# TOWARDS CYBERSECURITY ACT: A SURVEY ON IOT EVALUATION FRAMEWORKS

**Maxime Puys**, Jean-Pierre Krimm, Raphaël Collado

Univ. Grenoble Alpes, CEA, LETI, DSYS, Grenoble, France

Firstname.Name@cea.fr

SECURWARE 2020, Nov. 21, 2020 to Nov. 25, 2020 - Valencia, Spain

# ABOUT ME

- Maxime Puys
- Research Engineer at CEA-LETI, Grenoble, France

- Ph.D in Cybersecurity (2018)
  - University Grenoble Alpes, France

- Research Topics:
  - Cybersecurity of industrial systems
  - Cryptographic protocol verification
  - Smart-cards security against fault attacks
  - Formal methods for cybersecurity
  - Certification process and frameworks

# CONTEXT

- Cybersecurity Act officially adopted by EU on 7th of June 2019

  → Includes the definition of a European cybersecurity certification framework

- Cybersecurity certification framework:
  - Delivered certificates mutually recognized among European countries
  - Encourage/enforce the use of certification throughout the EU

- Three certification levels are considered:
  - **Basic level → non-critical, consumer objects;**
  - Substantial level → median risk;
  - High level → critical solutions.

- Basic level is tricky due to the very wide range of products.

- Already existing framework for each levels:
  - Which one is picked? New one from scratch?

CONFIDENTIEL

# OUTLINE

1. Survey/comparison of existing evaluation frameworks considered for basic level
2. A unified IoT evaluation framework for basic level
3. Conclusion

CONFIDENTIEL

# OUTLINE

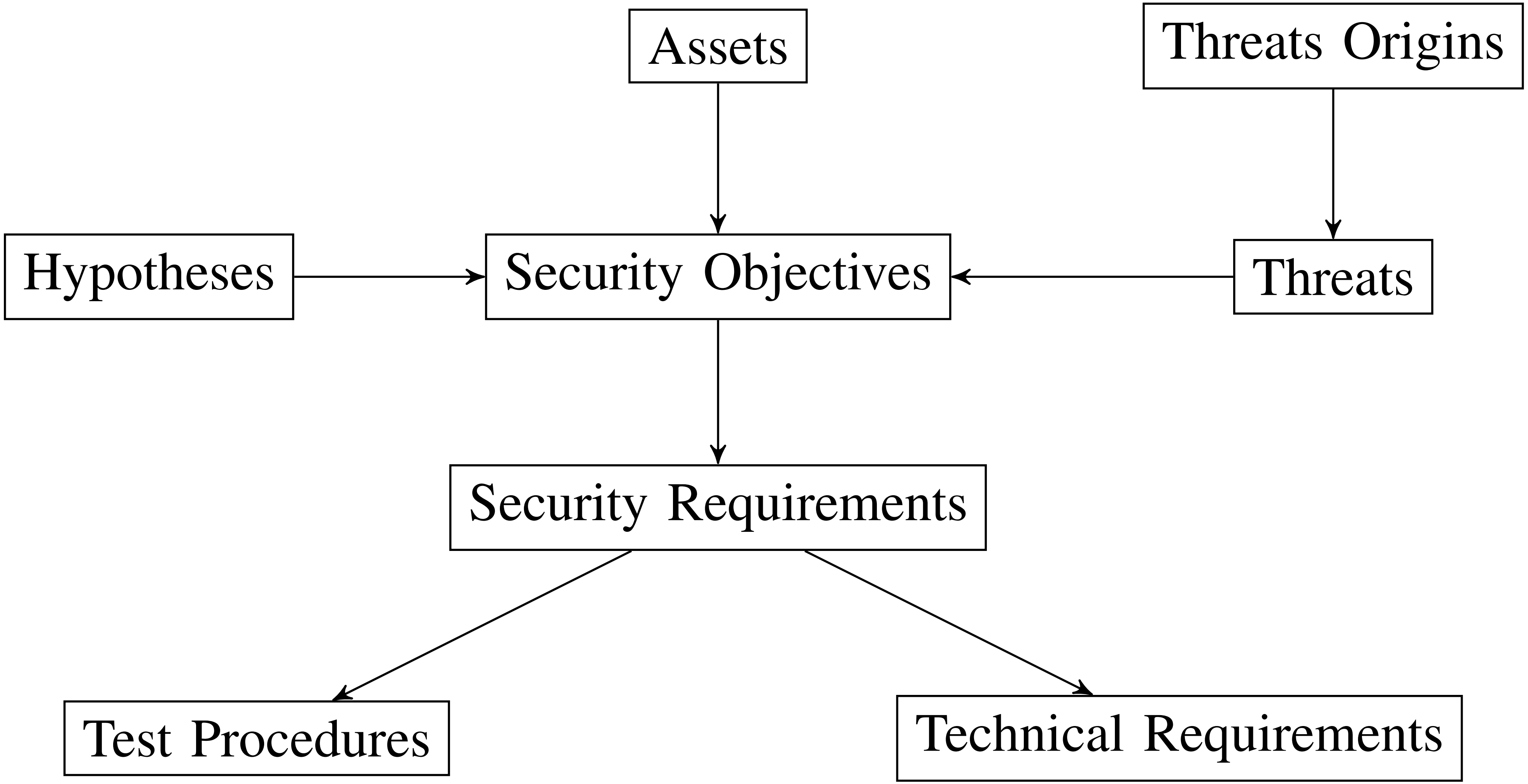
1. Survey/comparison of existing evaluation frameworks considered for basic level

