CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

SUPPLY CHAIN SECURITY FORUM

SUPPLY CHAIN SECURITY FORUM

從零開始面對EU CRA

TEAM CYBERSECURITY

賴俊福 AFU LAI

台達電子/ IABG技術發展部

軟體設計副理

Basic **understanding** of the EU CRA

Challenges for manufacturers

Security **development** concepts

Security Regulation Insight

EU RED DA	2025/8
EU Machinery	2027/1
EU Cyber Resilient Act	2026/9, 2027/12

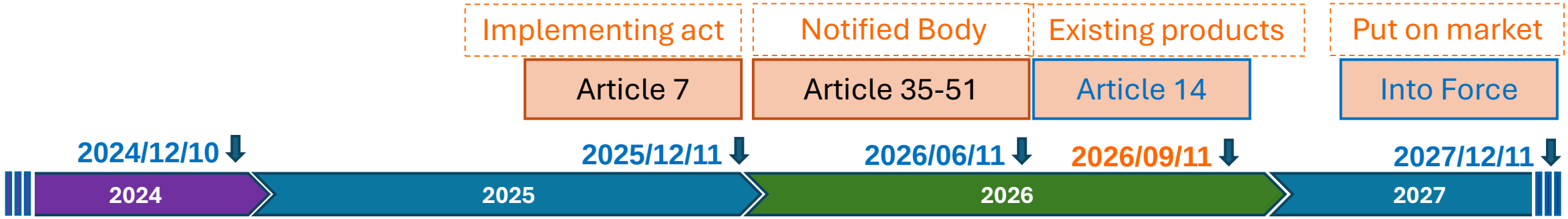
EU Cyber Resilient Act

Article 2

This Regulation applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

NOT APPLY TO

- Regulation (EU) 2017/745; (medical devices)
- Regulation (EU) 2017/746; (in vitro diagnostic medical device)
- Regulation (EU) 2019/2144; (motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles)
- certified in accordance with Regulation (EU) 2018/1139 (common rules in the field of civil aviation)
- Directive 2014/90/EU (marine equipment)
- national security or defence purposes or to products specifically designed to process classified information



Penalties Related to Manufacturer

Article 64

2. Non-compliance with the essential cybersecurity requirements set out in Annex I and the obligations set out in Articles 13 and 14 shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 2,5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

ANNEX I: Requirements
Article 13: Obligations of manufacturers
Article 14: Reporting obligations of manufacturers

3. Non-compliance with the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Article 18: Authorised representatives
Article 19: Obligations of importers
Article 20: Obligations of distributors

Article 31: Technical documentation
Article 32: Conformity assessment procedures for products with digital elements
Article 53: Access to data and documentation

4. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Penalty Overview

Violation	Penalty Amount	Description	Liable Party
General violation of CRA	Up to €15 million or 2.5% of the company's total worldwide annual turnover, whichever is higher.	Failure to comply with the essential security requirements of the CRA, such as: - Failure to design and develop products with appropriate security features - Failure to provide necessary security updates - Failure to address known vulnerabilities	Manufacturer
Providing incorrect, incomplete, or misleading information	Up to €5 million or 1% of the company's total worldwide annual turnover, whichever is higher.	Providing incorrect, incomplete, or misleading information to notified bodies or market surveillance authorities.	Manufacturer
Violations by authorized representatives, importers, distributors, and conformity assessment bodies	Up to €10 million or 2% of the company's total worldwide annual turnover, whichever is higher.	Failure of authorized representatives, importers, and distributors to fulfill their obligations under the CRA, such as: - Failure to verify that products comply with CRA requirements - Placing non-compliant products on the market - Conformity assessment bodies failing to correctly implement conformity assessment procedures	Authorized representatives, importers, distributors, conformity assessment bodies
Certain requirements related to the EU declaration of conformity, technical documentation, and CE marking	Up to €10 million or 2% of the company's total worldwide annual turnover, whichever is higher.	Failure to comply with requirements related to the EU declaration of conformity, technical documentation, and CE marking, such as: - Failure to prepare correct technical documentation - Issuing incorrect declarations of conformity - Affixing the CE marking to non-compliant products	Manufacturer, importer

