Vulnir

Exploring Security Controls of Products based on CRA

5 March 2025

Angelo D'Amato
Founder

Meet your speaker

Angelo D'Amato
Founder / Cybersecurity Expert, Vulnir

Background

- With over fifteen years of experience, he is the subject matter expert for:
  - End-to-end cybersecurity assessments (Penetration testing)
  - Certifications (e.g., UL 2900, Common Criteria)
  - Regulatory compliance (e.g., Radio Equipment Directive, Cyber Resilience Act)
- I currently cover the role of rapporteur (*) for CRA as a CEN contractor within CEN/CLC/JTC 13/WG 9 for
  - PT2: Generic Security Requirements
  - PT3: Vulnerability handling requirements

* The European Union funds my activities within the STAN4CR project through the European Innovation Council and SMEs Executive Agency (EISMEA) under Grant Agreement No. 101196779.

Vulnir

Agenda

01 CRA context and work program overview

02 SDL Overview

03 Security controls Framework

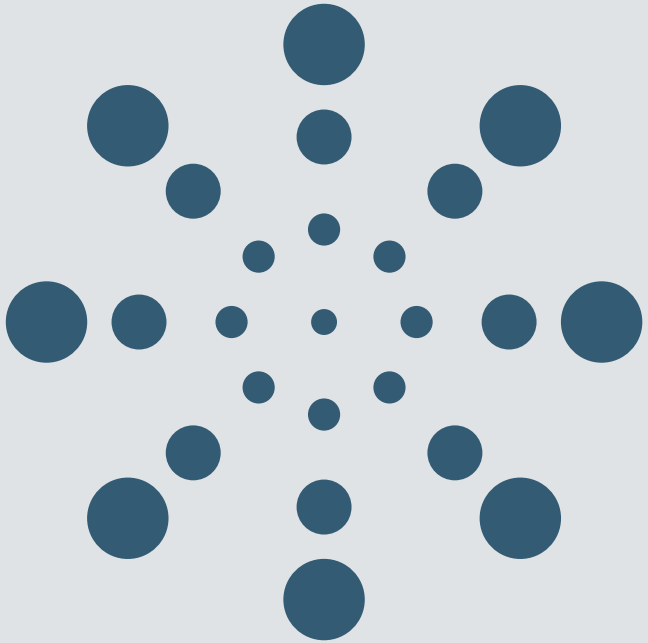
04 CRA’s Product Related essential requirements

05 Next steps

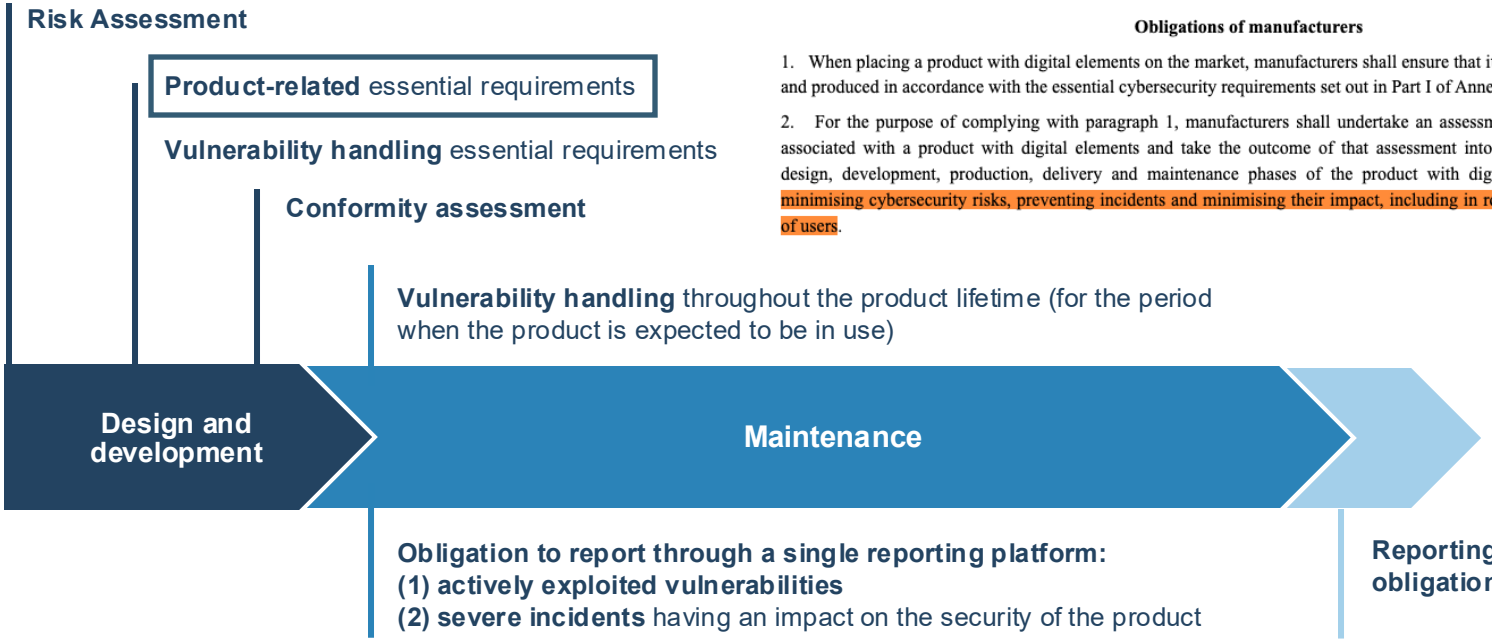
01

CRA context

CEN/CENELEC AND ETSI Work Program Overview



Obligations of manufacturers (CRA)



Article 13

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.