2. A unified IoT evaluation framework for basic level

3. Conclusion

CONFIDENTIEL

# PRODUCT EVALUATION STRUCTURE



Assets

Threats Origins

Hypotheses

Security Objectives

Threats

Security Requirements

Test Procedures

Technical Requirements

CONFIDENTIEL

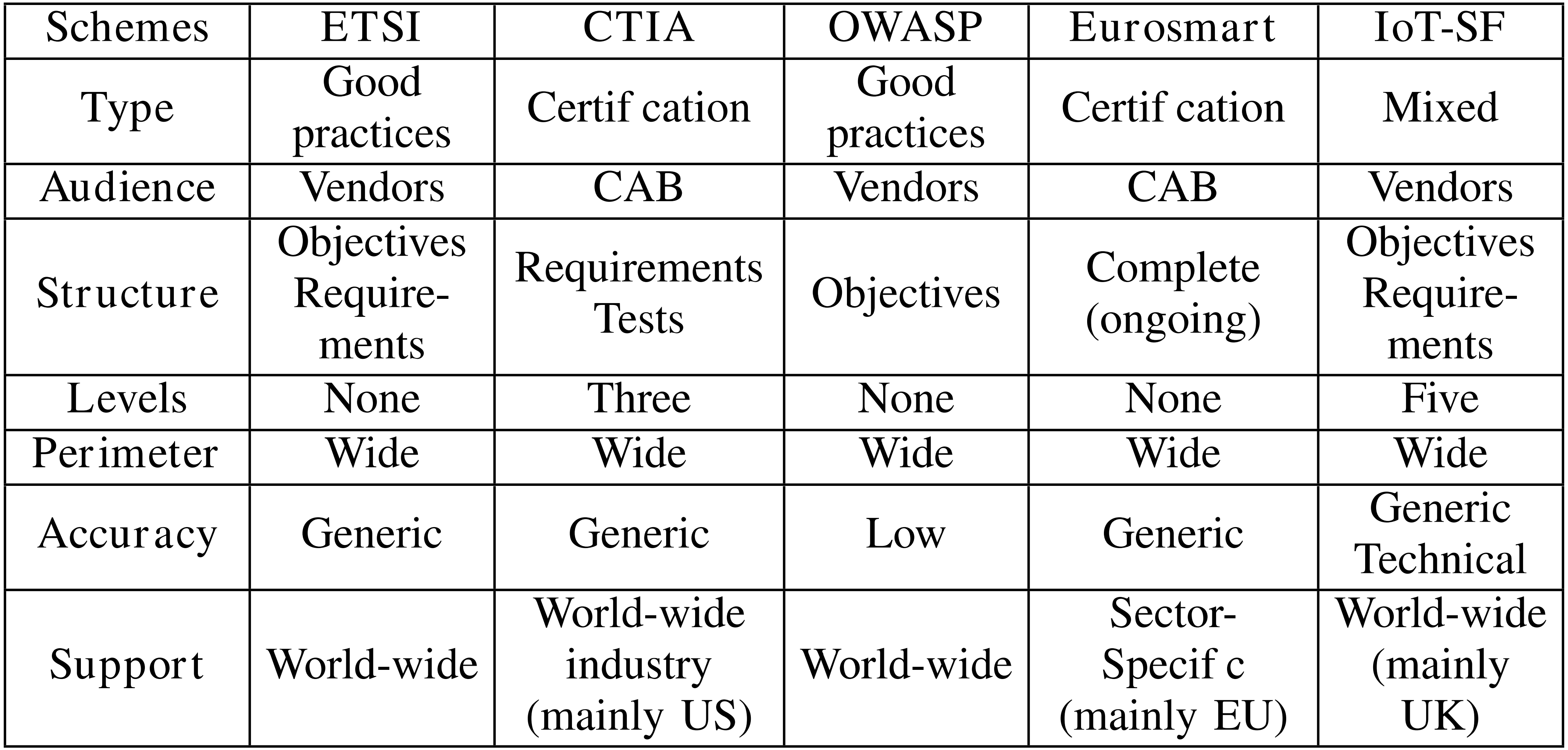
# EXISTING FRAMEWORKS 1/2

- Comparison criteria (might be subjective /!\):
  - **Type of document:** Main purpose of the document (evaluation/certification, good practices, etc);
  - **Targeted audience:** CAB, CISO, CTO, Developers, etc;
  - **Structure of the document:** Part of the previous structure covered by the scheme;
  - **Split in different security levels**: If the scheme proposes different inner security levels;
  - **Technical perimeter:** Technical cybersecurity topics covered (HW, SW, web, crypto, etc);
  - **Level of accuracy of the requirements:** Precision of the requirements provided by the scheme;
  - **Support from the community/industry.**

- Existing framworks dealing with IoT:
  - ETSI-EN-303-645
  - CTIA Cybersecurity Certification Test Plan for IoT Devices