** Content summarized by Gemini

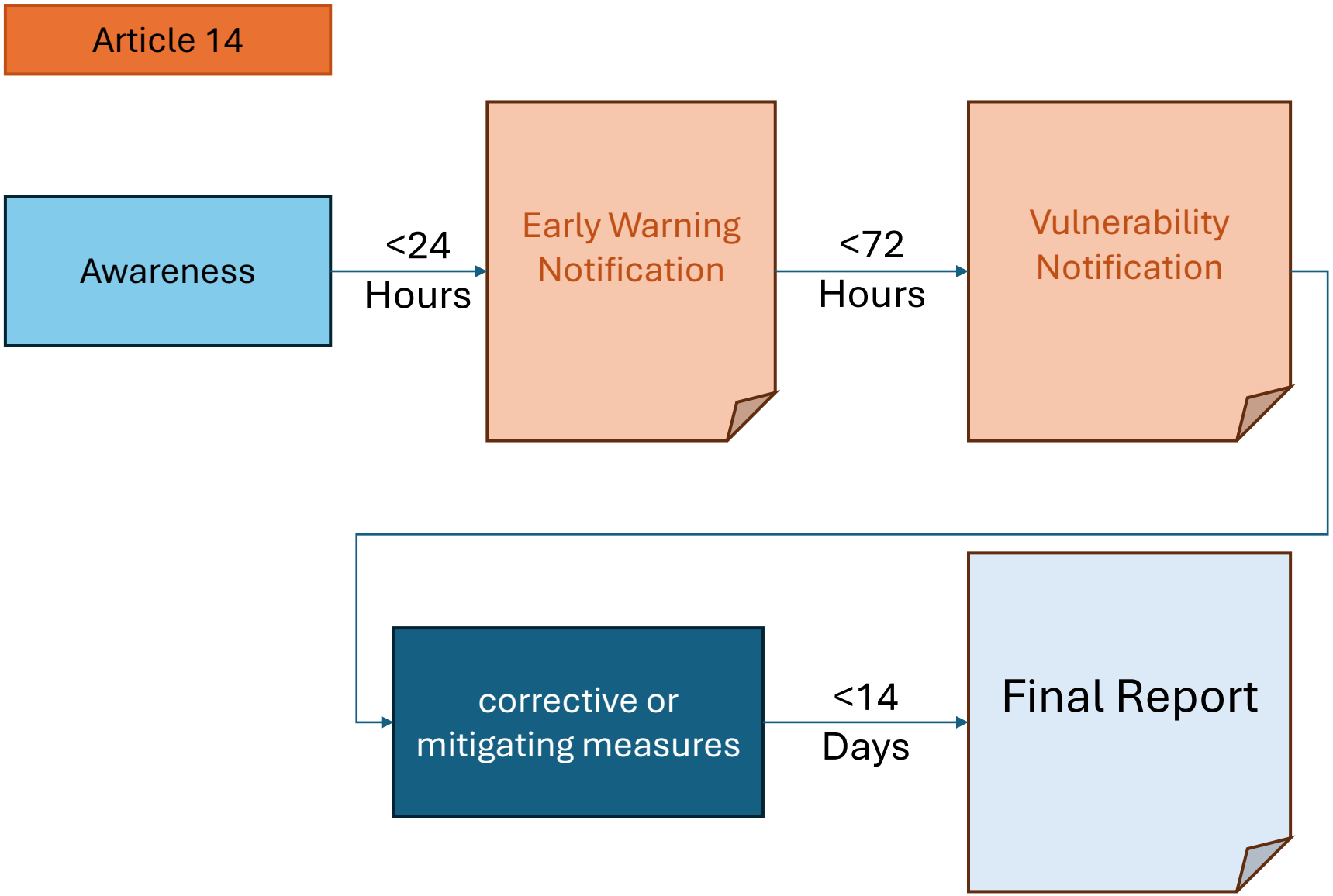
Obligations of Manufacturers

Article 13

- Essential cybersecurity requirements set out in Part I of Annex I
- Vulnerability handling requirements set out in Part II of Annex I
- Cybersecurity Risk Assessment documentation
- Due Diligence for 3rd party components
- Support period (end date including exact year and month)
- Security update
- SBOM

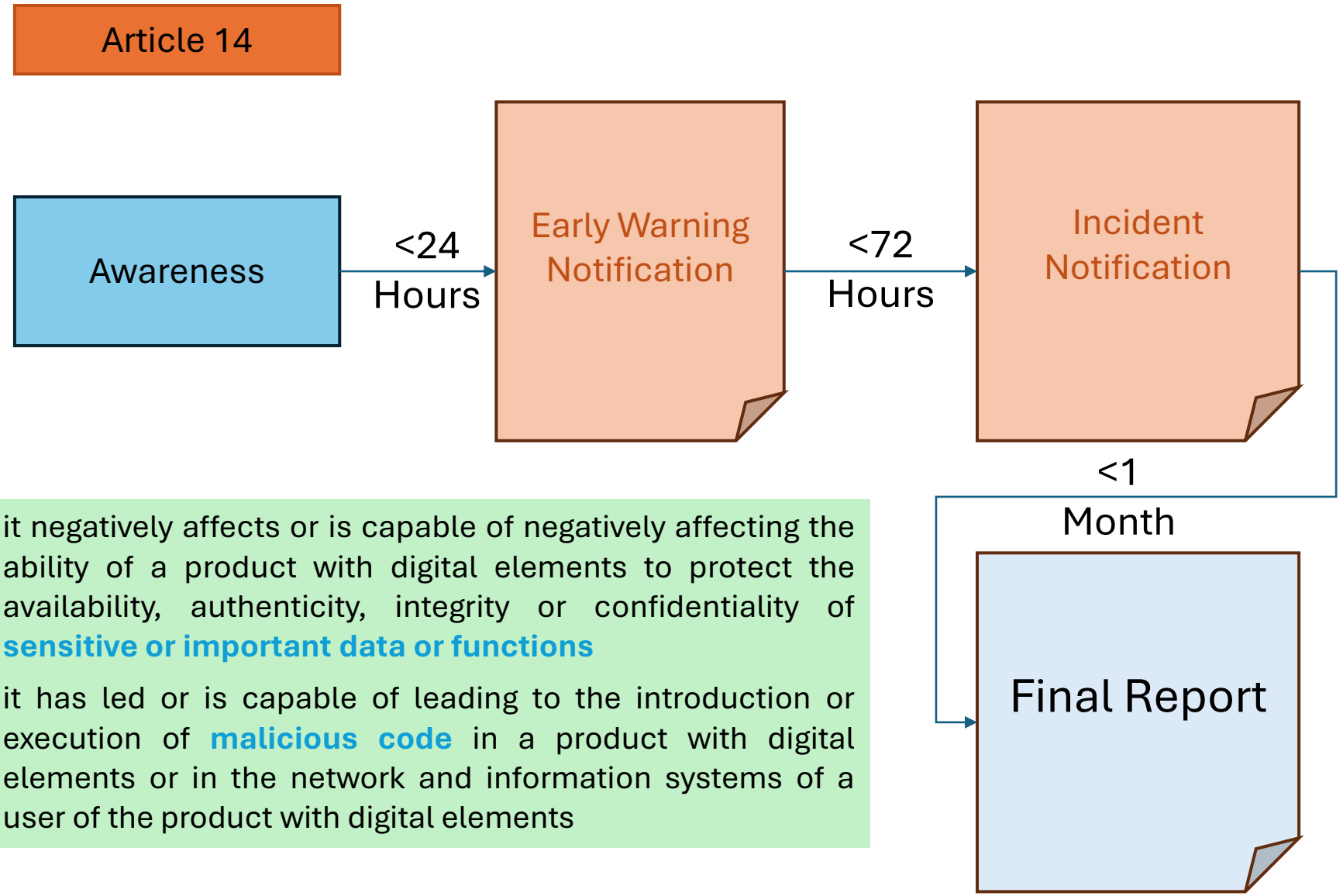
- Draw up the technical documentation referred to in Article 31
- Carry out the chosen conformity assessment procedures referred to in Article 32 or have them carried out.
- Draw up the EU declaration of conformity in accordance with Article 28
- Affix the CE marking in accordance with Article 30
- Ensure that the end date of the support period

Notification of Actively Exploited Vulnerability



- a **description** of the vulnerability, including its **severity** and **impact**
- information concerning any **malicious actor** that has exploited or that is exploiting the vulnerability
- details about the **security update** or other **corrective measures** that have been made available to remedy the vulnerability.