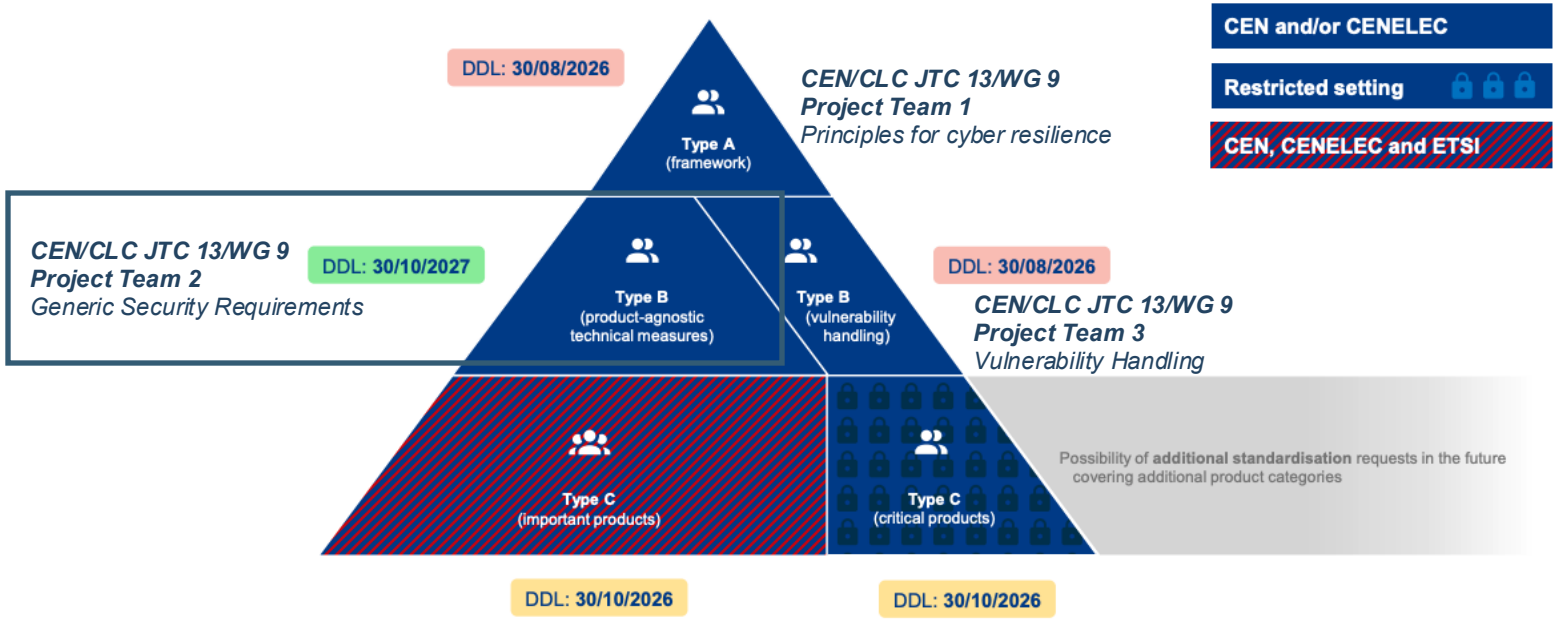
2. For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance 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.

Vulnir

***Source**: CEN/CENELEC Webinar on 10 March 2025 – Standardisation for the Cyber Resilience Act*

European Commission

CRA standardisation request in a nutshell



European Commission

Source: *Webinar on 26 February 2025 – Co-organised by Cyberstand.eu, HSbooster.eu & Stan4CR* *The Cyber Resilience Act and where we stand*

Reference: *CEN, CENELEC and ETSI Work Programme - Version: V 0.1 - Date: 2025-04-01 –* **source:** *CYBERSTAND*.

Vulnir

Exploring PT2 standard objectives

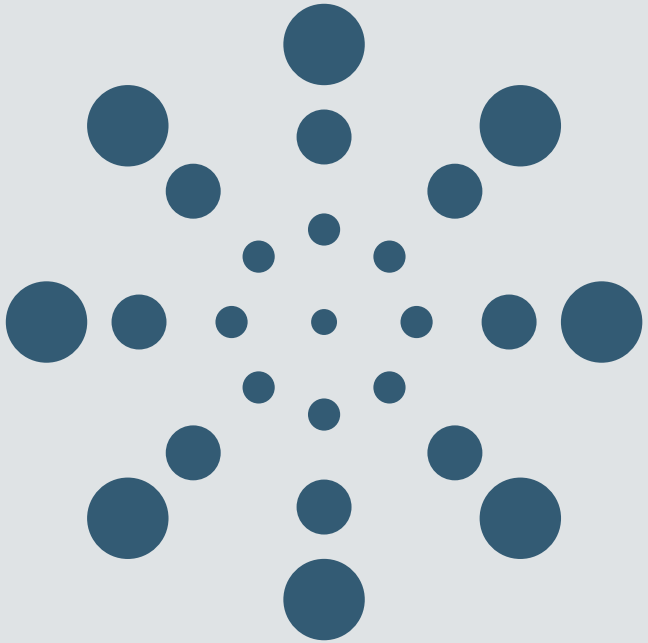
- The objective is to develop the horizontal standard for Annex I part II, the 2-14th deliverable of standardization request M/606 on Generic Security Requirements.
- The title of PT2 Standard is “Cybersecurity requirements for products with digital elements — Generic Security Requirements .”
- The PT2 is stated in the Standardization request M/606 to be published by 30/10/2027.
- The PT2 standard is product-centric—a collection of security controls and related assessment criteria.
  - It should reuse security controls already included in EN 18031-X:2024.
  - Wherever relevant, the requested horizontal standards shall include provisions on secure software development.
  - It should guide verticals and products that fall in the default category.
- PT2 standard will serve as a security control catalogue and will include at least provisions related to the
  - Security problem definition
  - Security objectives
  - Technical specification of security requirements,
  - Assessment methodology.

