2019 INTERNATIONAL CONFERENCE ON THE EU CYBERSECURITY ACT

EUROSMART

The Voice of the Digital Security Industry

RED ALERT LABS
IoT Security

E-IoT-SCS
Eurosmart
IoT Security Certification Scheme

Roland Atoui - Managing Director, Red Alert Labs

Ayman Khalil - COO & Managing Partner, Red Alert Labs

Nov 2019

R

SINCE 1995

EUROSMART
The Voice of the Digital Security Industry

Non-Profit
Organization

The Voice of the Digital Security industry
is an association gathering technological experts in the field of the Digital security

Members are: manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers; Laboratories, Research organizations and Associations.

EUROSMART
The Voice of the Digital Security Industry

Companies

BACTECH

business card associates

FINGERPRINTS

gemalto
a Thales company

G+D Mobile Security

IDEMIA

+iD

IN GROUPE

TOSHIBA

infineon

Linxens
crafting the future of connections

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre

NEDCARD

NXP

Sanoïa
e-health for the real life

SAMSUNG

ST
life.augmented

TRUSTED OBJECTS

WISeKey

winbond

INTERNET OF TRUST

Laboratories

leti
ceatech

KEOLABS

SERMA
TECHNOLOGIES

brightsight
the number one security lab in the world

Cabinet Louis Reynaud

RED ALERT LABS
IoT Security

(TIC) Testing, Inspection, Certification

SGS

BUREAU VERITAS

TRUSTCB
TRUST AND VERIFY

Associations

SECURED COMMUNICATING SOLUTIONS

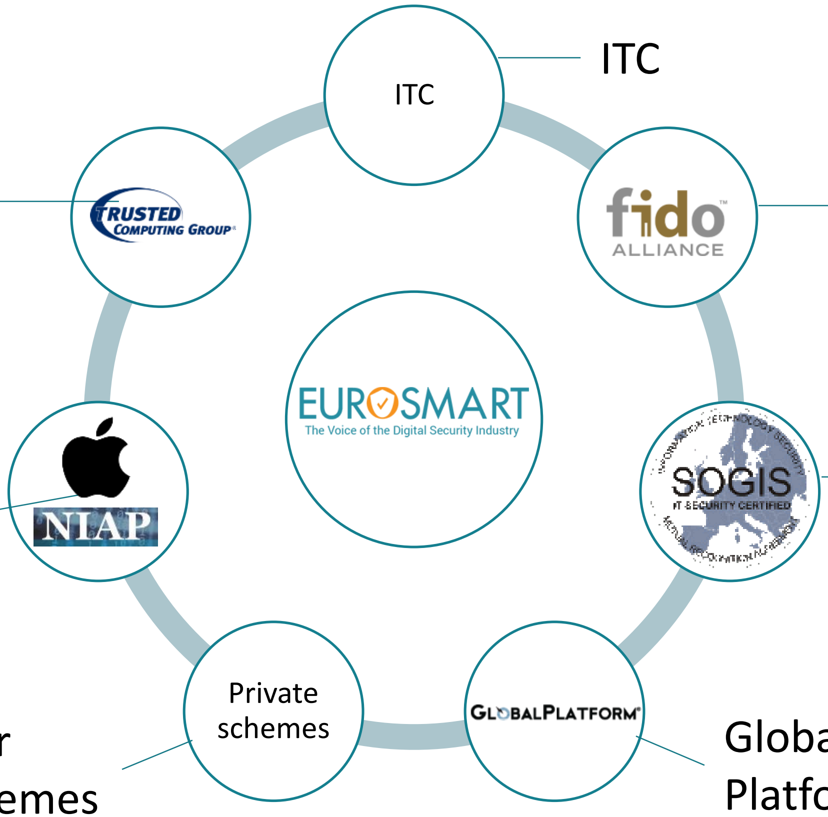
SMART PAYMENT ASSOCIATION

Academics and Research Organisations

Fraunhofer
AISEC

ISEN
ALL IS DIGITAL!
yncréa

Certification Scheme contribution


ITC
TRUSTED COMPUTING GROUP
fido ALLIANCE
EUROSMART The Voice of the Digital Security Industry
NIAP
SOGIS IT SECURITY CERTIFIED
Private schemes
GLOBALPLATFORM