Notification of Severe Incident



- it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of **sensitive or important data or functions**
- it has led or is capable of leading to the introduction or execution of **malicious code** in a product with digital elements or in the network and information systems of a user of the product with digital elements

- a **description** of the incident, including its **severity** and **impact**
- the type of **threat or root cause** that is likely to have triggered the incident
- applied and ongoing **mitigation measures**

Compliance Activities for Manufacturers

Effective cybersecurity lifecycle development process

- Management of known vulnerability (include 3rd party component)
- Management of mitigation documentation (workaround)
- Management of supply chain
- Effective and regular tests (may require external report)
- **Free** security update (at least **5** years according to use time, **10** years after release)

Essential security measure

- SBOM and known vulnerability monitoring
- Secure by Default
- Minimization / protection / authorization of data / communication
- Secure restore and decommissioning

Rapid vulnerability handling

- Early warning notification within 24 hours
- Vulnerability notification within **72 hours**
- Final report within 14 days after a corrective or mitigating measure is available
- Final report within **1 month** after vulnerability notification

Reference: Cyber Resilience Act Requirements Standards Mapping

Conformity and Validation

Notified Body required

Category	Module A	Module B+C	Module H	Cert. Scheme	Remark
Default	Internal Control	O	O	O	Article 2 (Scope)
Class I	Harmonized Standard	O	O		Annex III Important Products Class I
Class II		O	O	Article 27(9)	Annex III Important Products Class II
Critical				Article 8(1) Article 8(3)	Annex IV Critical Products

Conformity assessment of products with digital elements that are not listed as important or critical products with digital elements in this Regulation can be carried out by the manufacturer under its own responsibility following the internal control procedure based on module A of Decision No 768/2008/EC in accordance with this Regulation. This also applies to cases where a manufacturer chooses not to apply in whole or in part an applicable harmonised standard, common specification or European cybersecurity certification scheme.

Important Products

Class I

1.Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers;

2.Standalone and embedded browsers;

3.Password managers;

4.Software that searches for, removes, or quarantines malicious software;

5.Products with digital elements with the function of virtual private network (VPN);

6.Network management systems;

7.Security information and event management (SIEM) systems;

8.Boot managers;

9.Public key infrastructure and digital certificate issuance software;

10.Physical and virtual network interfaces;

11.Operating systems;

12.Routers, modems intended for the connection to the internet, and switches;

13.Microprocessors with security-related functionalities;

14.Microcontrollers with security-related functionalities;

15.Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities;

16.Smart home general purpose virtual assistants;

17.Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems;

18.Internet connected toys covered by Directive **2009/48/EC** of the European Parliament and of the Council(45) that have social interactive features (e.g. speaking or filming) or that have location tracking features;

19.Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation **(EU) 2017/745** or Regulation **(EU) 2017/746** do not apply, or personal wearable products that are intended for the use by and for children.

Class II

1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;

2. Firewalls, intrusion detection and prevention systems;

3. Tamper-resistant microprocessors;

4. Tamper-resistant microcontrollers.

Article 7

Products with digital elements which have the core functionality of a product category set out in Annex III

Technical Documentation

Annex VII

Product Description

- Intended purpose
- Version
- External features, marking, layout for HW
- Information set out in Annex II

Process Description

Necessary information and specifications:

- Design and development
- Vulnerability handling processes
- Production and monitoring processes

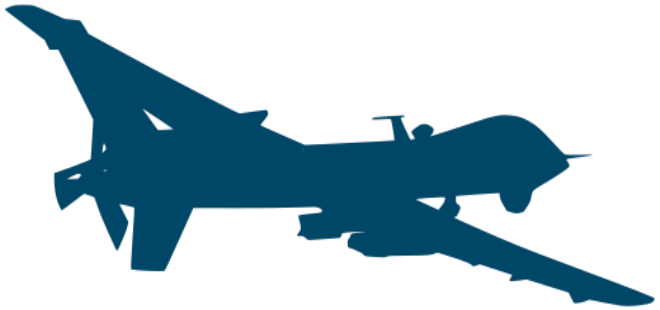
- Cybersecurity risk assessment for Part I of Annex I
- Support Period
- A list of the harmonised standards
- Test report
- EU declaration of conformity
- SBOM

Regulation as Weapon

Expect the unexpected.

What If A Product...

- Maintained for more than 10 years
- Limited or Lacking associated knowledge
- Resource shortage



A decade after its release, the product is facing a significant increase in reported security problems, some of which are critical.