***Reference**: C(2025)618 – Standardisation request M/606*

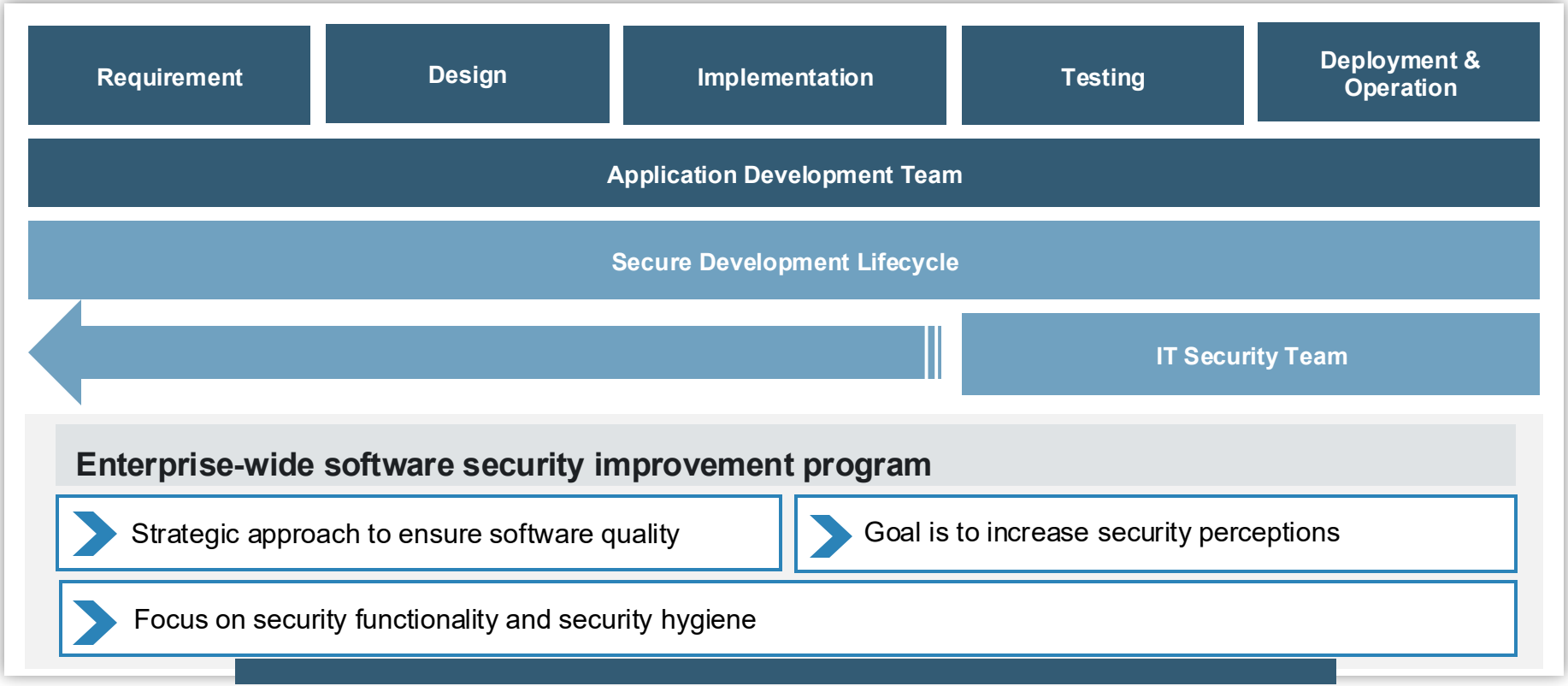
02

SDL Overview

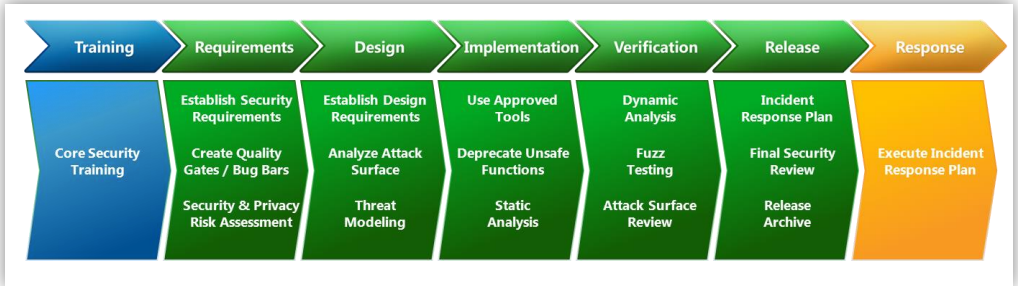
Secure Development Lifecycle



State of Practice: Integrated Security



Multiple SDL options



Microsoft SDL

Cisco SDL

OWASP SAMM

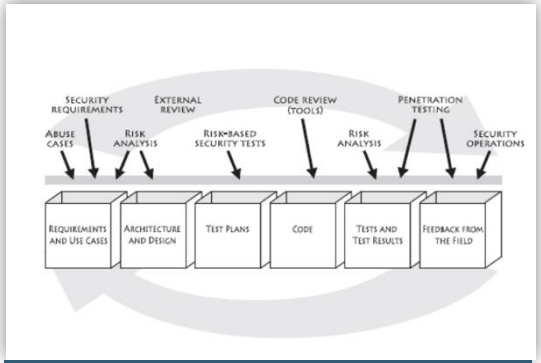
BSIMM

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SP 800-64

PCI SLC

ISO/IEC 27034



McGraw's TouchPoint

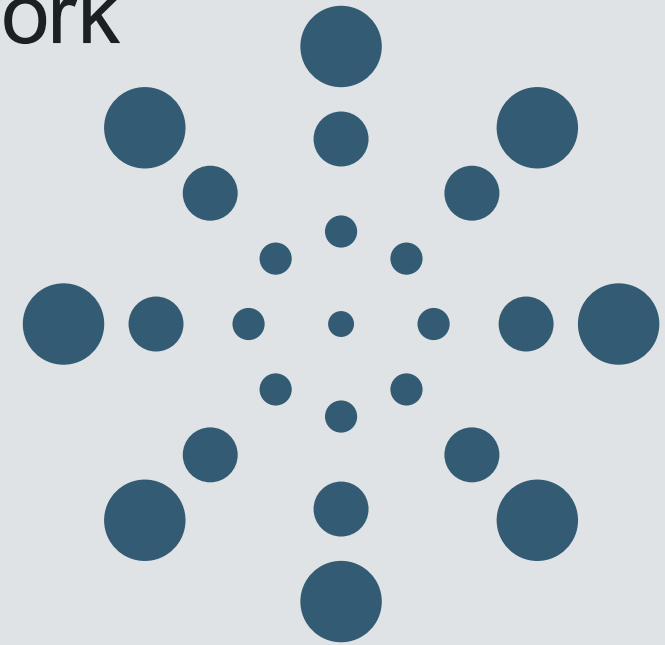
Software Engineering Institute | Carnegie Mellon University

