SECURITY PATTERN

La protezione dei dati nelle applicazioni Internet of Things

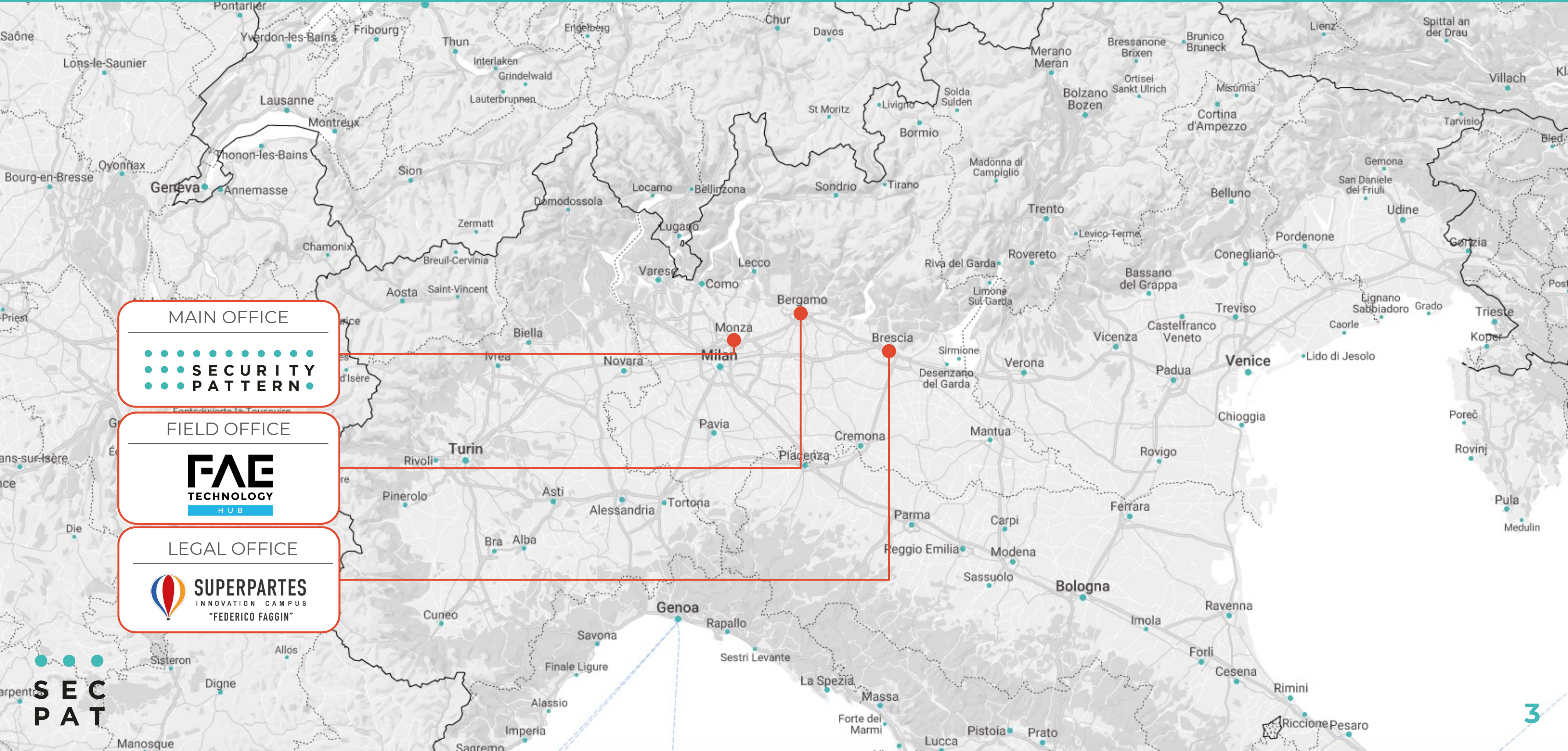
Guido Bertoni

Mission

We help creators of
intelligent connected devices
to **design**, **implement** and **operate**
their systems with a
sustainable security level