ITC

TCG

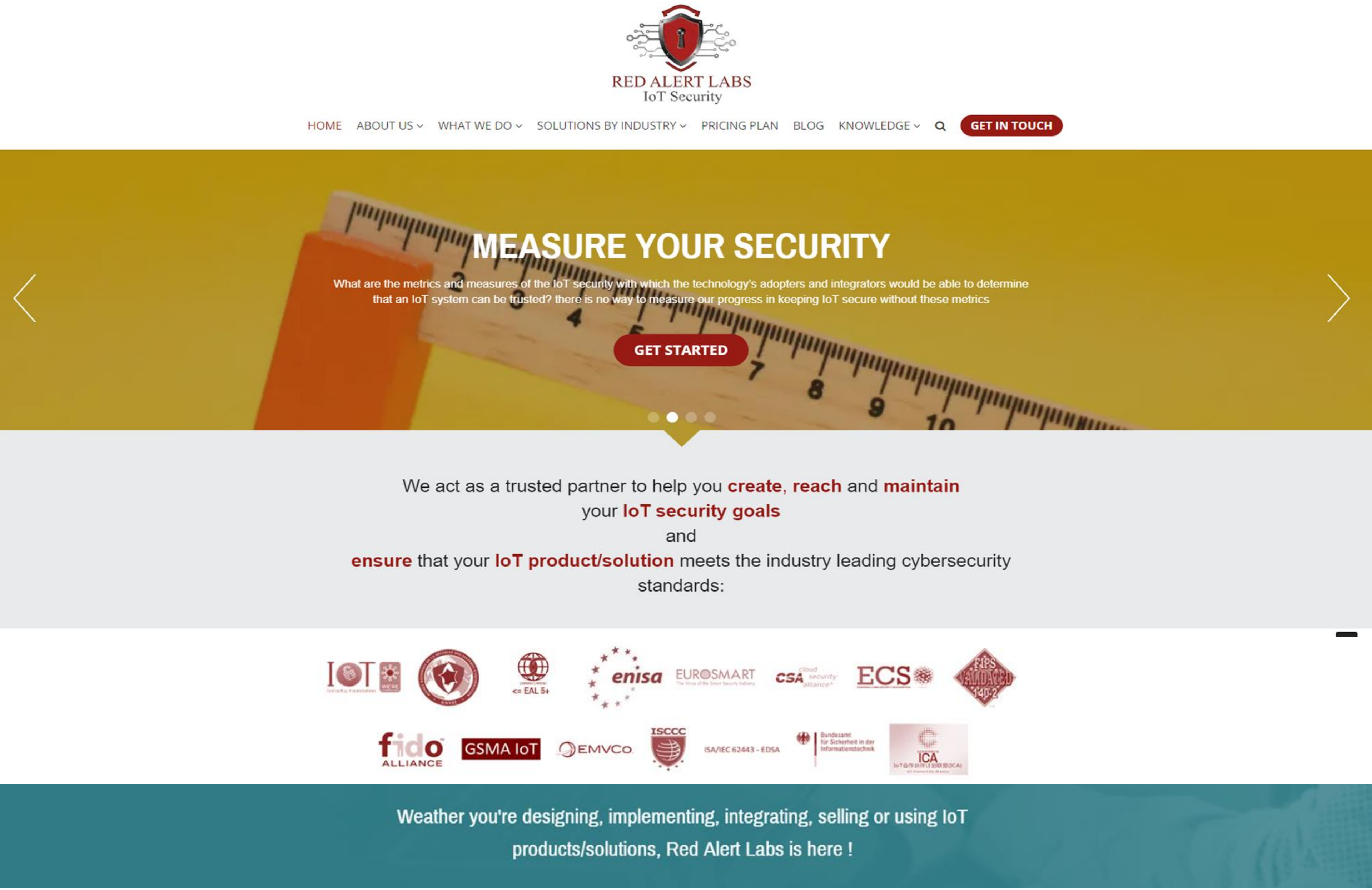
FIDO alliance

ITC
Apple/NIAP

SOG-IS

Many other private schemes

Global Platform



MEASURE YOUR SECURITY

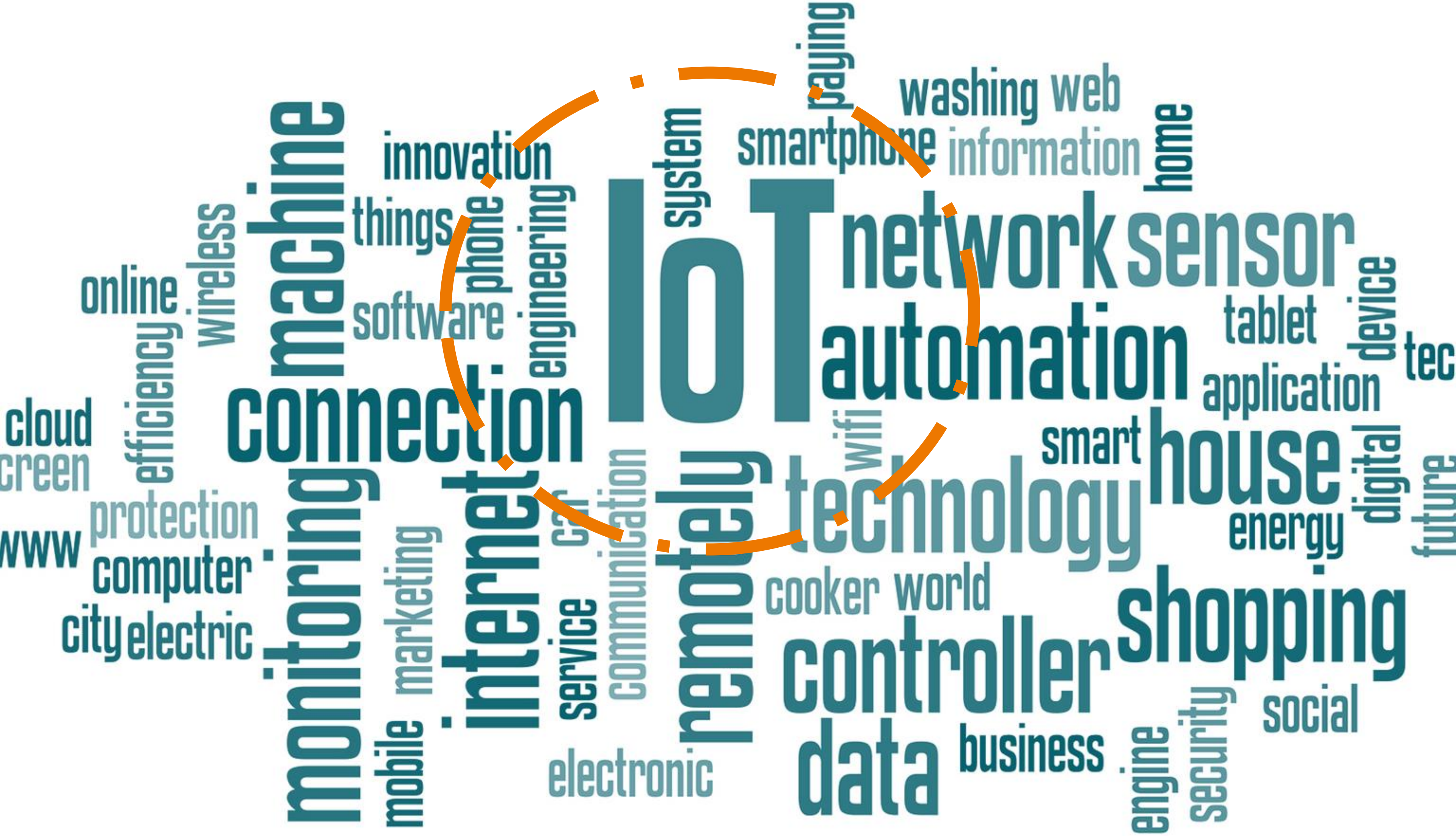
What are the metrics and measures of the IoT security with which the technology's adopters and integrators would be able to determine that an IoT system can be trusted? there is no way to measure our progress in keeping IoT secure without these metrics

We act as a trusted partner to help you **create**, **reach** and **maintain** your **IoT security goals** and **ensure** that your **IoT product/solution** meets the industry leading cybersecurity standards:

Weather you're designing, implementing, integrating, selling or using IoT products/solutions, Red Alert Labs is here !

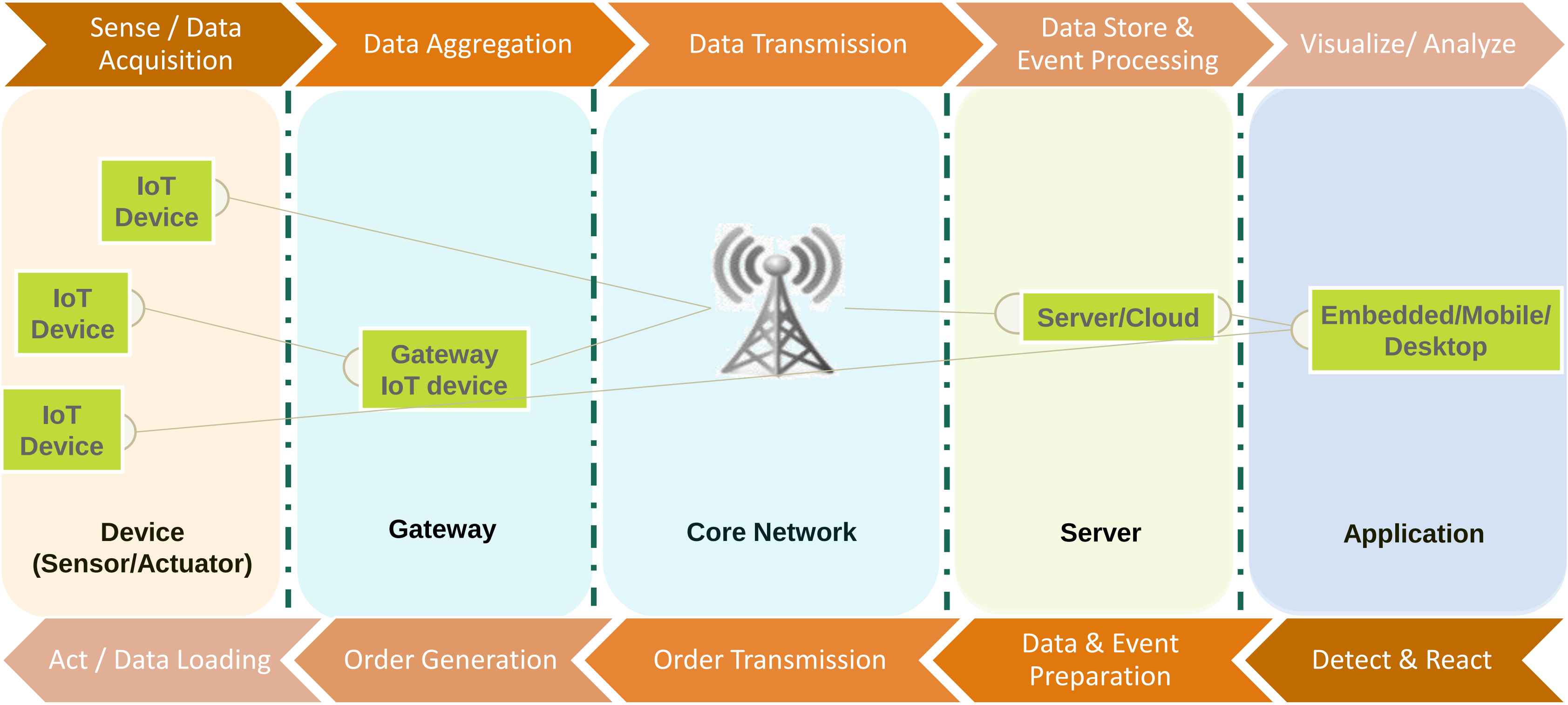
https://www.redalertlabs.com

A


IoT
network
sensor
automation
connection
machine
monitoring
internet
remotely
technology
house
shopping
controller
data
paying
washing
web
smartphone
information
home
system
innovation
things
phone
engineering
software
online
wireless
efficiency
cloud
creen
www
protection
computer
city
electric
marketing
mobile
service
car
communication
electronic
wifi
smart
tablet
device
tec
application
digital
future
energy
cooker
world
business
engine
security
social

Typical IoT Infrastructure

RED ALERT LABS
IoT Security



EUROSMART
The Voice of the Digital Security Industry

A lot of Benefits … with high security risk !