Competitor

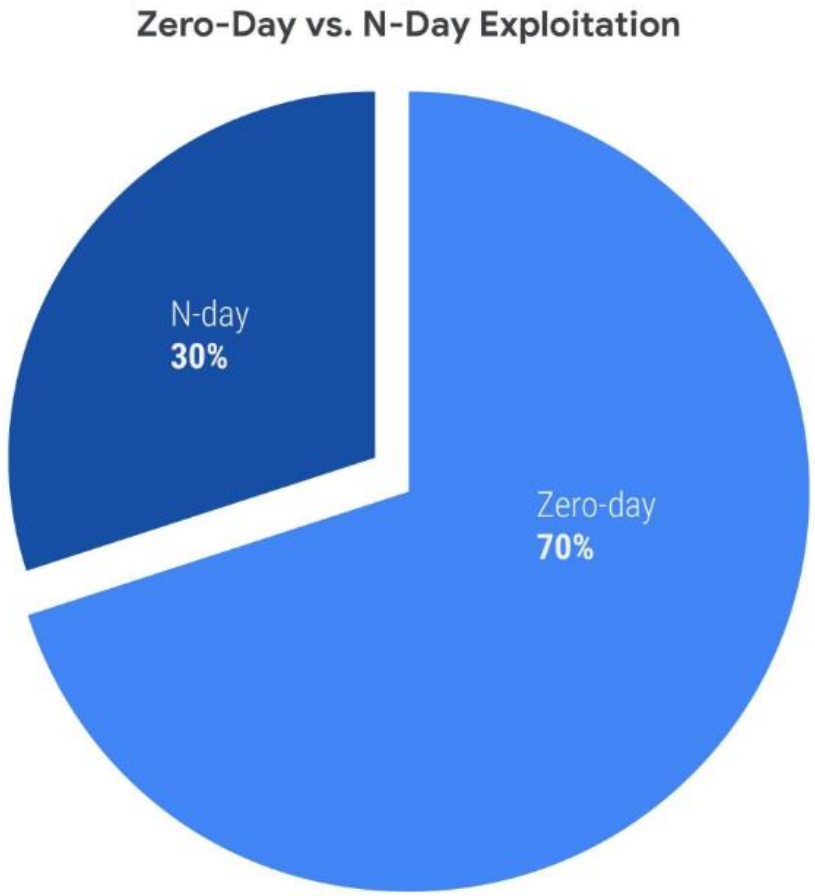
Exploitation Timelines

Time-to-Exploit (TTE)

- the average time taken to exploit a vulnerability before or after a patch is released

Year	TTE
2018 - 2019	63
2020 - 2021	44
2021 - 2022	32
2023	**5**

Year	0-Day : N-Day
2020 - 2021	39:61
2021 - 2022	38:62
2023	**70:30**



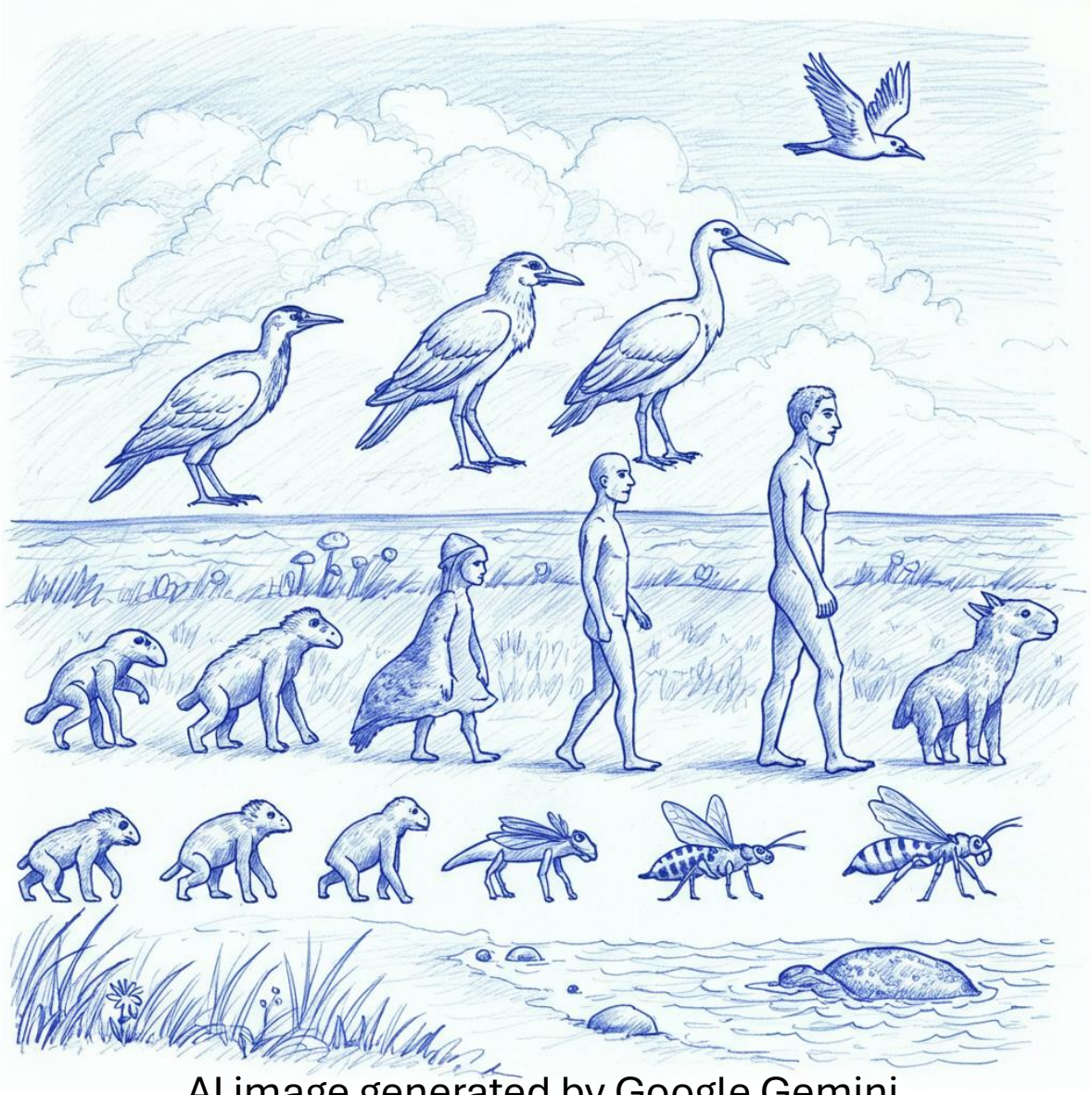
Source from: https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023

Security Awareness

Seek knowledge to mitigate risk when facing the unknown.