SEC
PAT

Where we are



MAIN OFFICE

SECURITY PATTERN

FIELD OFFICE

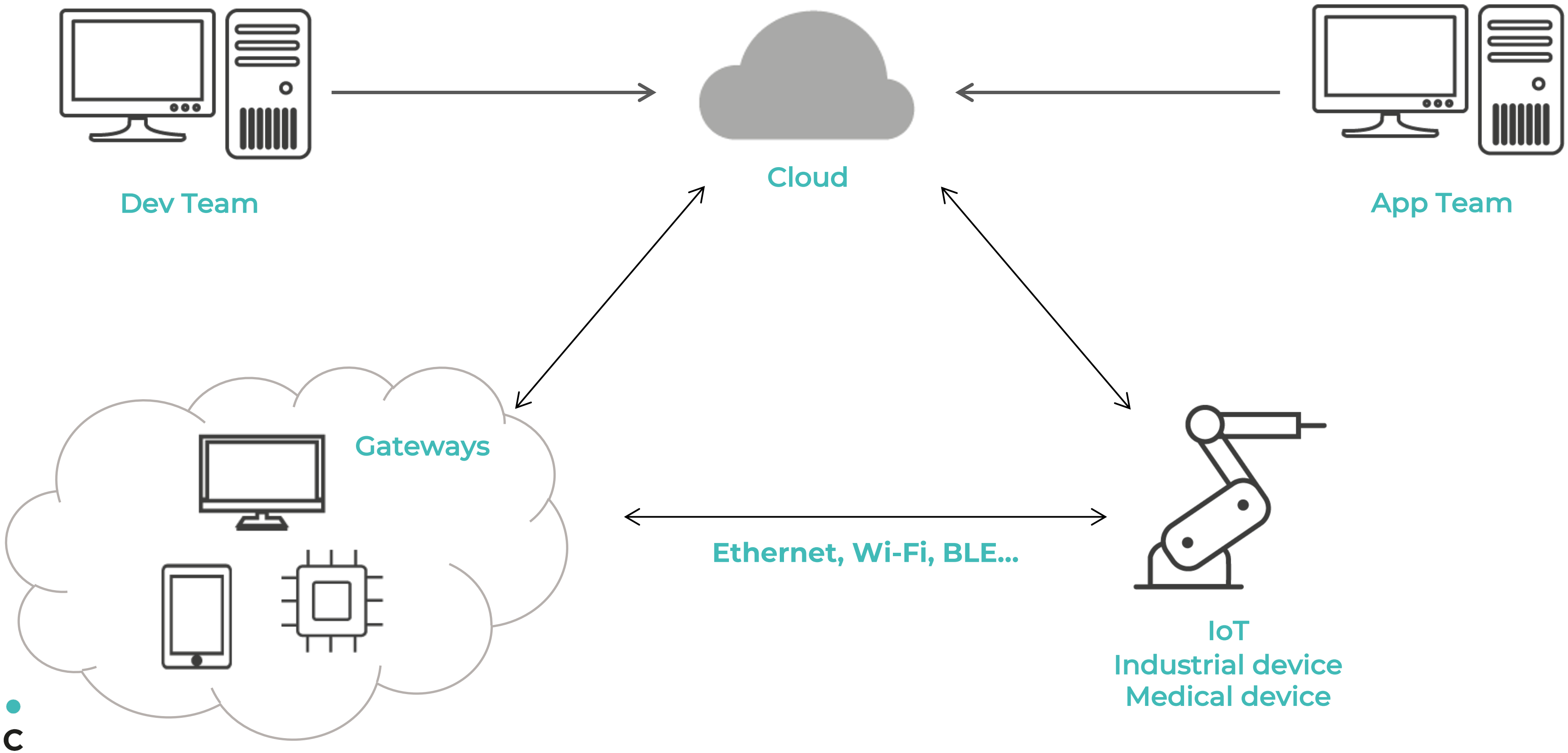
FAE TECHNOLOGY HUB

LEGAL OFFICE

SUPERPARTES INNOVATION CAMPUS "FEDERICO FAGGIN"