Fraud & Misuse

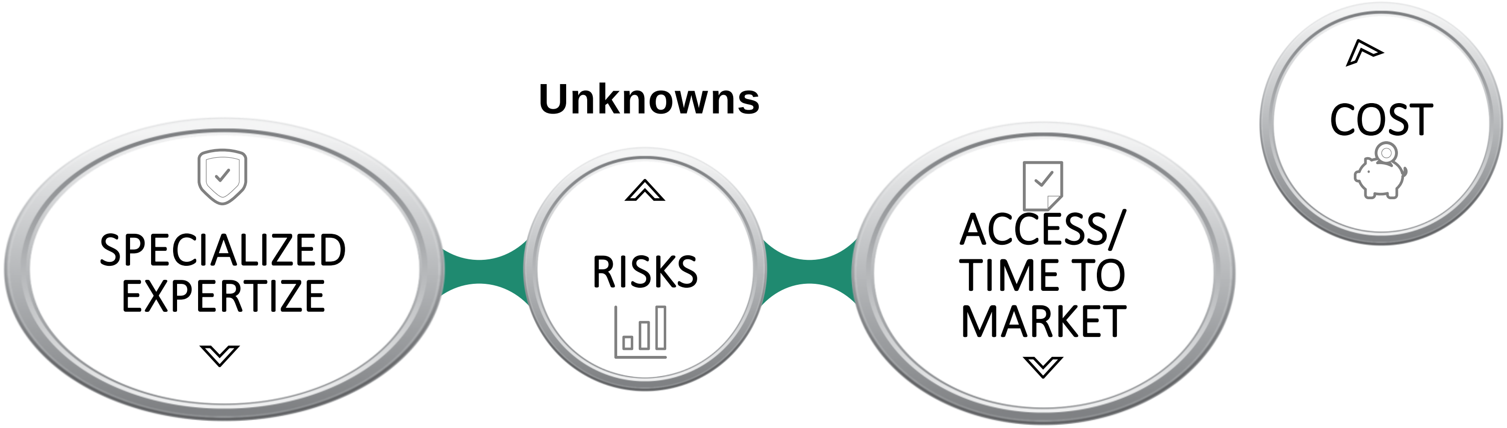
Privacy

Safety

~25 billions
in
2021

Gartner forecast 2019

Vendors Problems !



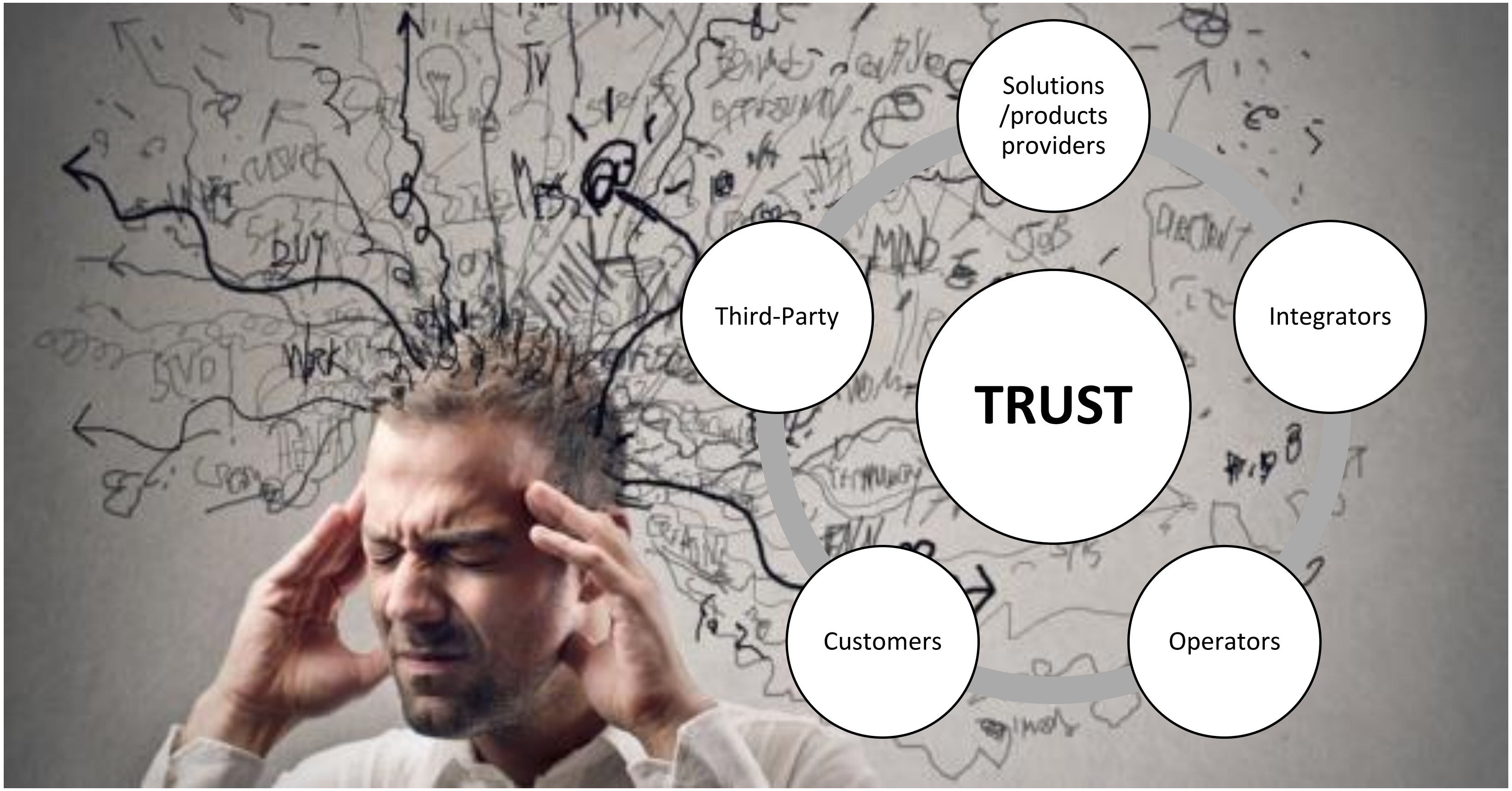
Lack of Incentive & Awareness

Unknowns

Lack of Security Experts

Compliance & Regulations vs. TTM

Users/Service Providers Problem !



TRUST

Solutions /products providers

Integrators

Operators

Customers

Third-Party

http://www.flickr.com/photos/lwr/

“**TRUST** should be further **strengthened** by offering information in a **transparent** manner on the **level of security** of ICT products, ICT services and ICT processes …”

“An **increase in trust** can be facilitated by **Union-wide CERTIFICATION** providing for **common cybersecurity requirements** and **evaluation criteria** across national markets and sectors.”

EU Cybersecurity Act – Section (7)

CERTIFICATION → TRUST

WITH THE NEW EU CSA REGULATION WE NEED A NEW CERTIFICATION SCHEME FOR IoT TO TACKLE :

- Cost, time, validity
  - Can’t be applied to the 25 Billion IoT product market ! Not enough resources to do that…
- Subjective
  - What is the credibility of the evaluation lab/pentester/etc.? What does secure mean? Can we compare more or less secure products?
- Scope
  - Silo Approach - they often cover part of the problem, specific to an industry (banking, ID) but security & privacy is now a concern of every business and citizen.
- Poor Security Definition
  - There is no common and holistic approach to define security requirements per profile taking into account the threat model & risks due to the intended usage

AT EUROSMART WE HAVE PREPARED :

A Tailor Made
IoT Device
Certification
Scheme

SOLVING BOTH VENDORS and USERS PROBLEMS...

Eurosmart IoT Security Certification Scheme

E-IoT-SCS

E-IoT SCS

The scope of this certification scheme is the **IoT device** while taking into account the full threat model (from Chip to Cloud) with a focus on the **Basic & Substantial** security assurance level as defined by the **Cybersecurity Act**.

The purpose is to ensure that IoT devices certified under this scheme comply with **specified requirements defined in a risk-based approach and supported by the industry** with the aim to protect the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions or services offered by, or accessible via IoT devices **throughout their life cycle**.

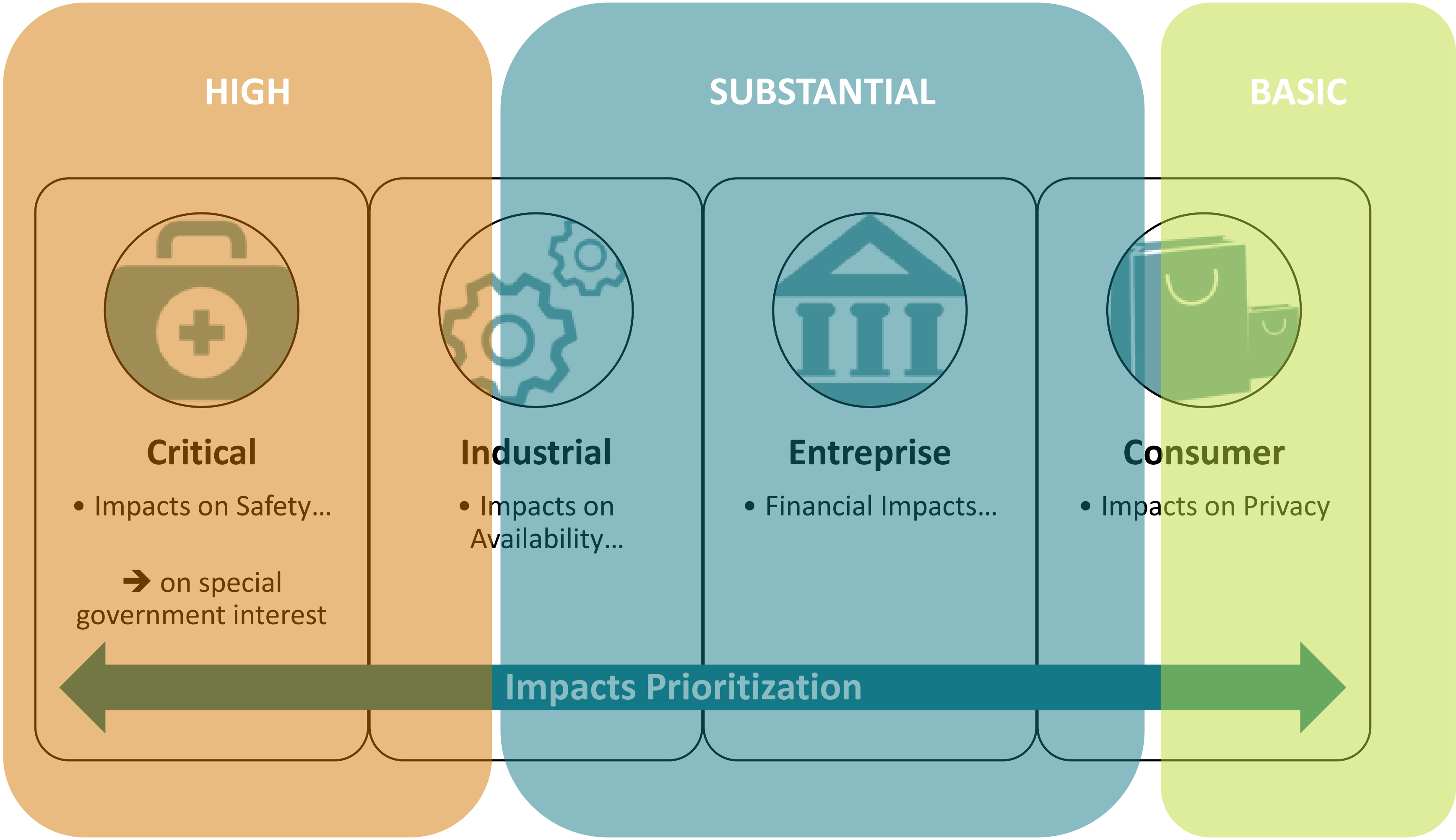
3 Security Assurance Levels – From Basic to Substantial

