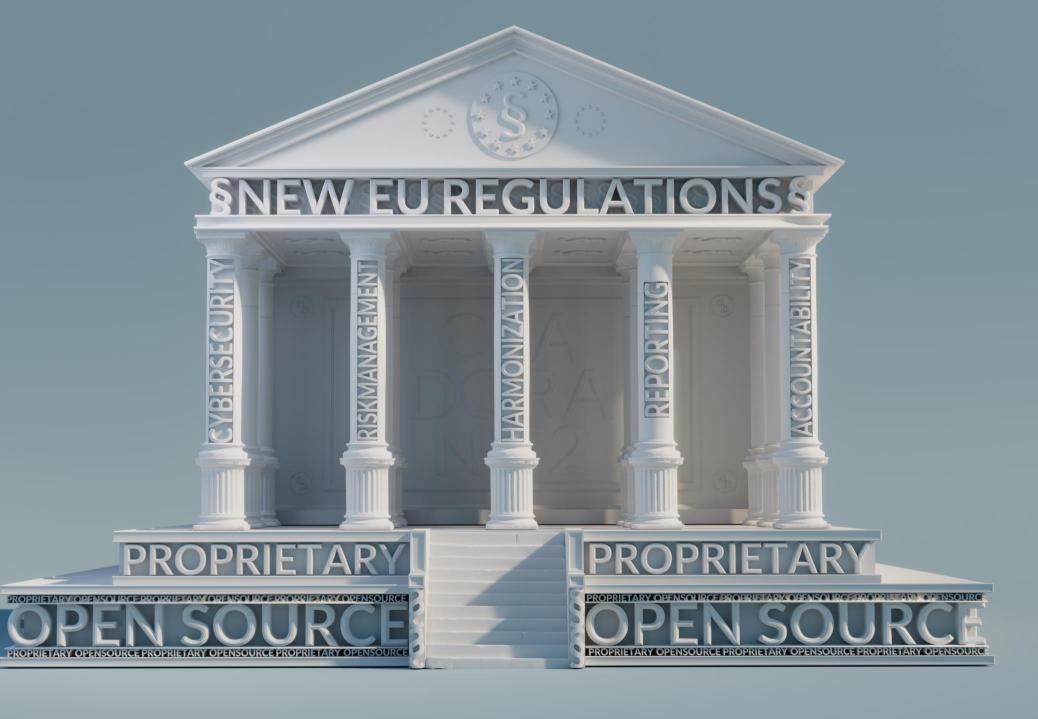












CRA Objectives

All cybersecurity risks are documented

Once sold, manufactures must ensure that for the expected product lifetime or for a period of five years, vulnerabilities are handled effectively

Security updates to be made available for at least five years



Cybersecurity is taken into account in planning, design, development, production, delivery and maintenance phase

Manufactures will have to report actively exploited vulnerabilities and incidents

Clear and understandable instructions for the use of products within digital elements

Obligations

- 1 Identify and document vulnerabilities and components, including in the form of machine-readable format
- Address vulnerabilities immediately, including by providing patches
- 3 Effective and regular testing and verification of safety
- Inform about fixed vulnerabilities, security holes, impact and severity after patching

- Introduce and enforce a policy of coordinated disclosure of security vulnerabilities
- 6 Measures to pass on information about potential vulnerabilities, including the provision of a contact address
- Mechanisms to distribute updates so that exploitable vulnerabilities are fixed/migrated in a timely manner
- Disseminate patches or updates to address security issues promptly and free of charge with notices



& OCCTET

Open CyberSecurity Compliance Toolkit



- ORT is a key building block in providing the open automation solution within OCCTET
 - Also Ort server, Double Open server
- Key partners re ORT in OCCTET: Bitsea, Double Open and Eclipse Foundation
- By participating to OCCTET, SMEs can influence work within OCCTET, and learn a lot of CRA requirements
 - Now is the best time! Occtet.eu:

