SEC PAT

The big picture



Dev Team

Cloud

App Team

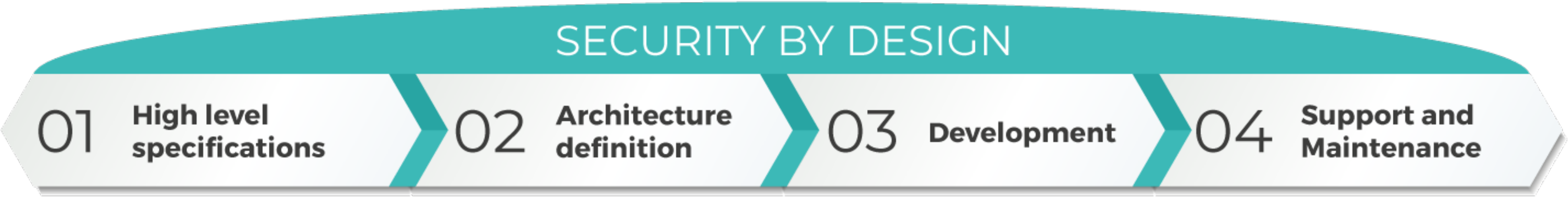
Gateways

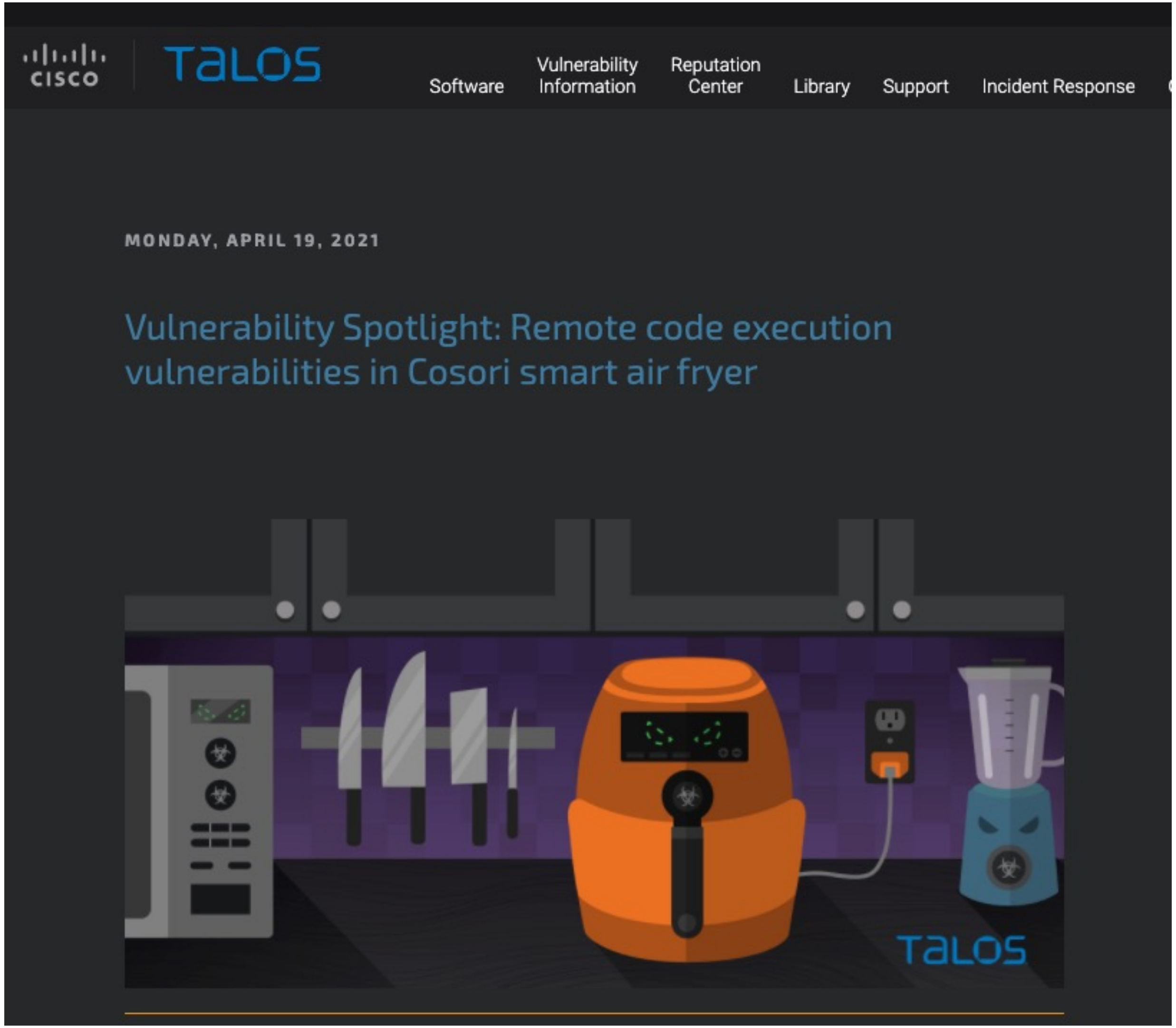
Ethernet, Wi-Fi, BLE...