- **Basic**
  - Minimize the known basic risks of incidents and cyberattacks

- **Substantial**
  - Minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources

- **High**
  - Minimize the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources

RISK-BASED IoT MARKET VERTICALS



HIGH

SUBSTANTIAL

BASIC

Critical

- Impacts on Safety…

➔ on special government interest

Industrial

- Impacts on Availability…

Entreprise

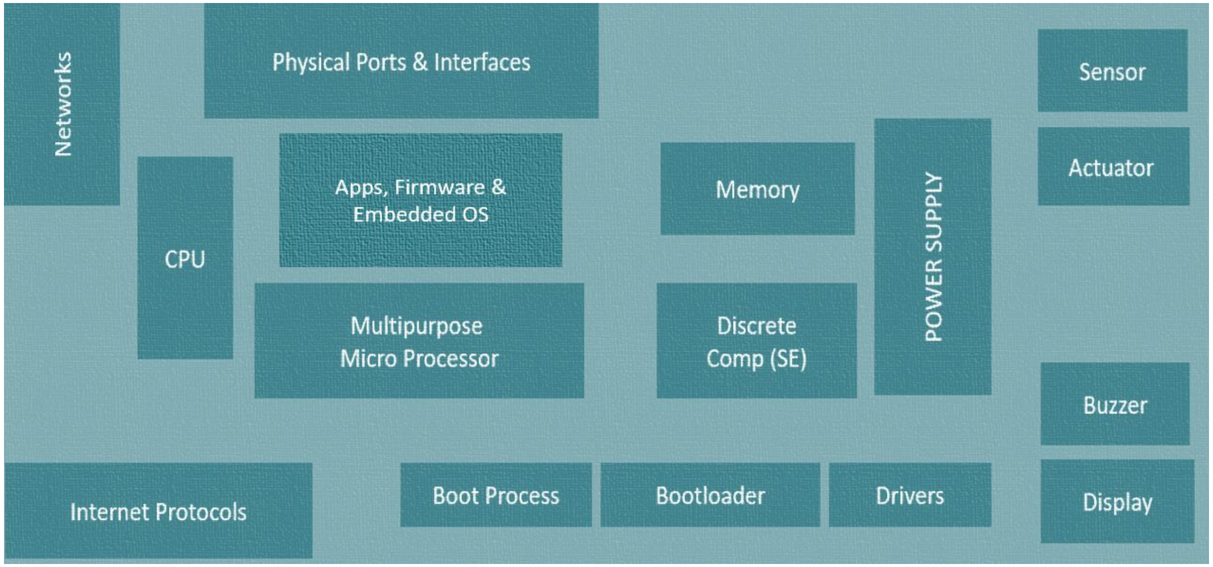
- Financial Impacts…

Consumer

- Impacts on Privacy

Impacts Prioritization

Multi-Sensor — Sigfox



Networks

Physical Ports & Interfaces

Sensor

Actuator

CPU

Apps, Firmware & Embedded OS

Memory

POWER SUPPLY

Multipurpose Micro Processor

Discrete Comp (SE)

Buzzer

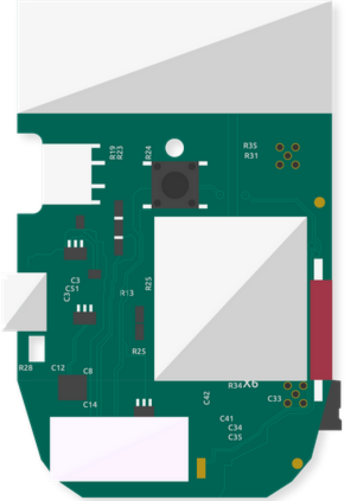
Internet Protocols

Boot Process

Bootloader

Drivers

Display



Custom antenna
Great performance for all Radio Configurations

250mAh battery
Enough for several months of lifetime (depending on the use case)

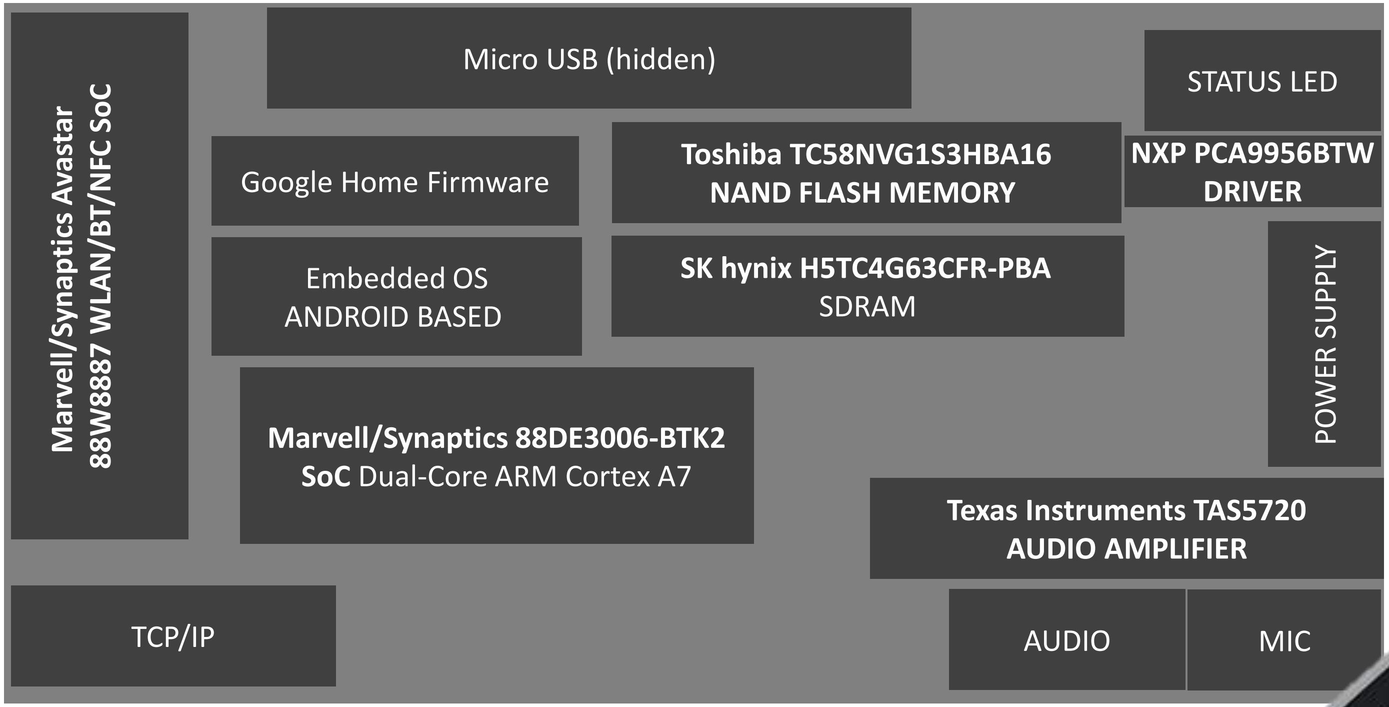
Micro-USB port
Recharge the device and dump firmware