  - OWASP IoT Top Ten
  - Eurosmart IoT Device Certification Scheme
  - IoT Security Foundation Security Compliance Framework

CONFIDENTIEL

# EXISTING FRAMEWORKS 2/2



| Schemes | ETSI | CTIA | OWASP | Eurosmart | IoT-SF |
|---|---|---|---|---|---|
| Type | Good practices | Certification | Good practices | Certification | Mixed |
| Audience | Vendors | CAB | Vendors | CAB | Vendors |
| Structure | Objectives<br>Requirements | Requirements<br>Tests | Objectives | Complete (ongoing) | Objectives<br>Requirements |
| Levels | None | Three | None | None | Five |
| Perimeter | Wide | Wide | Wide | Wide | Wide |
| Accuracy | Generic | Generic | Low | Generic | Generic<br>Technical |
| Support | World-wide | World-wide industry (mainly US) | World-wide | Sector-Specific (mainly EU) | World-wide (mainly UK) |

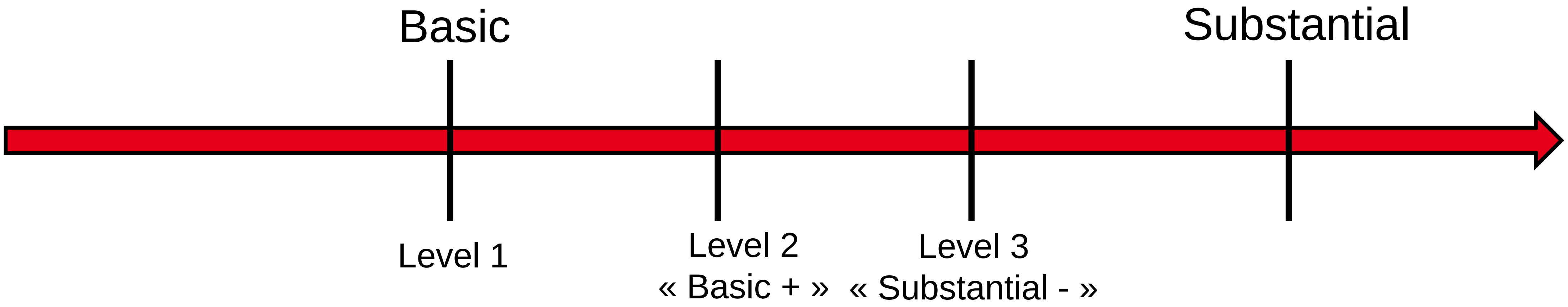
# A UNIFIED EVALUATION FRAMEWORK FOR CONSUMER IOT

# GENERAL IDEA

- Created during on-going discussions about the final scheme
  - Goal: Preparation of CABs before final scheme choice