IoT
Industrial device
Medical device

Typical product cycle

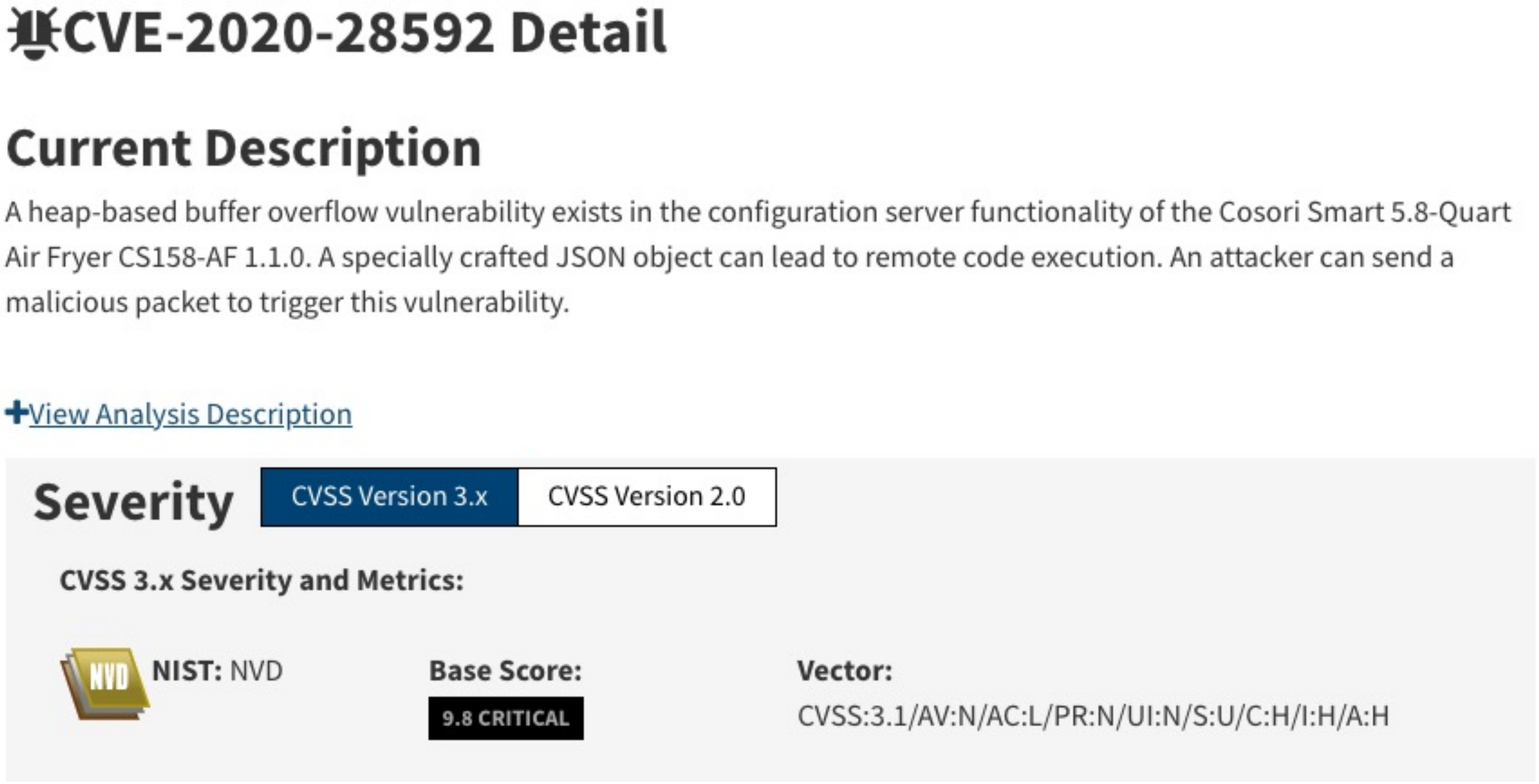
- Development cycle from few months up to some years
- Life cycle on the market of some years up to 10+ years
- Security spans on the entire life of the device


SECURITY BY DESIGN
01 High level specifications
02 Architecture definition
03 Development
04 Support and Maintenance



MONDAY, APRIL 19, 2021

Vulnerability Spotlight: Remote code execution vulnerabilities in Cosori smart air fryer



CVE-2020-28592 Detail

Current Description

A heap-based buffer overflow vulnerability exists in the configuration server functionality of the Cosori Smart 5.8-Quart Air Fryer CS158-AF 1.1.0. A specially crafted JSON object can lead to remote code execution. An attacker can send a malicious packet to trigger this vulnerability.