Central RGB LED
Improves user experience

STM32 micro-controller
Controls the device

TI CC1125 radio transceiver
The core of the unique multi-RCs RF design

SMART SPEAKER - Wifi



Marvell/Synaptics Avastar 88W8887 WLAN/BT/NFC SoC

Micro USB (hidden)

STATUS LED

Google Home Firmware

Toshiba TC58NVG1S3HBA16 NAND FLASH MEMORY

NXP PCA9956BTW DRIVER

Embedded OS ANDROID BASED

SK hynix H5TC4G63CFR-PBA SDRAM

POWER SUPPLY

Marvell/Synaptics 88DE3006-BTK2 SoC Dual-Core ARM Cortex A7

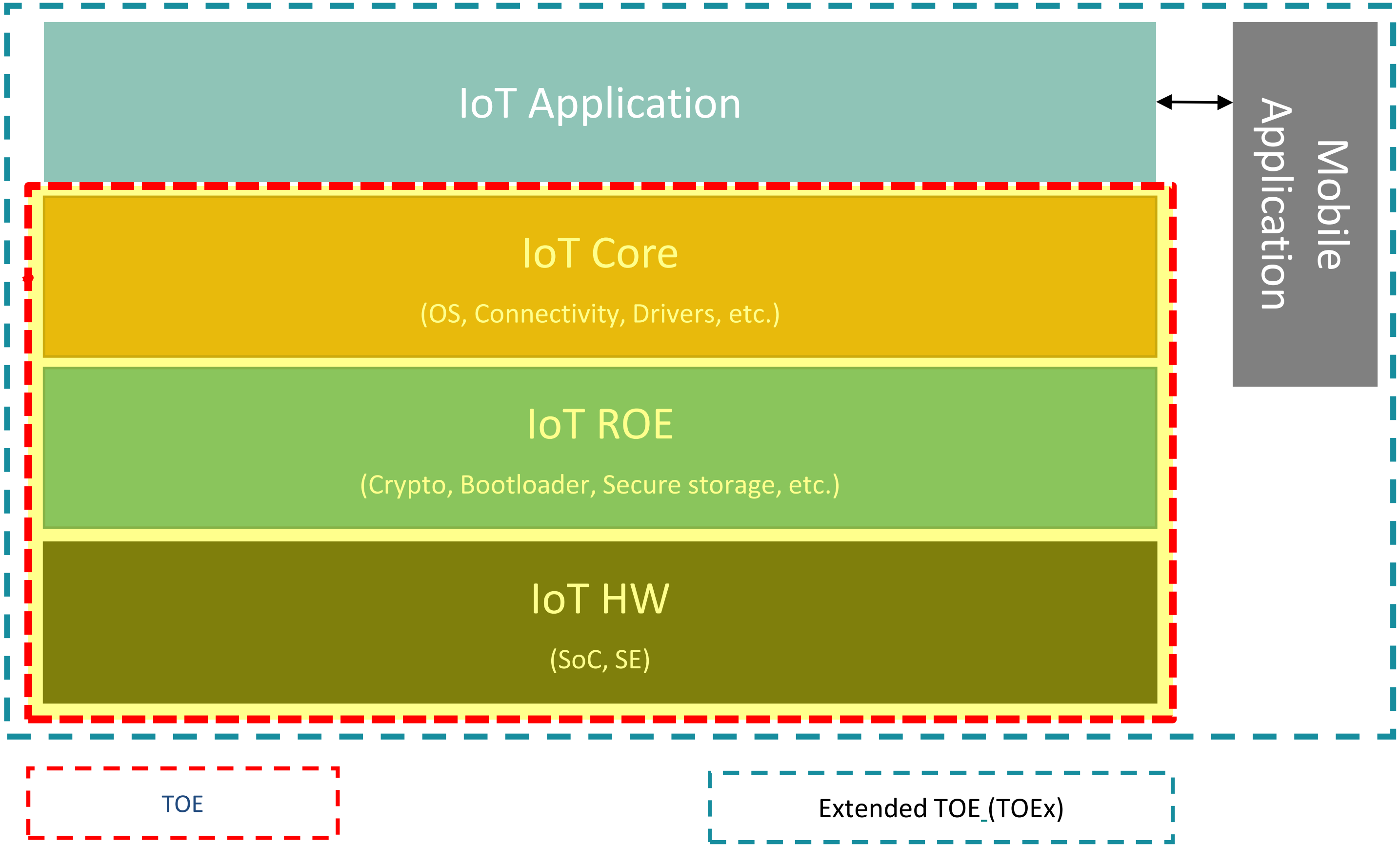
Texas Instruments TAS5720 AUDIO AMPLIFIER

TCP/IP

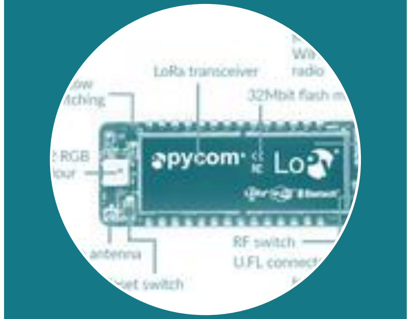
AUDIO

MIC

MODULAR TOE


IoT Application
Mobile Application
IoT Core
(OS, Connectivity, Drivers, etc.)
IoT ROE
(Crypto, Bootloader, Secure storage, etc.)
IoT HW
(SoC, SE)
TOE
Extended TOE (TOEx)