- **Rather than trying to predict which existing scheme to implement, find a middle-gound.**

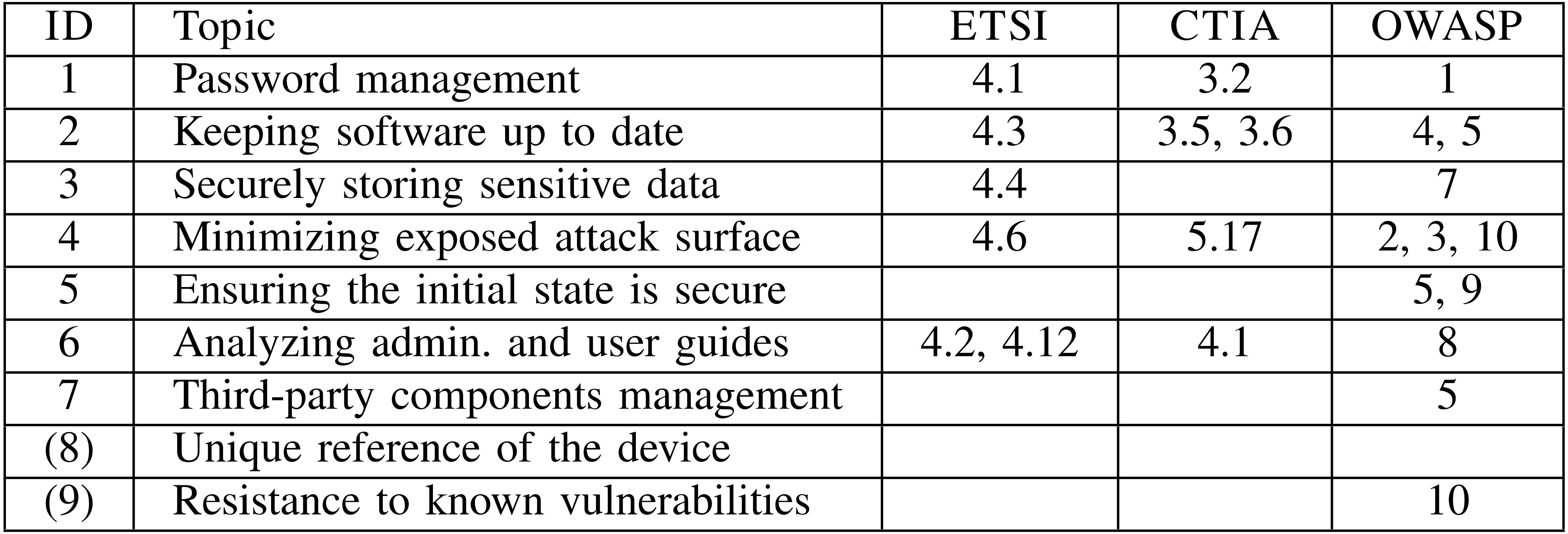
- Marketing requirement: 3 inner levels



- Target of Evaluation (TOE): Product (HW/SW) + documentations
  - Simply said: what the custommer has in hands