+View Analysis Description

Severity

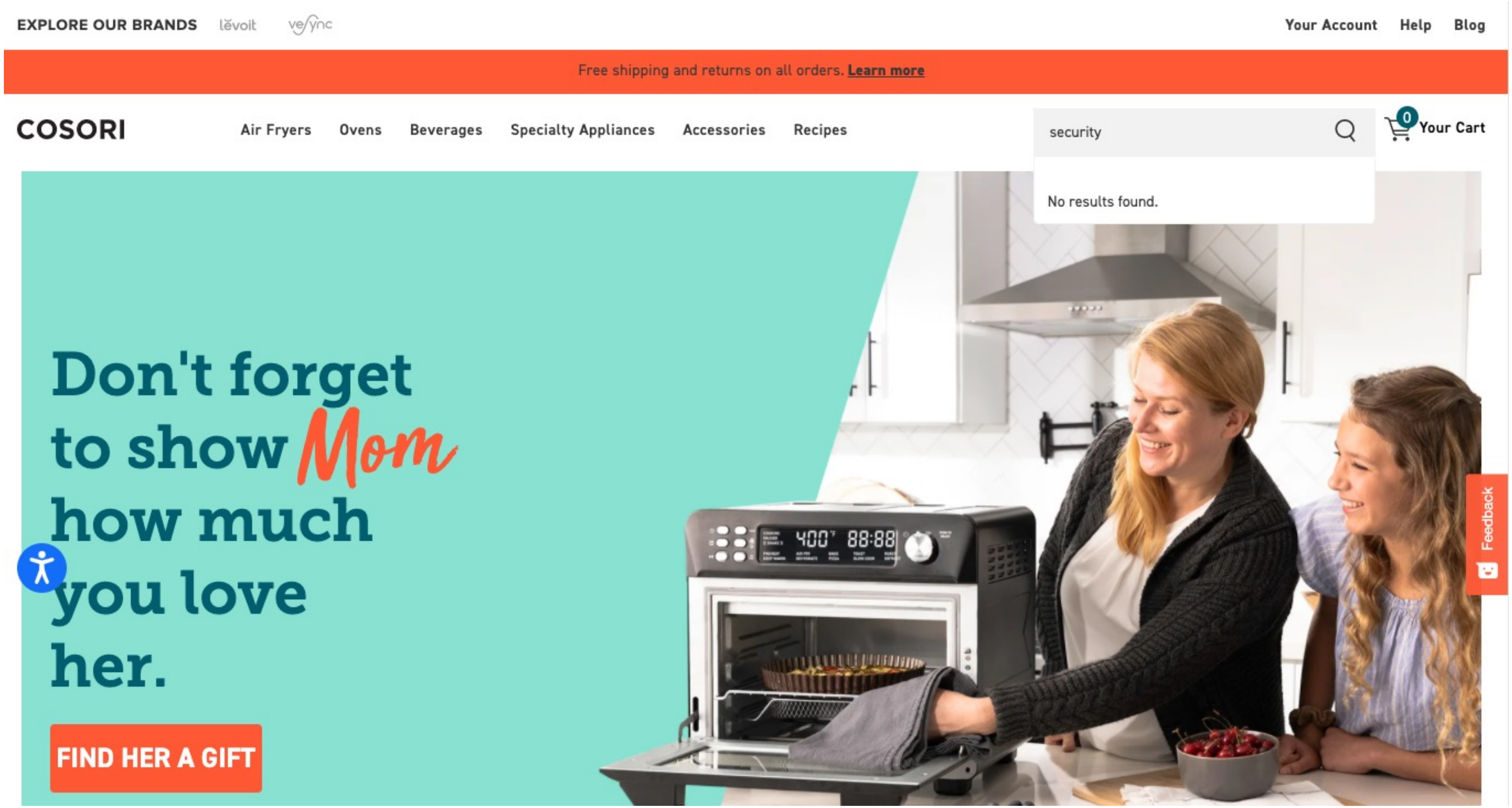
CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score:
9.8 CRITICAL

Vector:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Free shipping and returns on all orders. **Learn more**

security

No results found.