Software Engineering Institute

And many others

03

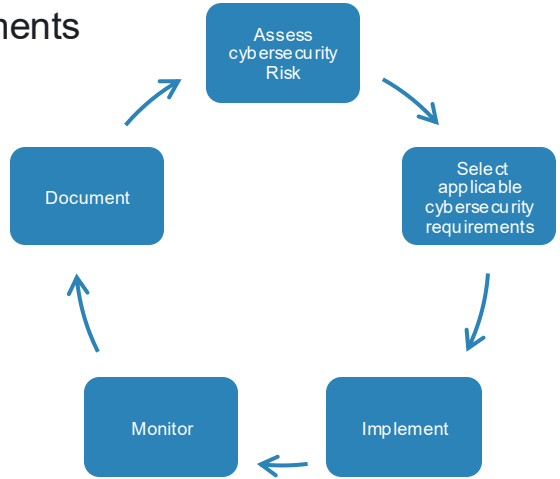
Security controls Framework

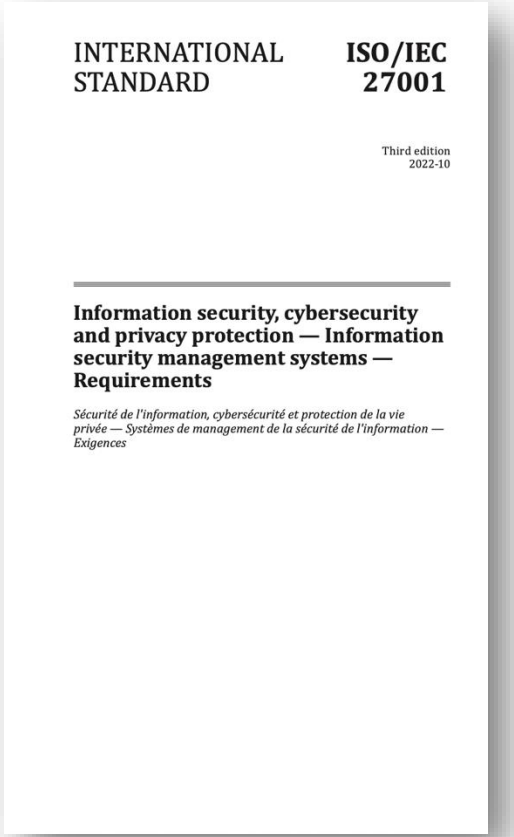


ISMS

ISO 27001 is a security standard that helps protect information assets by establishing an information security management system

- Identifying information security requirements
- Assessing information security risks
- Treating information security risks
- Selecting and implementing controls
- Monitor, maintain, and improve the effectiveness of the ISMS
- Continual improvement




INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

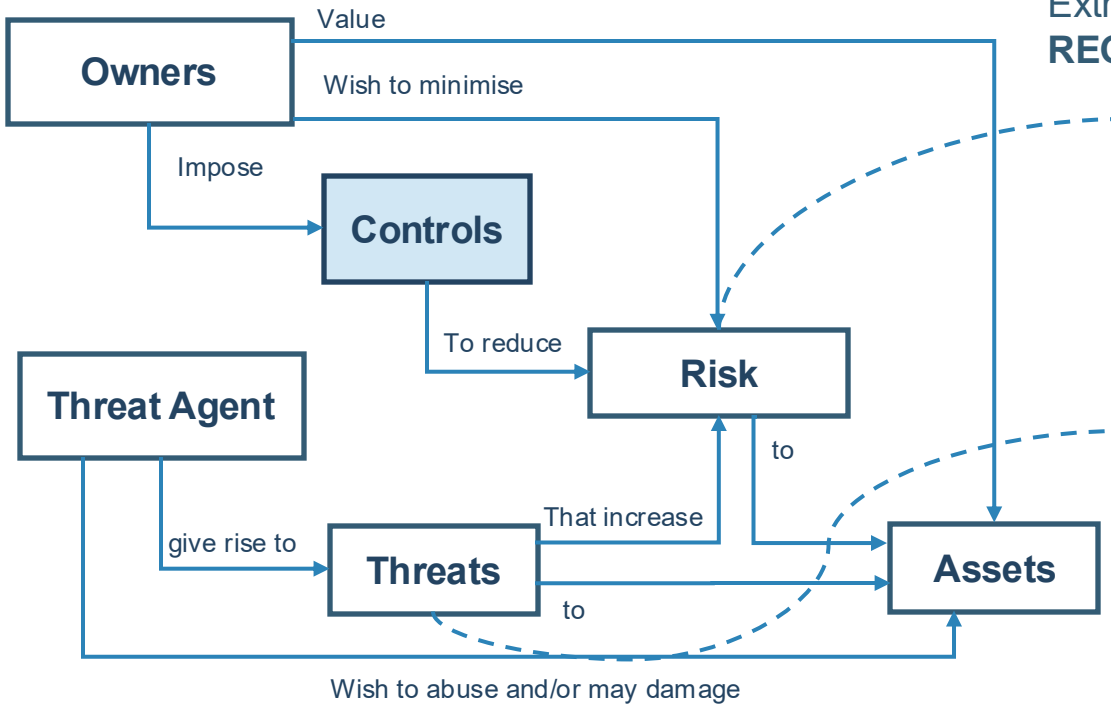
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Vulnir

***Source**: Cyber Resilience Act Requirements Standards Mapping - [Joint Research Centre & ENISA Joint Analysis]*

Security concepts and relationships



Extract from:
REGULATION (EU) 2024/2847 (CRA)

- (37) '**cybersecurity risk**' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

….

- (40) **'vulnerability'** means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat;

….

***Source**: CC:2022 Part 1: Introduction and general model (CCMB-2022-11-001) – Page 37 - Figure 1 — Security concepts and relationships*

Type of Controls

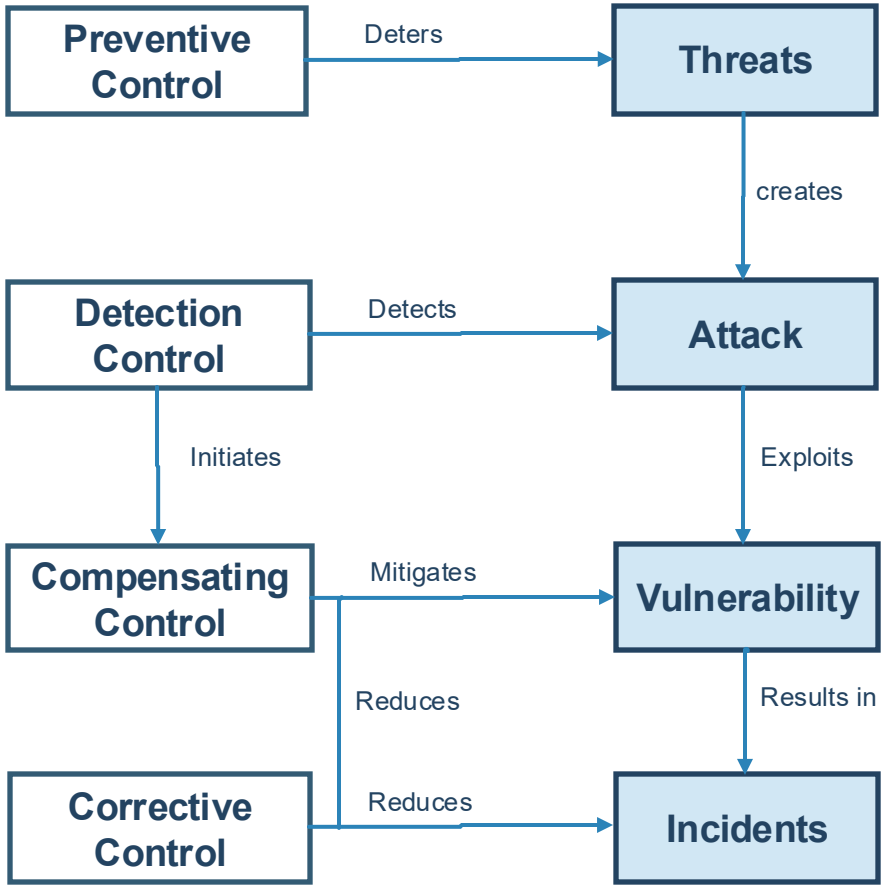
Controls are measures taken to detect, prevent, and mitigate the risks associated with the threats a system faces