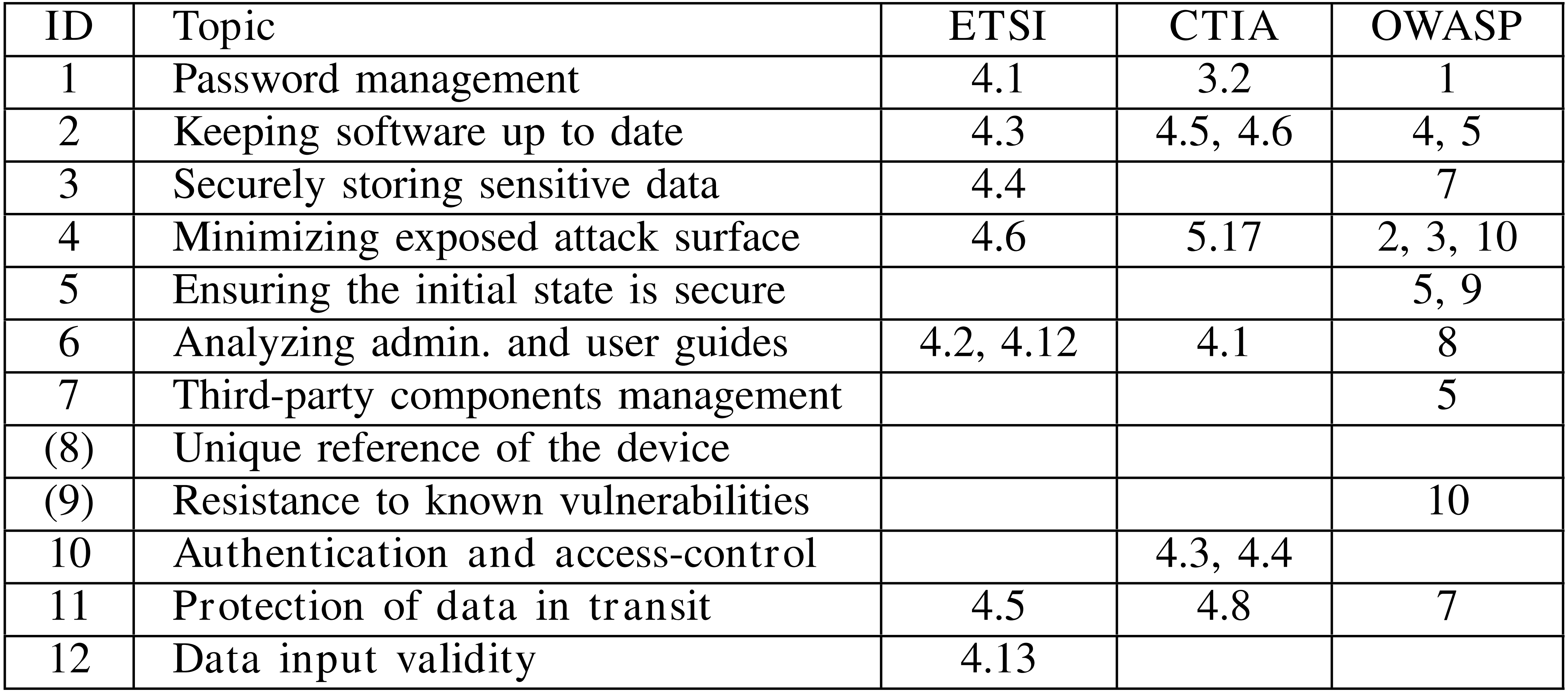
CONFIDENTIEL

# LEVEL 1



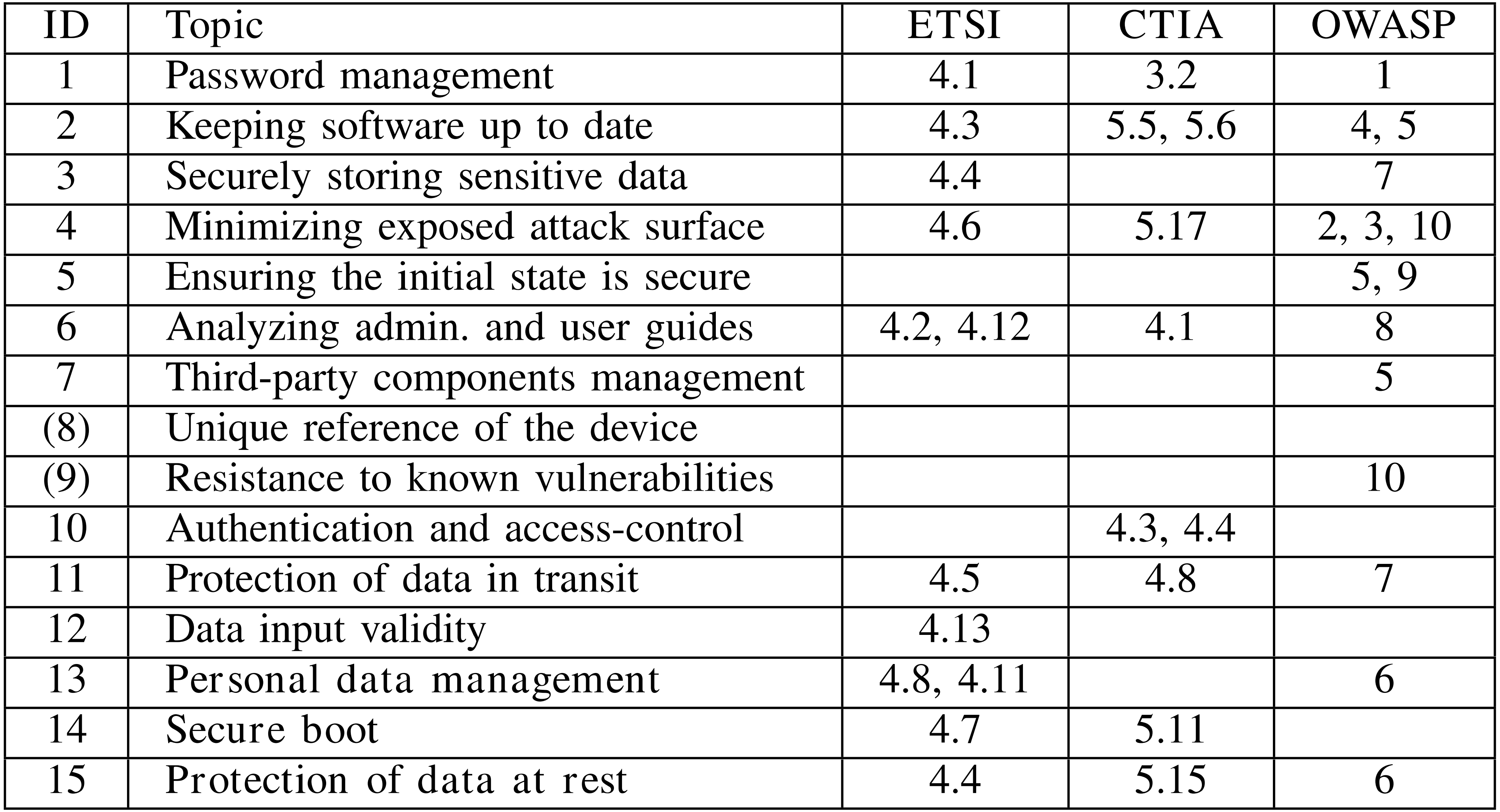
| ID | Topic | ETSI | CTIA | OWASP |
|---|---|---|---|---|
| 1 | Password management | 4.1 | 3.2 | 1 |
| 2 | Keeping software up to date | 4.3 | 3.5, 3.6 | 4, 5 |
| 3 | Securely storing sensitive data | 4.4 |  | 7 |
| 4 | Minimizing exposed attack surface | 4.6 | 5.17 | 2, 3, 10 |
| 5 | Ensuring the initial state is secure |  |  | 5, 9 |
| 6 | Analyzing admin. and user guides | 4.2, 4.12 | 4.1 | 8 |
| 7 | Third-party components management |  |  | 5 |
| (8) | Unique reference of the device |  |  |  |
| (9) | Resistance to known vulnerabilities |  |  | 10 |

# LEVEL 2



| ID | Topic | ETSI | CTIA | OWASP |
|---|---|---|---|---|
| 1 | Password management | 4.1 | 3.2 | 1 |
| 2 | Keeping software up to date | 4.3 | 4.5, 4.6 | 4, 5 |
| 3 | Securely storing sensitive data | 4.4 |  | 7 |
| 4 | Minimizing exposed attack surface | 4.6 | 5.17 | 2, 3, 10 |
| 5 | Ensuring the initial state is secure |  |  | 5, 9 |
| 6 | Analyzing admin. and user guides | 4.2, 4.12 | 4.1 | 8 |
| 7 | Third-party components management |  |  | 5 |
| (8) | Unique reference of the device |  |  |  |
| (9) | Resistance to known vulnerabilities |  |  | 10 |
| 10 | Authentication and access-control |  | 4.3, 4.4 |  |
| 11 | Protection of data in transit | 4.5 | 4.8 | 7 |
| 12 | Data input validity | 4.13 |  |  |