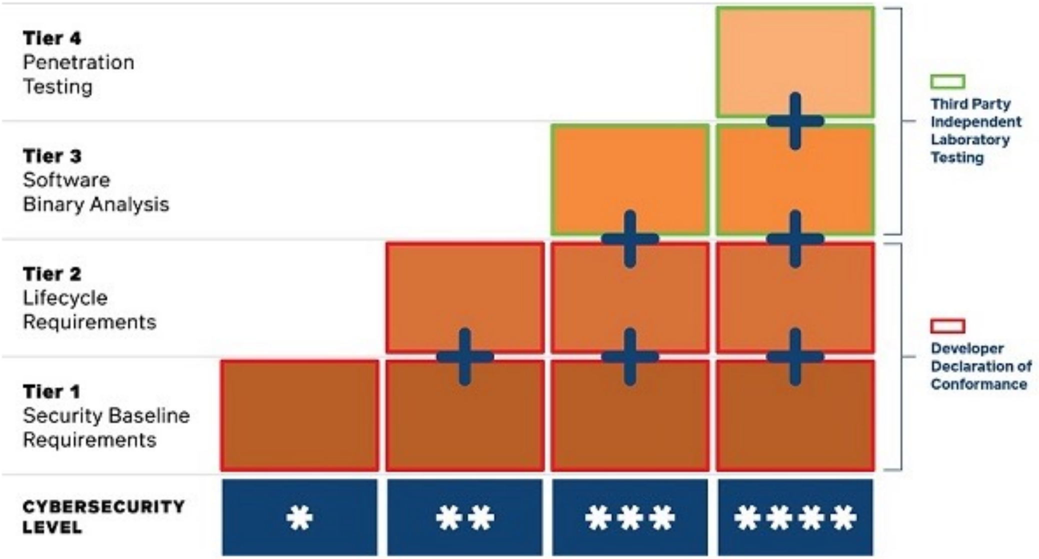
IoT Security Standard

Singapore CSA

- *CSA (Cyber Security Agency of Singapore) has launched the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of efforts to improve Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace.*
- https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls

Labeling

- First Wi-Fi routers and smart home hubs.
  - Prioritized because of their wider usage and impact
- Extended to include all categories of consumer IoT
  - IP cameras, smart door locks, smart lights and smart printers.