Control type

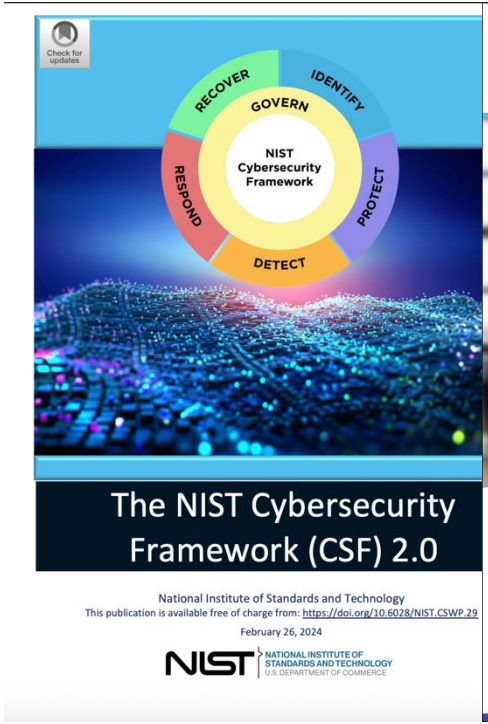
- Administrative
- Technical
- Physical

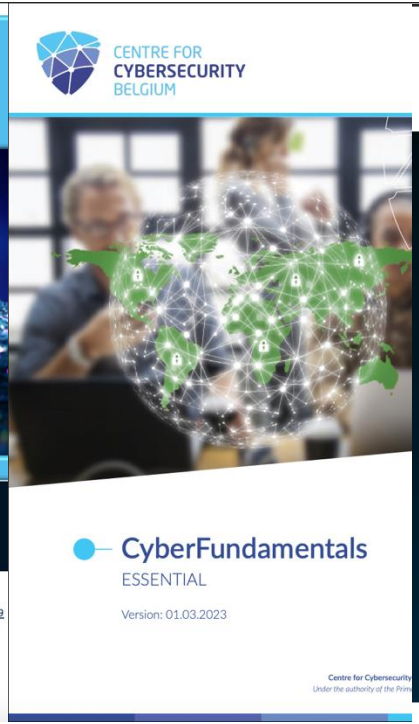
Control functions

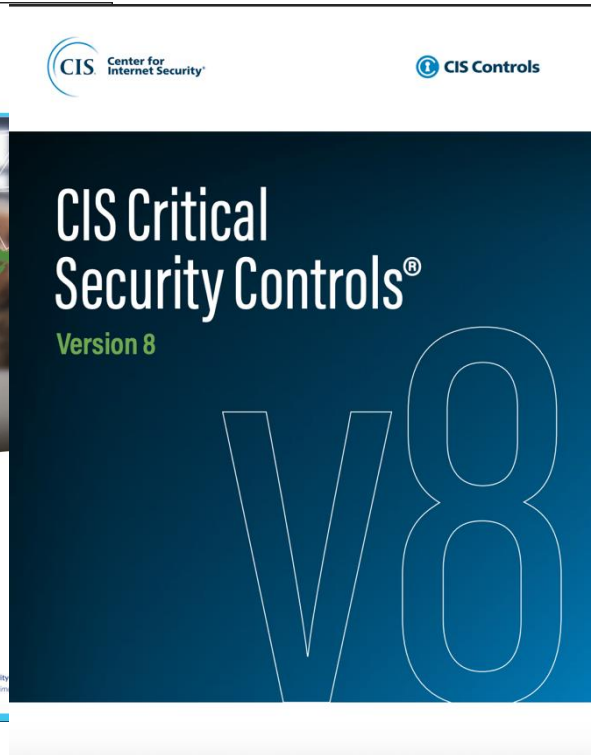
- Preventive (deterrent)
- Detective
- Corrective (recovery)
- Additional: Compensating



Example of security frameworks



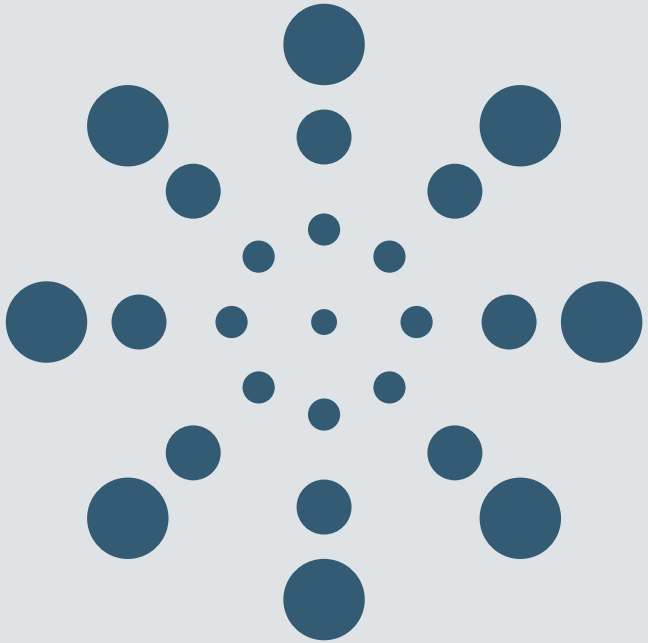




04

CRA

Product Related essential requirements



Role of essential requirements

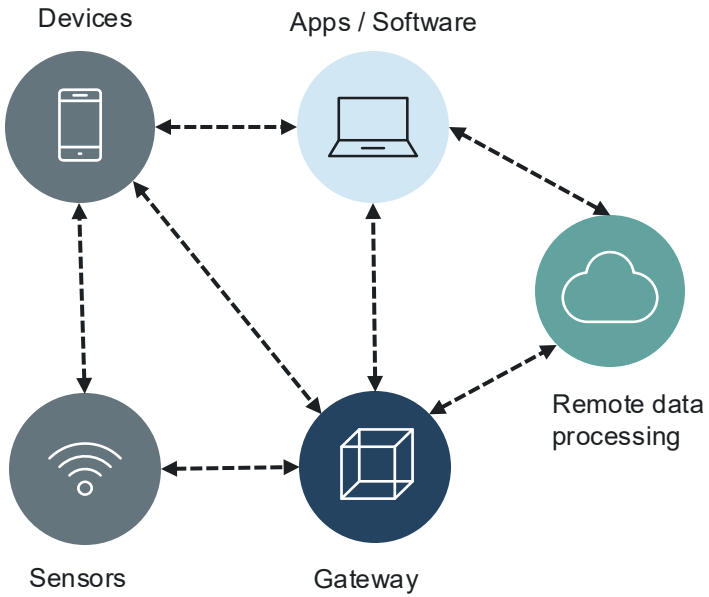
Mirai IoT Botnet, Aug 2016

- The first ever botnet of Internet of Things devices
- **Root causes**:
  - Weak default configuration (default password)
- **Effect:**
  - High-profile websites and services that relied on Dyn for DNS resolution, including Twitter, Reddit, Netflix, Airbnb, Amazon were disrupted
- **Highlighted the importance of:**
  - Secure by default configuration