TARGETED AUDIENCE



IoT
DEVICE
VENDOR

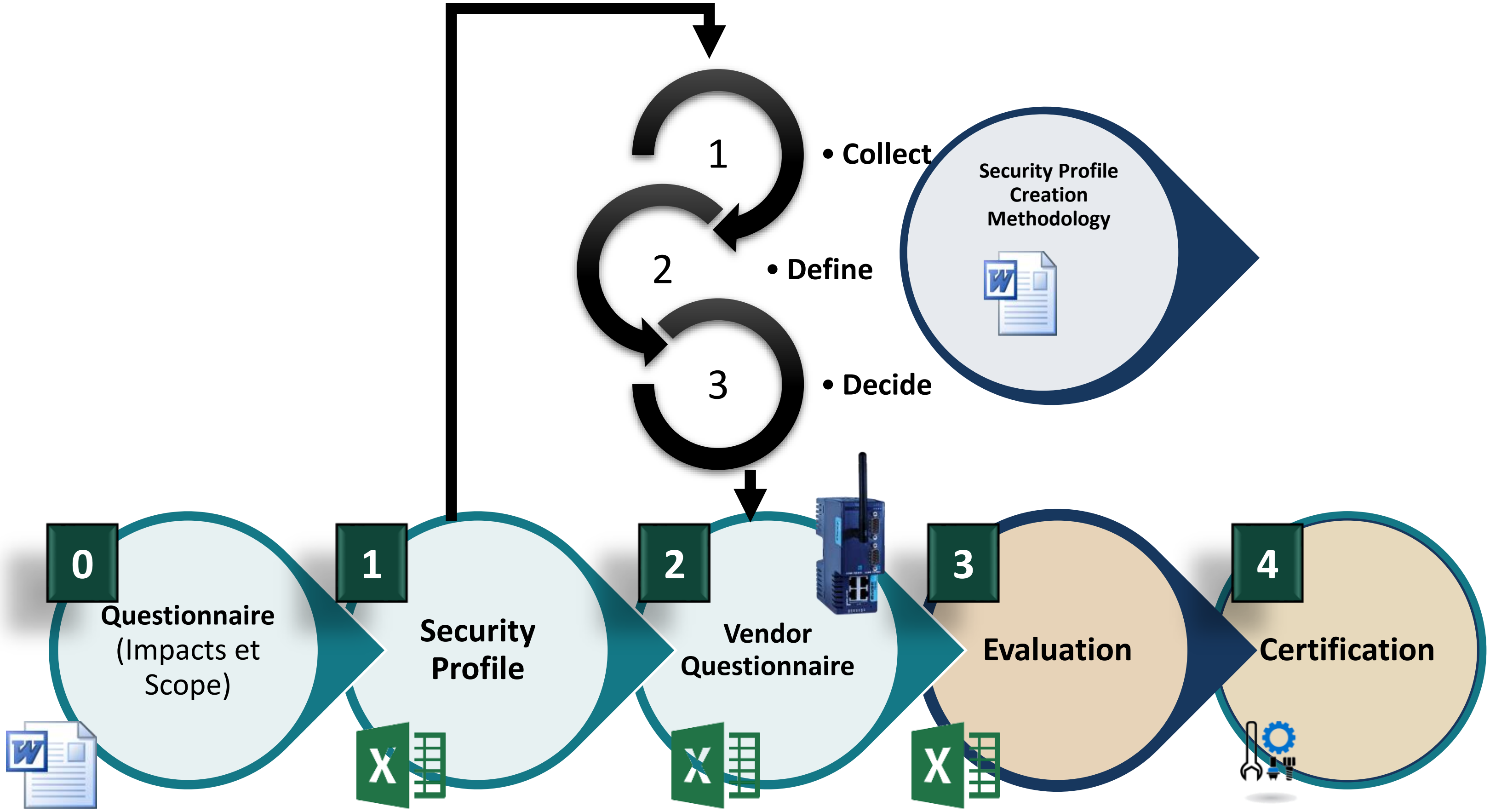
IoT
PRODUCT
VENDOR

IoT
SERVICE
PROVIDER

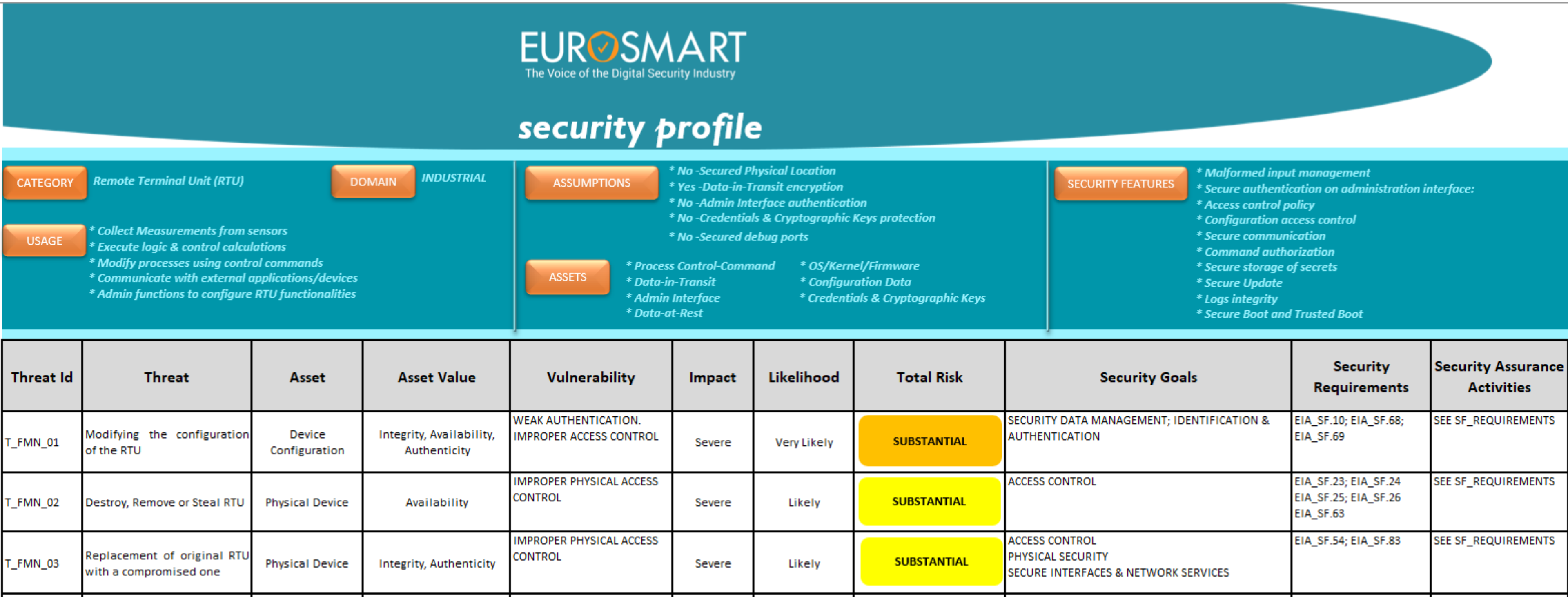
IoT
DEVICE
OWNER

SPONSORS | CONSUMERS

VENDOR's STEPS



A security profile looks like this:



EUROSMART
The Voice of the Digital Security Industry

security profile

CATEGORY Remote Terminal Unit (RTU)

DOMAIN INDUSTRIAL

USAGE
* Collect Measurements from sensors
* Execute logic & control calculations
* Modify processes using control commands
* Communicate with external applications/devices
* Admin functions to configure RTU functionalities

ASSUMPTIONS
* No -Secured Physical Location
* Yes -Data-in-Transit encryption
* No -Admin Interface authentication
* No -Credentials & Cryptographic Keys protection
* No -Secured debug ports

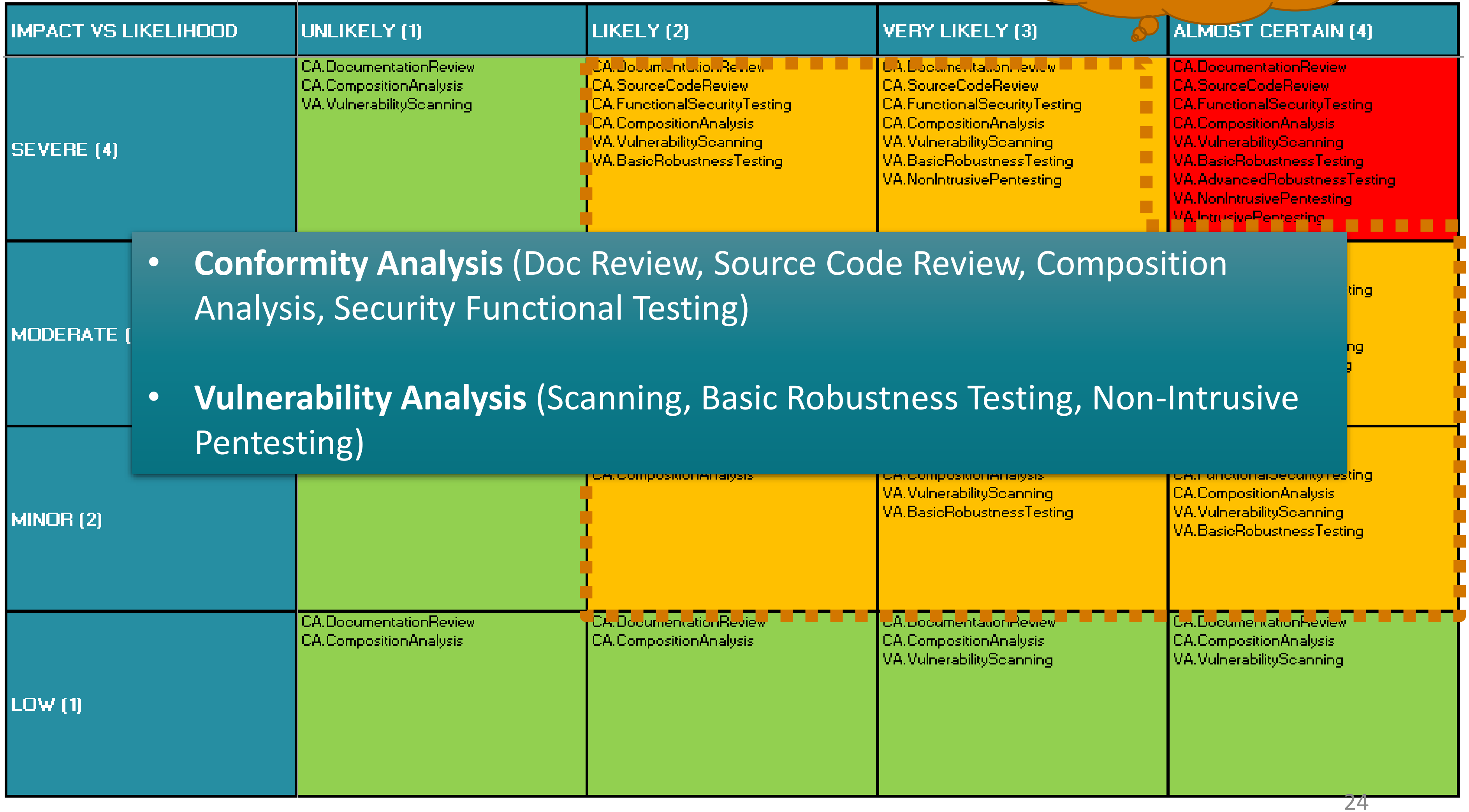
ASSETS
* Process Control-Command
* Data-in-Transit
* Admin Interface
* Data-at-Rest
* OS/Kernel/Firmware
* Configuration Data
* Credentials & Cryptographic Keys

SECURITY FEATURES
* Malformed input management
* Secure authentication on administration interface:
* Access control policy
* Configuration access control
* Secure communication
* Command authorization
* Secure storage of secrets
* Secure Update
* Logs integrity
* Secure Boot and Trusted Boot