Tier 4
Penetration Testing

Tier 3
Software Binary Analysis

Tier 2
Lifecycle Requirements

Tier 1
Security Baseline Requirements

CYBERSECURITY LEVEL

| * | ** | *** | **** |

🟩 Third Party Independent Laboratory Testing

🟥 Developer Declaration of Conformance

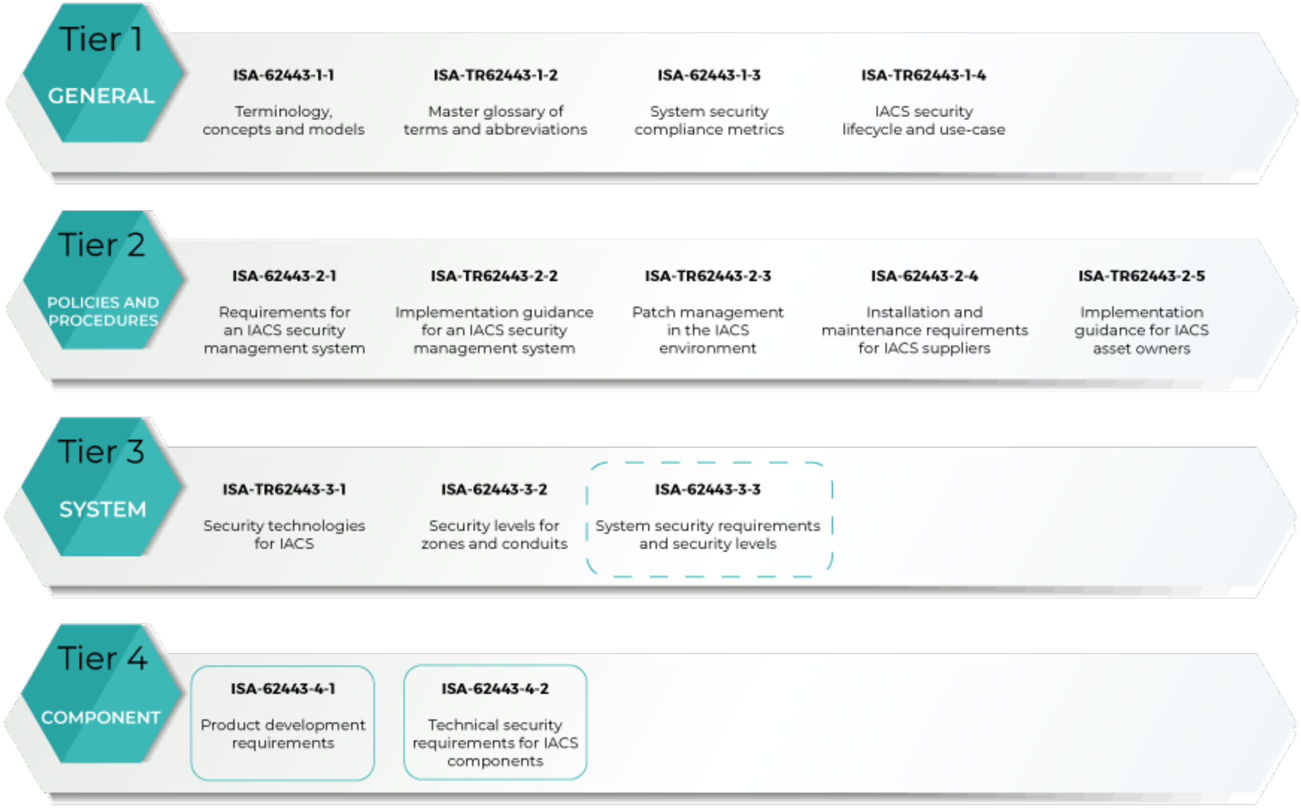
ETSI EN 303 645 Guidelines

- No default passwords
- **Implement a vulnerability disclosure policy**
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

IIoT

ISA/IEC 62443 – Industrial Automation and Control Systems

- General
  - Contains standards and reports that are general in nature
- Policies and Procedures
  - Addresses the people and process aspects of an effective security program (OPERATION)
- System
  - address the technology related aspects of security (INTEGRATION)
- Component
  - Focuses on the security-related procedural and technical requirements related to products/components (DEVELOPMENT)



Tier 1 – GENERAL

- ISA-62443-1-1: Terminology, concepts and models
- ISA-TR62443-1-2: Master glossary of terms and abbreviations
- ISA-62443-1-3: System security compliance metrics
- ISA-TR62443-1-4: IACS security lifecycle and use-case

Tier 2 – POLICIES AND PROCEDURES

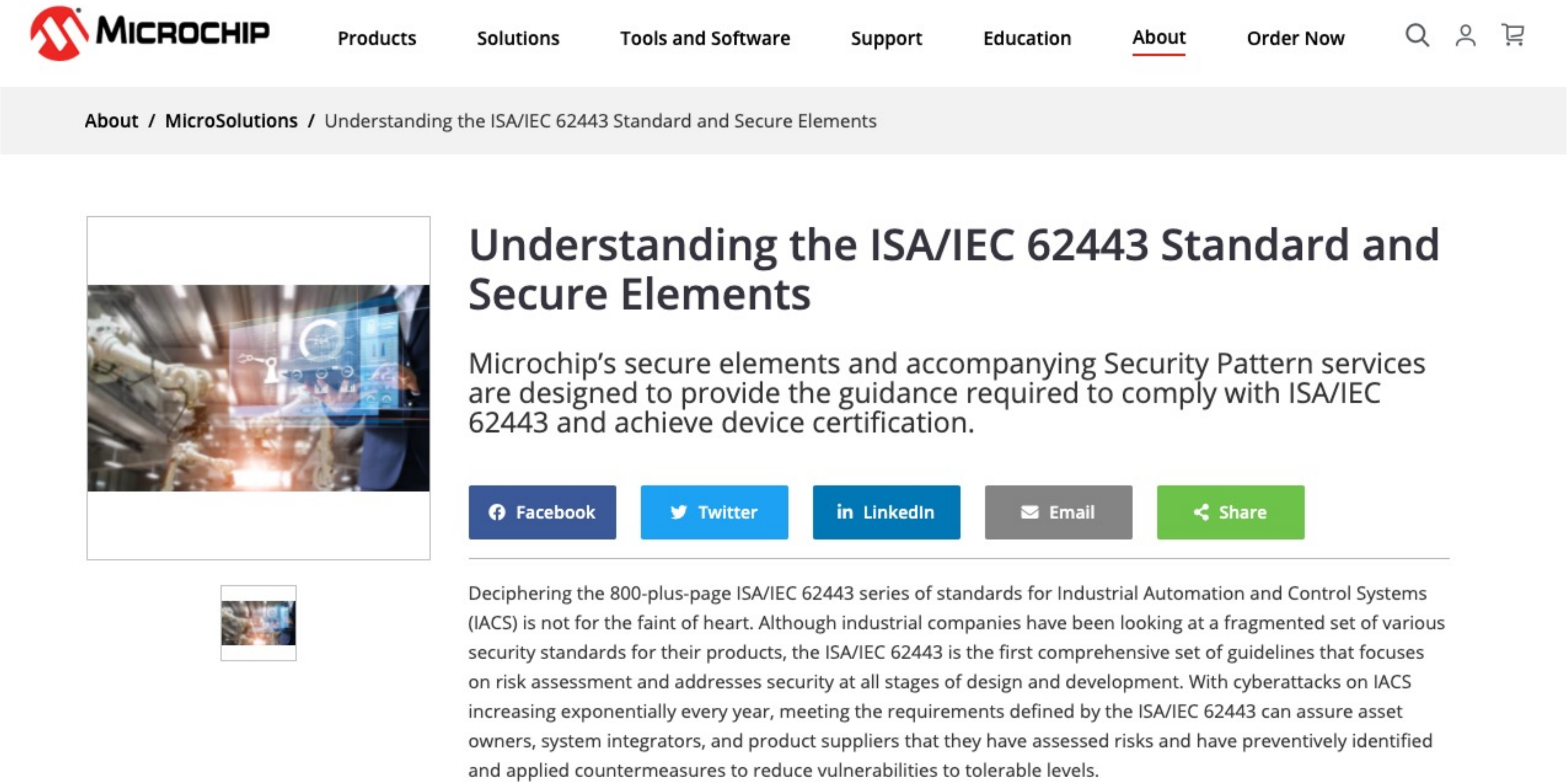
- ISA-62443-2-1: Requirements for an IACS security management system
- ISA-TR62443-2-2: Implementation guidance for an IACS security management system
- ISA-TR62443-2-3: Patch management in the IACS environment
- ISA-62443-2-4: Installation and maintenance requirements for IACS suppliers
- ISA-TR62443-2-5: Implementation guidance for IACS asset owners