Log4j (Log4Shell), Dec 2021

- The first ever botnet of Internet of Things devices
- **Root cause**:
  - JNDI lookups within log messages without sufficient validation or sanitization
- **Effect:**
  - Its impact stemmed from the ubiquitous nature of the vulnerable Log4j library and the severe nature of the vulnerability itself (Remote Code Execution).
- **Highlighted the importance of:**
  - Security updates / SBOM

Overview of the PT2's essential requirements

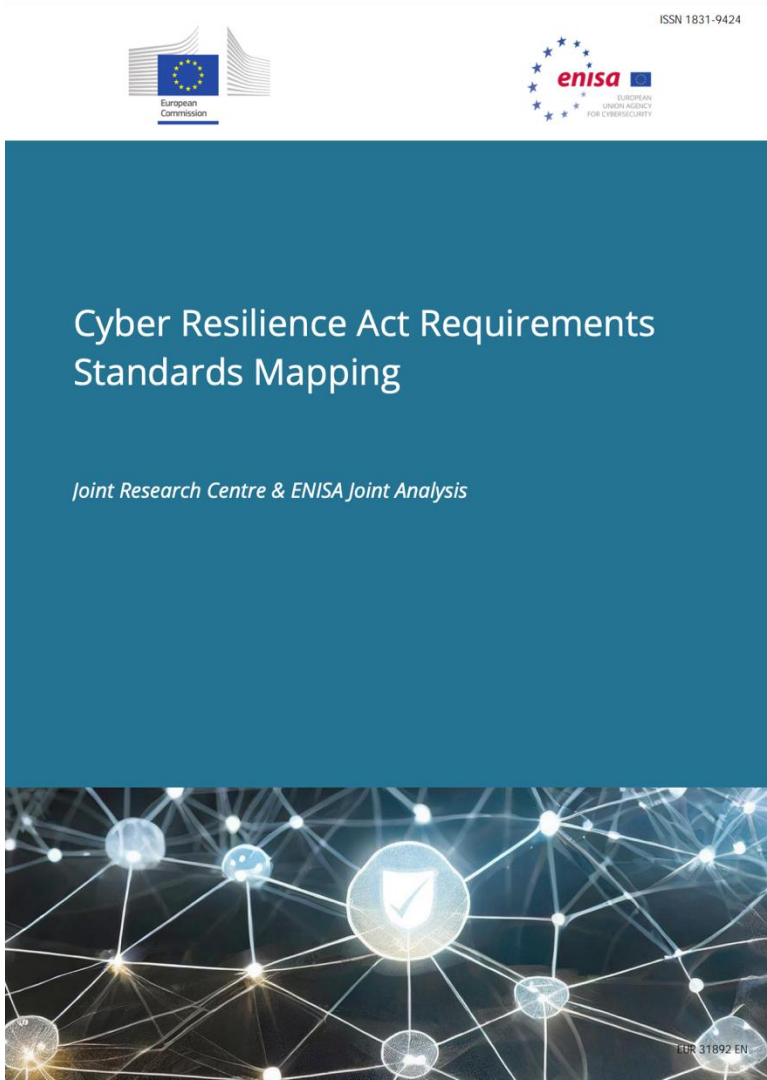


- ❑ Ensure that products with digital elements **hardware and software** placed on the EU market **have fewer cybersecurity vulnerabilities**.
- ❑ **Better protection** for consumers, supply chains, organisations, businesses, and IT Infrastructure

- No known exploitable vulnerabilities
- Secure by default configuration
- Security updates
- Authorized access
- Confidentiality protection
- Integrity protection
- Data minimization
- Availability protection
- Minimize negative impact
- Attack surface minimization
- Reduce the impact of an incident
- Logging and monitoring controls
- Secure deletion mechanisms

Gaps identified

- (1) Risk assessment not specific to the system or product design
- (2) Find the right balance in the assessment for the no known exploitable vulnerabilities (Common Criteria vs ETSI EN 303 645)
- (3 a) The particular use of non-erasable memories for configuration management is not covered.
- (3 f) More detailed guidance on the implementation of availability principles for generic user products
- (3 h) Lack of concrete requirements targeting the attack surface minimisation
- (3 i) some aspects of defence in depth, sandboxing, and certain mitigation techniques might not be explicitly covered by the selected standards
- (3 k) Do not explicitly cover the requirement of notifying users about the availability of updates.