Make It as Simple as You Can Imagine

Secure by Default



AI image generated by Google Gemini

Secure by Guideline

People Matter Most

Security Measure

- Technical
- Administrative
- Physical

Process

- Maintenance
- Manufacturing
- Development
- Review & Audit

People

- Operation
- Design
- Plan

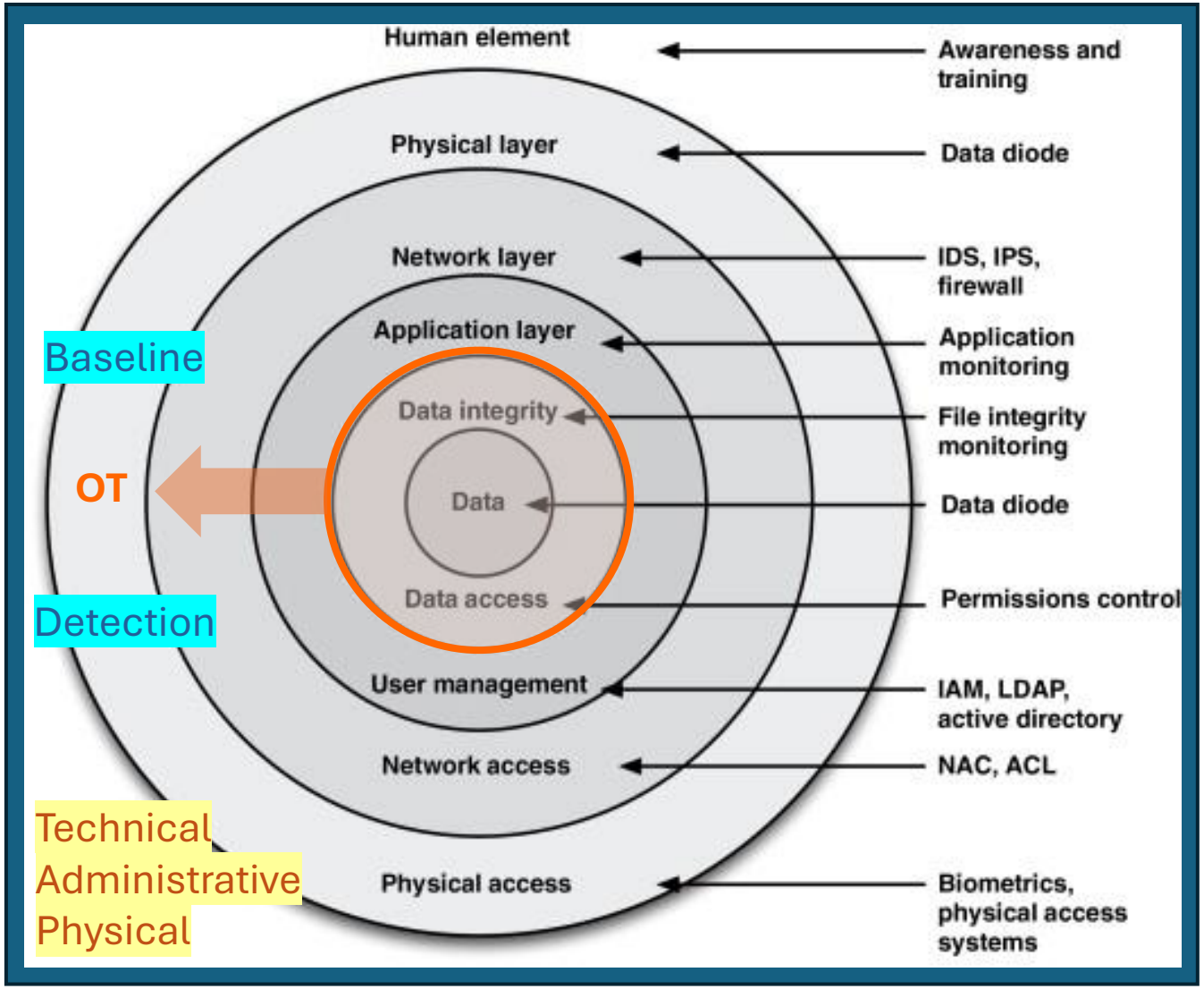
ISA/IEC 62443 Cybersecurity Certificate Program

Qualify the facilitator

Earn all four certificates and receive the Cybersecurity Expert Certificate

https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program

Defense in Path



https://www.sciencedirect.com/topics/computer-science/defense-in-depth

Identification

Authentication

Secure Channel

Conduit Device

Authorization

Interface

Function / App

Module / OS

Storage

Reference Practice

Cybersecurity is like writing; there's no perfect score, but there's good and bad.
Neglecting protection or relying on luck greatly increases risk.

Countdown to EU CRA

Don’t leave it until the last minute

Direct or indirect logical or physical data connection to device or network

- Default
- Class I
- Class II
- Critical

Now

- Secure Process
- Due diligence
- CE marked products
- Awareness & Training
  - IEC 62443-4-1
  - IEC 62443-4-2
  - IEC 62443-3-3
  - EN 18031
  - SBOM
  - Vulnerability Scan
  - Penetration Test