Tier 3 – SYSTEM

- ISA-TR62443-3-1: Security technologies for IACS
- ISA-62443-3-2: Security levels for zones and conduits
- ISA-62443-3-3: System security requirements and security levels

Tier 4 – COMPONENT

- ISA-62443-4-1: Product development requirements
- ISA-62443-4-2: Technical security requirements for IACS components



Understanding the ISA/IEC 62443 Standard and Secure Elements

Microchip's secure elements and accompanying Security Pattern services are designed to provide the guidance required to comply with ISA/IEC 62443 and achieve device certification.

Deciphering the 800-plus-page ISA/IEC 62443 series of standards for Industrial Automation and Control Systems (IACS) is not for the faint of heart. Although industrial companies have been looking at a fragmented set of various security standards for their products, the ISA/IEC 62443 is the first comprehensive set of guidelines that focuses on risk assessment and addresses security at all stages of design and development. With cyberattacks on IACS increasing exponentially every year, meeting the requirements defined by the ISA/IEC 62443 can assure asset owners, system integrators, and product suppliers that they have assessed risks and have preventively identified and applied countermeasures to reduce vulnerabilities to tolerable levels.

https://www.microchip.com/en-us/about/blog/learning-center/understanding-the-isa-iec-62443-standard-and-secure-elements-0

Medical Devices

UL 2900-1 and UL 2900-2-1

- FDA (U.S. Food and Drug Administration) has recognized the UL2900-1 as a reference for product development
- UL 2900-2-1 focuses on secure design and security testing
- High level requirements:
    - **Security-specific static analysis**: Detects problems in source code like buffer overflows.
    - **Software composition analysis (SCA):** Detects problems with third-party and open source software usage.
    - **Fuzz testing:** Detects problems with handling unexpected inputs.
    - **Dynamic application security testing (DAST) & Interactive application security testing (IAST):** Detect problems related to application execution and interaction with other applications

IoT Secure Suite
Key ingredients

SEC
PAT

IOT
SECURE SUITE

The key ingredients

PKI with dedicated CA

Smart Key provisioning process

Secure Key storage architecture

Secure FOTA

The complete offering

- The technical ingredients
  - Key provisioning, secure update, secure protocolos, authentication, integration of secure elements
- Support in secure process development
- Dedicated training for internal team
- Management of security issue and communication
- Security assessment
  - From high level system
  - To process
  - Down to penetration testing

SECURITY PATTERN

Thank you!

hello@securitypattern.com