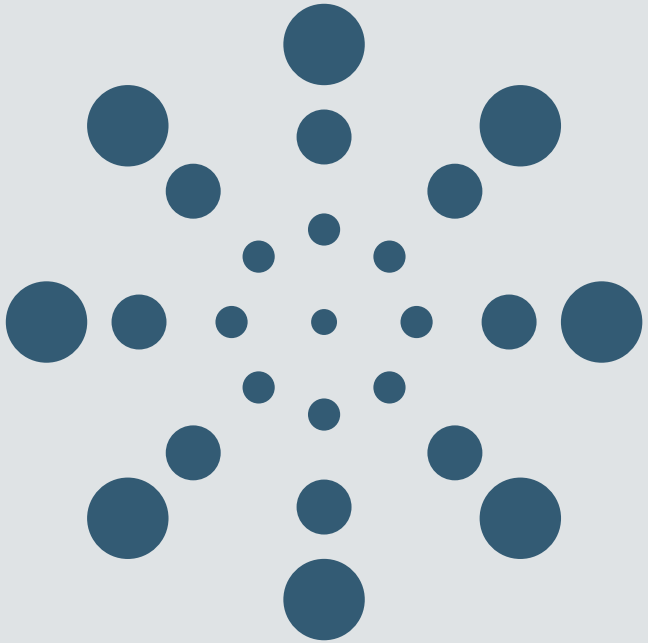


Vulnir

***Source**: Cyber Resilience Act Requirements Standards Mapping - [Joint Research Centre & ENISA Joint Analysis]*

05

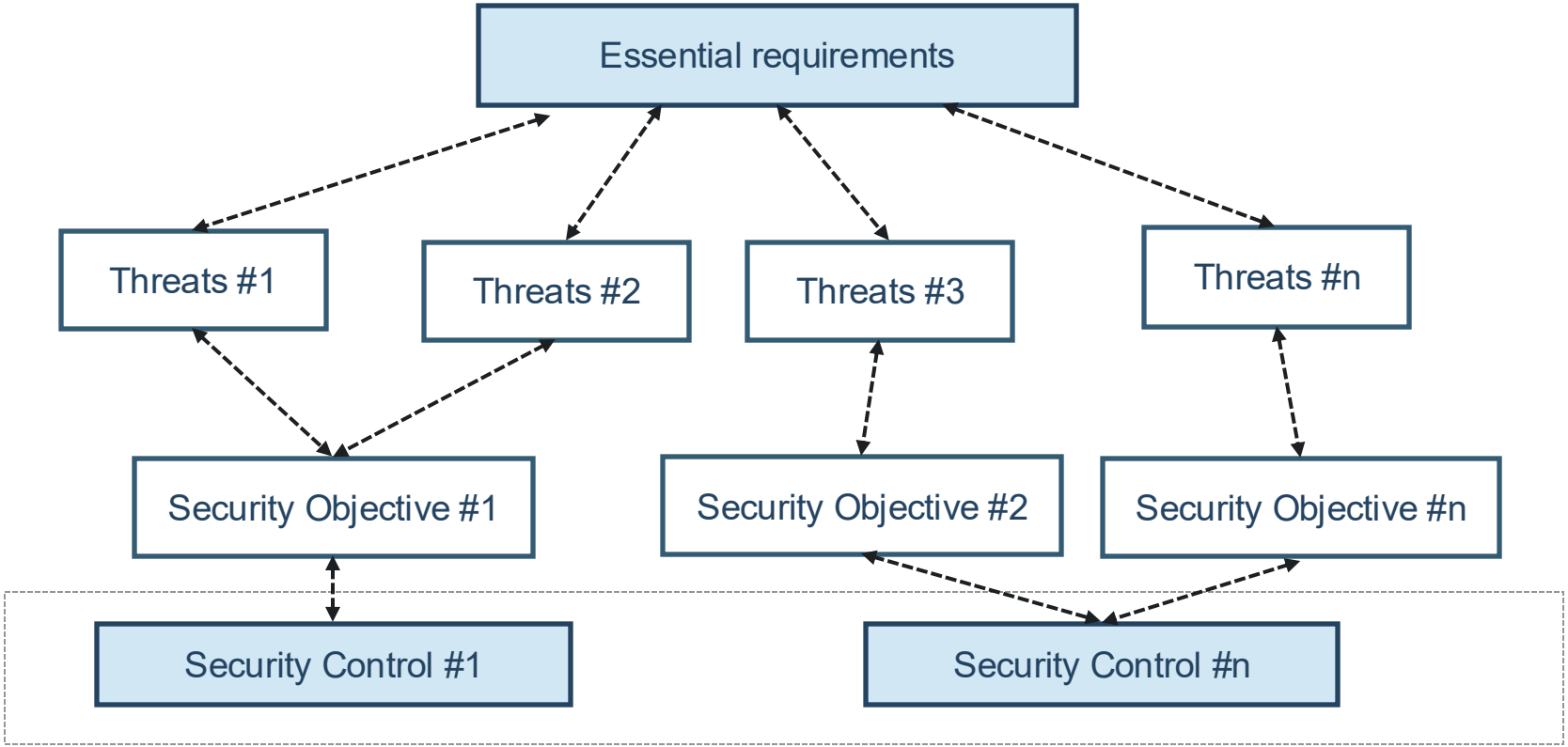
Next steps



Standard landscape as a potential reference

- Information Security Management
  - ISO/IEC 27001, ISO/IEC 27002
- Product and System Specific Security Requirements
  - ETSI EN 303 645
  - EN IEC 62443-4-2
  - EN 18031-1, EN 18031-2, EN 18031-3
- Security Evaluation and Testing
  - ISO/IEC 18045
  - EN 17640
- IoT Specifics (Architecture and Overarching Security)
  - ISO/IEC 30141
  - ISO/IEC 27400
- Privacy assurance
  - ETSI TS 103 485
- Security Throughout the Product Lifecycle
  - ISO/IEC TR 6114

Technical Report as a base for the PT2 standard



Thank you

VULNIR.com

info@vulnir.com