2025/E

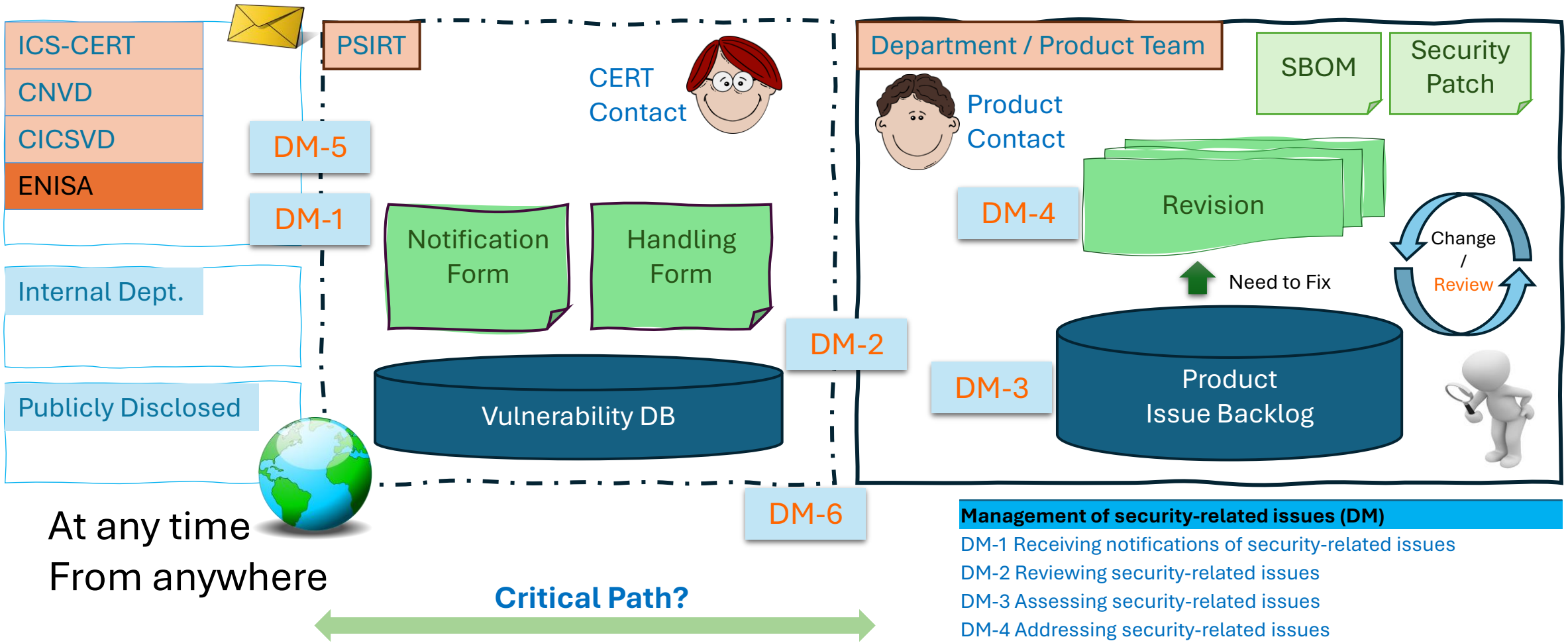
- Identification
- CERT Process
- Conformity
- NB Certification
- DQA Process

2026/09/11

- Legacy
- Security Update
- Security Platform

2027/12/11

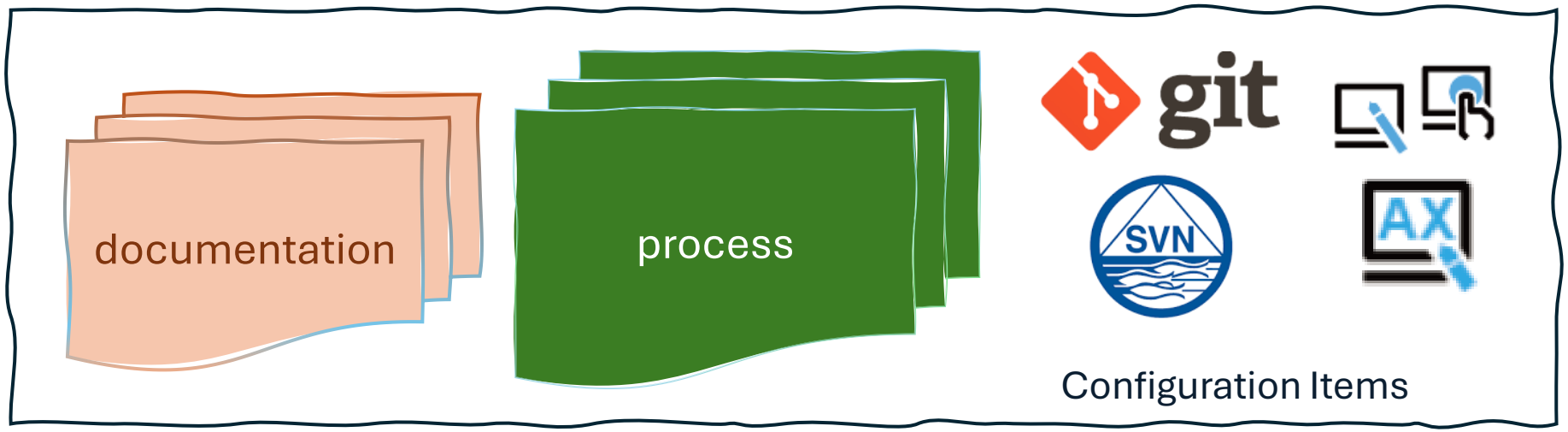
CERT Process



Management of security-related issues (DM)

DM-1 Receiving notifications of security-related issues
DM-2 Reviewing security-related issues
DM-3 Assessing security-related issues
DM-4 Addressing security-related issues
DM-5 Disclosing security-related issues
DM-6 Periodic review of security defect management practice