Threat Id	Threat	Asset	Asset Value	Vulnerability	Impact	Likelihood	Total Risk	Security Goals	Security Requirements	Security Assurance Activities
T_FMN_01	Modifying the configuration of the RTU	Device Configuration	Integrity, Availability, Authenticity	WEAK AUTHENTICATION. IMPROPER ACCESS CONTROL	Severe	Very Likely	SUBSTANTIAL	SECURITY DATA MANAGEMENT; IDENTIFICATION & AUTHENTICATION	EIA_SF.10; EIA_SF.68; EIA_SF.69	SEE SF_REQUIREMENTS
T_FMN_02	Destroy, Remove or Steal RTU	Physical Device	Availability	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL	EIA_SF.23; EIA_SF.24 EIA_SF.25; EIA_SF.26 EIA_SF.63	SEE SF_REQUIREMENTS
T_FMN_03	Replacement of original RTU with a compromised one	Physical Device	Integrity, Authenticity	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL PHYSICAL SECURITY SECURE INTERFACES & NETWORK SERVICES	EIA_SF.54; EIA_SF.83	SEE SF_REQUIREMENTS

RISK-BASED - SECURITY ASSURANCE ACTIVITIES

SUBSTANTIAL

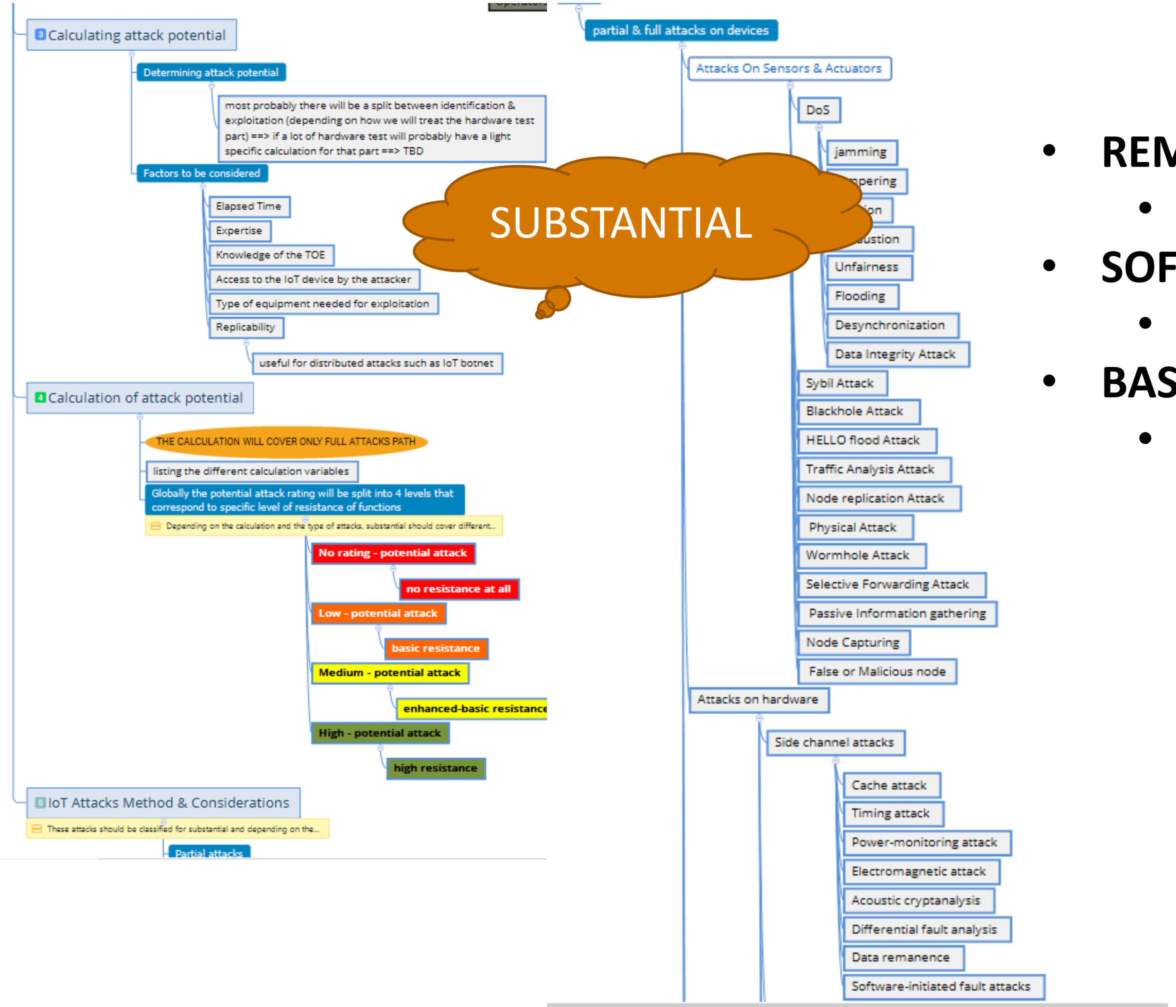


IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)	CA.DocumentationReview CA.CompositionAnalysis VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.NonIntrusivePentesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting VA.IntrusivePentesting
MODERATE (				ting ng g
MINOR (2)		CA.CompositionAnalysis	CA.CompositionAnalysis VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.FunctionalSecurityTesting CA.CompositionAnalysis VA.VulnerabilityScanning VA.BasicRobustnessTesting
LOW (1)	CA.DocumentationReview CA.CompositionAnalysis	CA.DocumentationReview CA.CompositionAnalysis	CA.DocumentationReview CA.CompositionAnalysis VA.VulnerabilityScanning	CA.DocumentationReview CA.CompositionAnalysis VA.VulnerabilityScanning

- **Conformity Analysis** (Doc Review, Source Code Review, Composition Analysis, Security Functional Testing)

- **Vulnerability Analysis** (Scanning, Basic Robustness Testing, Non-Intrusive Pentesting)

Attackers Profiles are methodologically selected for Each Security Profile in a risk-based approach



SUBSTANTIAL

- 3 Calculating attack potential
  - Determining attack potential
    - most probably there will be a split between identification & exploitation (depending on how we will treat the hardware test part) ==> if a lot of hardware test will probably have a light specific calculation for that part ==> TBD
  - Factors to be considered
    - Elapsed Time
    - Expertise
    - Knowledge of the TOE
    - Access to the IoT device by the attacker
    - Type of equipment needed for exploitation
    - Replicability
      - useful for distributed attacks such as IoT botnet
- 4 Calculation of attack potential
  - THE CALCULATION WILL COVER ONLY FULL ATTACKS PATH
  - listing the different calculation variables
  - Globally the potential attack rating will be split into 4 levels that correspond to specific level of resistance of functions
    - Depending on the calculation and the type of attacks, substantial should cover different...
    - No rating - potential attack
      - no resistance at all
    - Low - potential attack
      - basic resistance
    - Medium - potential attack
      - enhanced-basic resistance
    - High - potential attack
      - high resistance
- 5 IoT Attacks Method & Considerations
  - These attacks should be classified for substantial and depending on the...
  - Partial attacks

- partial & full attacks on devices
  - Attacks On Sensors & Actuators
    - DoS
      - jamming
      - pering
      - ion
      - ustion
      - Unfairness
      - Flooding
      - Desynchronization
      - Data Integrity Attack
    - Sybil Attack
    - Blackhole Attack
    - HELLO flood Attack
    - Traffic Analysis Attack
    - Node replication Attack
    - Physical Attack
    - Wormhole Attack
    - Selective Forwarding Attack
    - Passive Information gathering
    - Node Capturing
    - False or Malicious node
  - Attacks on hardware
    - Side channel attacks
      - Cache attack
      - Timing attack
      - Power-monitoring attack
      - Electromagnetic attack
      - Acoustic cryptanalysis
      - Differential fault analysis
      - Data remanence
      - Software-initiated fault attacks