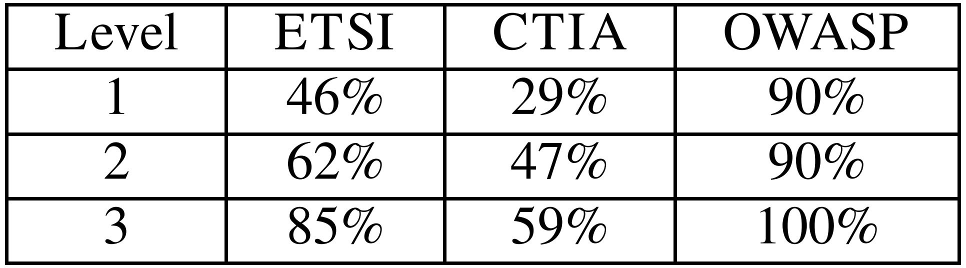
# LEVEL 3



| ID | Topic | ETSI | CTIA | OWASP |
|---|---|---|---|---|
| 1 | Password management | 4.1 | 3.2 | 1 |
| 2 | Keeping software up to date | 4.3 | 5.5, 5.6 | 4, 5 |
| 3 | Securely storing sensitive data | 4.4 |  | 7 |
| 4 | Minimizing exposed attack surface | 4.6 | 5.17 | 2, 3, 10 |
| 5 | Ensuring the initial state is secure |  |  | 5, 9 |
| 6 | Analyzing admin. and user guides | 4.2, 4.12 | 4.1 | 8 |
| 7 | Third-party components management |  |  | 5 |
| (8) | Unique reference of the device |  |  |  |
| (9) | Resistance to known vulnerabilities |  |  | 10 |
| 10 | Authentication and access-control |  | 4.3, 4.4 |  |
| 11 | Protection of data in transit | 4.5 | 4.8 | 7 |
| 12 | Data input validity | 4.13 |  |  |
| 13 | Personal data management | 4.8, 4.11 |  | 6 |
| 14 | Secure boot | 4.7 | 5.11 |  |
| 15 | Protection of data at rest | 4.4 | 5.15 | 6 |

# CONCLUSION

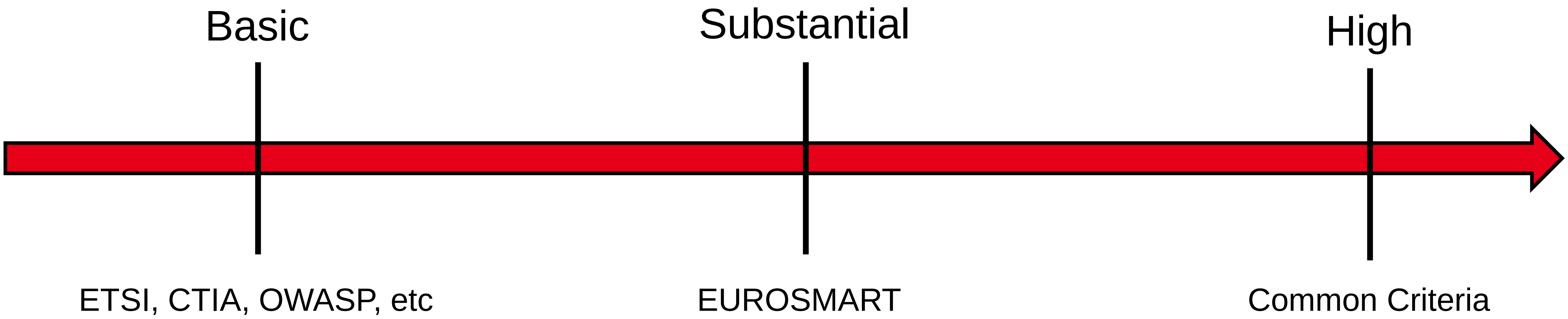
- Context: Basic evaluation level for EU CyberAct
- Not much related works on Cyberact:
  - Quite recent directive
  - More on US/international context (NISTIR 8259)
- Survey and comparison of existing frameworks:
  - ETSI, CTIA, OWASP, EuroSmart, IoT-SF
- Proposed a middle-gound evaluation scheme for ETSI, CTIA, OWASP (main contenders)
  - Idea: Allow CABs to prepare already whichever framework is chosen with minimal updates needed.
- Frameworks coverage display in Table:
  - Nice common ground but also different directions (HW, Privacy, etc).
- Perspectives: Update according discussion evolutions



| Level | ETSI | CTIA | OWASP |
|---|---|---|---|
| 1 | 46% | 29% | 90% |
| 2 | 62% | 47% | 90% |
| 3 | 85% | 59% | 100% |

# THANKS FOR YOUR ATTENTION

# CONTEXT



Basic

Substantial

High

ETSI, CTIA, OWASP, etc

EUROSMART

Common Criteria