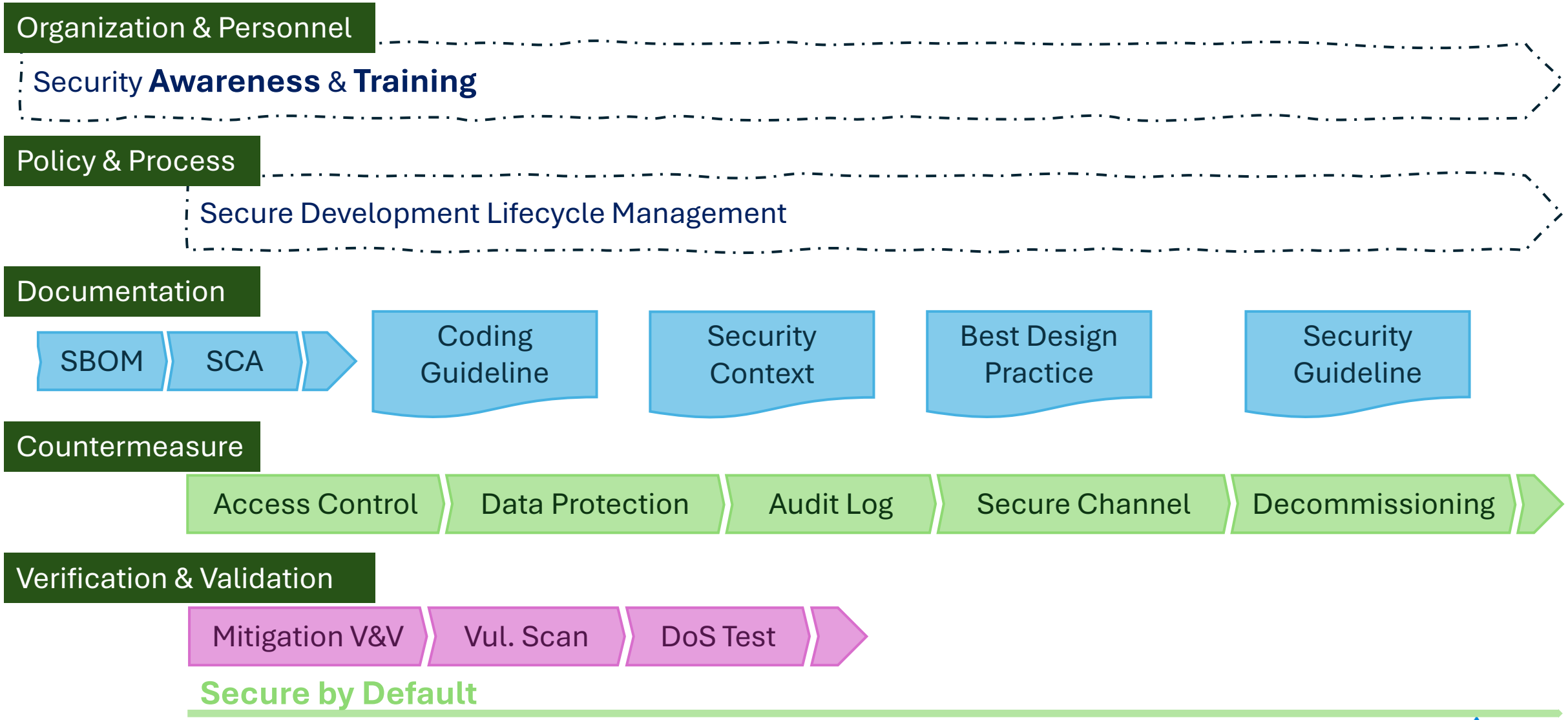
Configuration Management



Review & Communicate

- What to be managed
- How to produce or change it
- When to handle the change
- Role and responsibility
- …

Prioritizing Approach Selection



Vulnerability Management

SBOM

BLACKDUCK®

Version	Phase	Last Updated	Last Scanned	License	Security Risk	License Risk	Operational Risk
[redacted]_v1.7	In Development	2025年1月1日	2025年1月1日	Unknown License			
[redacted]_v1.8	In Development	2025年1月14日	2025年1月15日	Unknown License			
[redacted]r_v1.6	In Development	2024年11月15日	2024年6月20日	Unknown License			
[redacted]_v1.8	In Development	下午1:52	2025年1月6日	Unknown License			
[redacted]v2.4	In Development	2024年11月15日	2024年6月20日	Unknown License			
[redacted]1.0	In Development	2024年11月15日	2024年6月3日	Unknown License			
[redacted]v2.4	In Development	2024年11月15日	2024年6月20日	Unknown License			

Tool

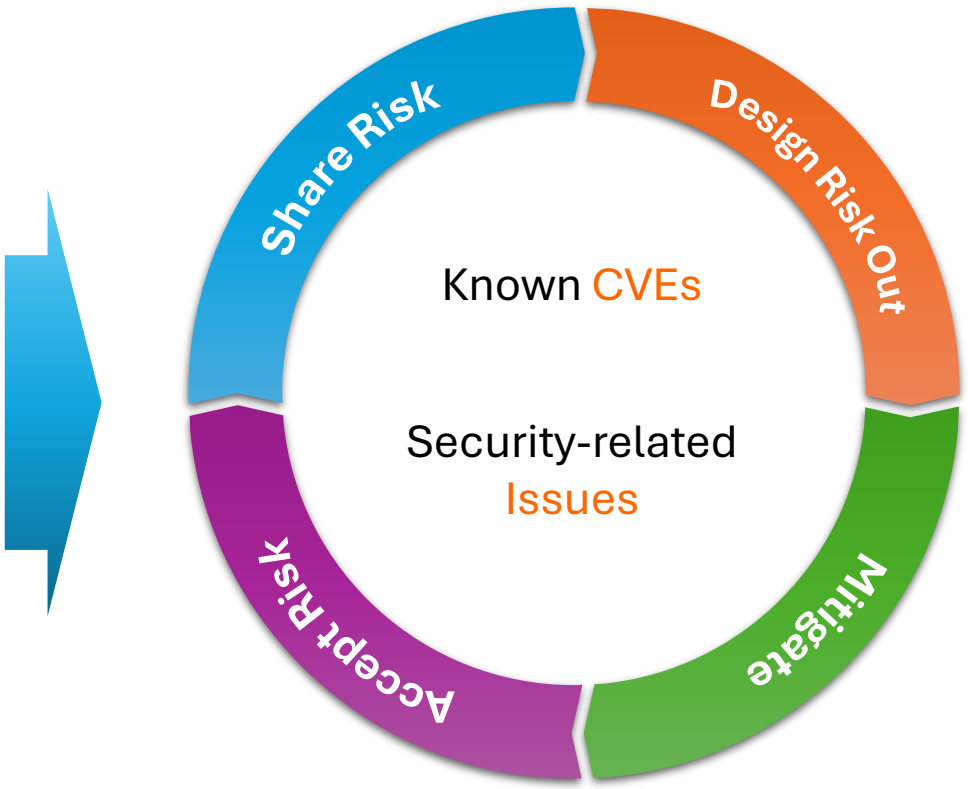
BURPSUITE PROFESSIONAL, sqlmap, Nmap, metasploit, Nessus vulnerability scanner, OWASP ZAP, KALI LINUX™

CERT

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

ZERO DAY INITIATIVE

CNNVD 国家信息安全漏洞库 China National Vulnerability Database of Information Security



SBOM

The Software Bill of Materials (**SBOM**) is a list of all the components, libraries, and other dependencies used in a software application.

Standard Format

- Software Package Data eXchange (SPDX)
  - ISO/IEC 5962:2021
- Software Identification (SWID) Tags
  - ISO/IEC 19770-2:2015
- CycloneDX

SBOM Tool

- OSV-Scanner (Image)
- Black Duck (Source, Binary)

Regulation Requirement

- US FAR-2021-0017
- US FDA Cybersecurity in Medical Devices
- EU CRA

NTIA Minimum Requirement

- Supplier Name
- Component Name
- Component Version
- Other Unique Identifiers
- Dependency Relationship
- Author of SBOM Data
- Timestamp

Future work:

- Component Hash
- License Information

Coding Guideline

Static Code Analysis (**SCA**) for source code to determine security coding errors such as buffer overflows, null pointer dereferencing, etc. using the secure coding standard for the supported programming language

- Report
- Acceptance criteria
- Reviewer

OWASP Secure Coding Practices
Quick Reference Guide

- Input Validation
- Sanitization Output Encoding
- Authentication and Password Management
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/
https://owasp.org/www-project-developer-guide/release/

Security Context

Assumptions about the intended usage of the product and the environment.

External Environment

Internal Connection

Network Asset
Security Asset
Privacy Asset

System Architecture

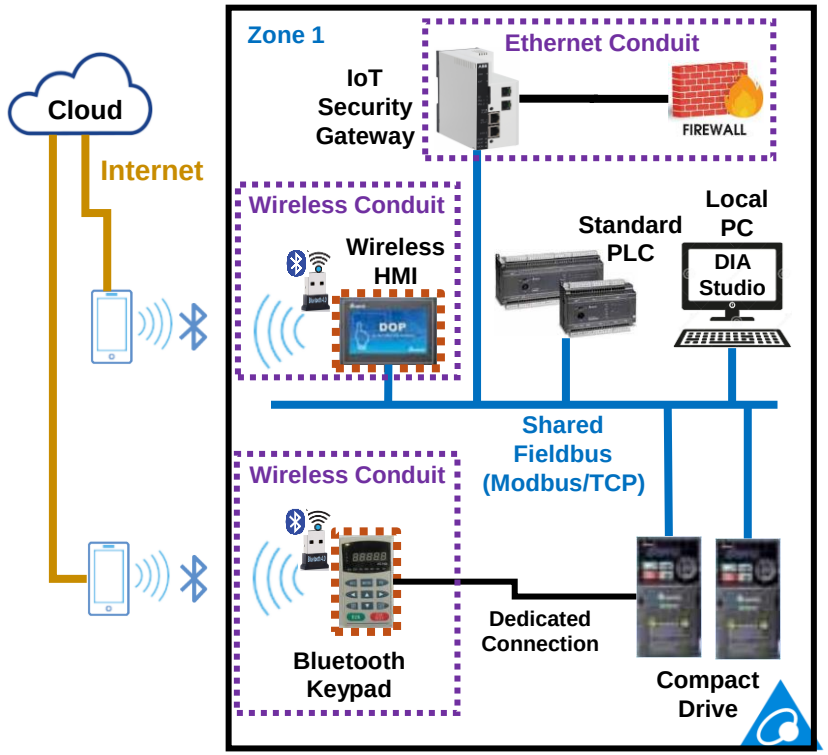
Network Topology

Threat Model

Expected Threat Analysis

Threat Modeling

- Common Vulnerabilities
- Known / Experienced Vulnerabilities



Security Guideline

SG-1 **Defense in Depth**

Security Level Capability (SL-C)
- IEC 62443-3-3 compliance
- IEC 62443-4-2 compliance

Access Control

SG-2

Installation and Configuration
- System Account
- Audit Records
- Networking
- Privileges and Roles

SG-3

Operation and Maintenance
- Anti-virus
- Digital Signature
- User Management
- Patch
- Periodic review
- Notification

SG-6

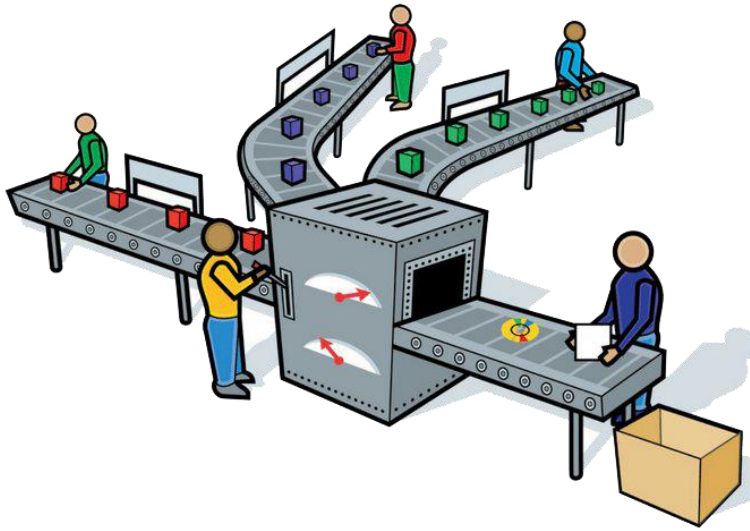
SG-5

Decommissioning
- Post-installation
- Uninstallation

SG-4

Security Guidelines (SG)
SG-1 Product defense in depth
SG-2 Defense in depth measures expected in the environment
SG-3 Security hardening guidelines
SG-4 Secure disposal guidelines
SG-5 Secure operation guidelines
SG-6 Account management guidelines
SG-7 Documentation review

Decommissioning (Data Sanitization)



Factory Default

Secure by Default

Reset ALL to Default

Easy & Secure

Partially Clear

- Configuration
- Data
- Log
- …

Use 1

Transfer to

Use 2

歡迎蒞臨

C112 台達電子

Smarter. Greener. Together.