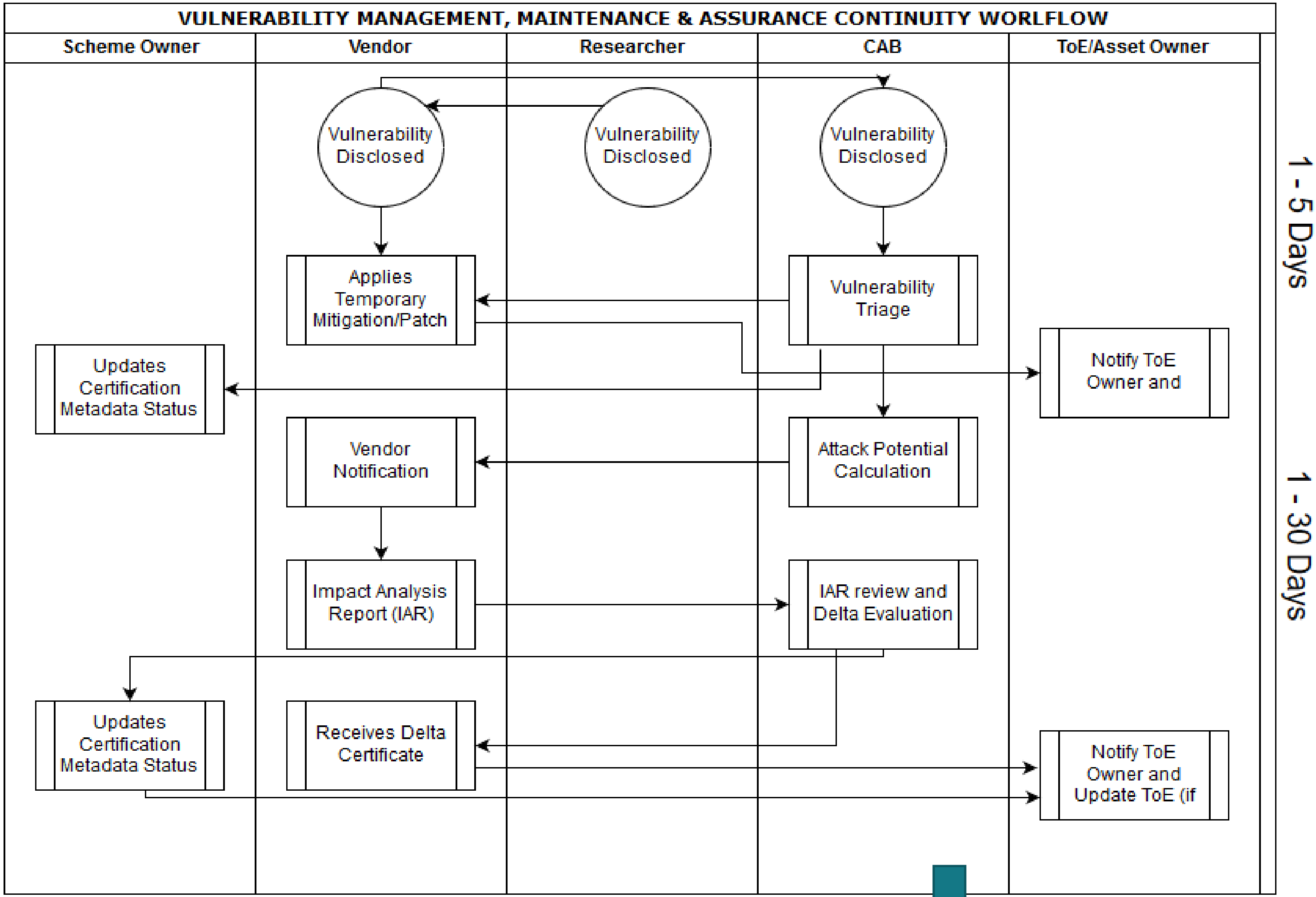
- **REMOTE SCALABLE ATTACKS**
  - (Covered by default)
- **SOFTWARE ATTACKS**
  - (Might be covered)
- **BASIC PHYSICAL ATTACKS**
  - (Might be covered)

Temporary Mitigation/Patching

- **Application Layer:**
  - patching with Integration mechanisms are verified once for all by the CAB
- **Core, ROE, HW Layers:**
  - patching first… evaluating later !
    - if and only if the vendor demonstrated a secure maintenance life-cycle process satisfying the flaw remediation requirements.
  - temporary measures will be deployed by the vendor within the time as specified in the Vulnerability Triage Protocol.

ADAPTED ASSURANCE CONTINUITY

Active Monitoring/Vulnerability Surveillance


VULNERABILITY MANAGEMENT, MAINTENANCE & ASSURANCE CONTINUITY WORLFLOW
Scheme Owner
Vendor
Researcher
CAB
ToE/Asset Owner
Vulnerability Disclosed
Vulnerability Disclosed
Vulnerability Disclosed
Applies Temporary Mitigation/Patch
Vulnerability Triage
Updates Certification Metadata Status
Notify ToE Owner and
Vendor Notification
Attack Potential Calculation
Impact Analysis Report (IAR)
IAR review and Delta Evaluation
Updates Certification Metadata Status
Receives Delta Certificate
Notify ToE Owner and Update ToE (if
1 - 5 Days
1 - 30 Days

[TR-e-IoT-SCS-Part-6]

KEY BENEFITS

AUTOMATISATION & AGILE METHODOLOGY

01

Security Reqs/Questionnaire acts as guidelines, not much overhead evidence docs, and reduced testing time

7-15 m/d w/ security profile

RECOGNIZE EXISTING EVALUATION METHODOLOGY

02

Requirements could be simply mapped to other certification schemes allowing recognition of existing methodologies by composition such as SOGIS CC evaluations for underlying platforms. In any case all types and formats of evidence could be reused as is under this Scheme.

REDUCE COSTS

03

The evaluation addresses priorities and is time-constrained, thus limiting its delays and cost, but still offering a guarantee that experts have spent time analyzing the product most valuable security functionalities

7K€ – 15K€

(in average)

COMPARE IOT DEVICES

04

The accurate evaluation scope coupled with the security functionalities and the defined set of security requirements are a result of accurate security analysis/threat modelling, The Evaluation metrics and ratings are simple and expressive

REQUIREMENTS TAILORED TO THE INTENDED USE

05

the scope of evaluation focuses on the HW & SW forming the IoT Device but the threat model covers the operational environment including the final application, interfaces and other components connected to the product if any..

KEY BENEFITS

06 COST-EFFICENT CERTIFICATION MAINTENANCE

This Scheme provides a smart framework to define, attest and maintain the certificates delivered for IoT devices after issuance . Patching & Temporary Mitigation are allowed.

07 CREATE INCENTIVE FOR VENDORS

Minimum Effort required on providing evidence, simple metrics, clear requirements, security valued by customer

08 INVOLVE IOT SERVICE PROVIDERS

Expressing SUBSTANTIAL Level Rating + Community creating awareness. IoT Service Providers and Customers trust the vendors

09 SIMPLE METRICS

Requirements and Test Procedures are expressed in simple wording allowing the vendors and CABs to implement and test efficiently.

10 CYBER SECURITY ACT COMPLIANT

This Scheme is a first world-wide to be created while incorporating the Cybersecurity Act principles by design.

	EU CYBERSECURITY ACT - ARTICLE 54	COVERAGE BY THIS SCHEME
(a)	subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services	[TR-e-IoT-SCS-Part-1], Chapter 1 + Executive Summary
(b)	a clear description of the purpose of the scheme and how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme.	[TR-e-IoT-SCS-Part-1], Chapter 1 + Executive Summary
(c)	references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II of Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;	[TR-e-IoT-SCS-Part-1], Section 1.3
(d)	where applicable, one or more assurance levels;	[TR-e-IoT-SCS-Part-1], Section 1.1 (BASIC & SUBSTANTIAL LEVEL)
(e)	an indication of whether conformity self-assessment of conformity is permitted under the scheme;	[TR-e-IoT-SCS-Part-3], Section 4.2.3 and Section 4.2.10
(f)	where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;	[TR-e-IoT-SCS-Part-5]
(g)	The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 51 are achieved;	[TR-e-IoT-SCS-Part-3]
(h)	where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;	[TR-e-IoT-SCS-Part-1], Section 4.1 [TR-e-IoT-SCS-Part-3] and [TR-e-IoT-SCS-Part-9]
(i)	where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;	[TR-e-IoT-SCS-Part-7]
(j)	rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;	[TR-e-IoT-SCS-Part-1], Section 4.2 and [TR-e-IoT-SCS-Part-6]
(k)	where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;	[TR-e-IoT-SCS-Part-1], Section 6
(l)	rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;	[TR-e-IoT-SCS-Part-1], Section 6.1.4.4.
(m)	rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;	[TR-e-IoT-SCS-Part-1] Section 6.1, 6.1.4 and [TR-e-IoT-SCS-Part-6]
(n)	where applicable, rules concerning the retention of records by conformity assessment bodies;	[TR-e-IoT-SCS-Part-1], Section 4.2
(o)	the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;	Refer to "e-IoT-SCS Candidate Certification Scheme Pre-Study – v1.0 RELEASE" – [Deliverables Annex], and [TR-e-IoT-SCS-Part-3]
(p)	the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;	[TR-e-IoT-SCS-Part-9]
(q)	the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;	[TR-e-IoT-SCS-Part-1], Section 5.2
(r)	maximum period of validity of European cybersecurity certificates issued under the scheme;	[TR-e-IoT-SCS-Part-1], Section 6
(s)	disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;	[TR-e-IoT-SCS-Part-1], Section 7
(t)	conditions for the mutual recognition of certification schemes with third countries;	[TR-e-IoT-SCS-Part-1], Section 1.7
(u)	where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;	N/A – Not relevant to the Basic & Substantial level
(v)	format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.	[TR-e-IoT-SCS-Part-1], Section 4.1 [TR-e-IoT-SCS-Part-3] and [TR-e-IoT-SCS-Part-9]

CERTIFICATION EXPECTED DURATION SUBSTANTIAL

5-12 MAN/DAYS

- Security Profile Creation

2-5 MAN/DAYS

- Vendor Questionnaire Analysis
- Conformity Analysis (docs)

5-10 MAN/DAYS

- Vulnerability Analysis
- Evaluation Report Creation (Template)
- Evaluation Report Review
- Certificate Issuance

5-12 + 7-15 MAN/DAYS

Pre-defined by the **Security Profile**

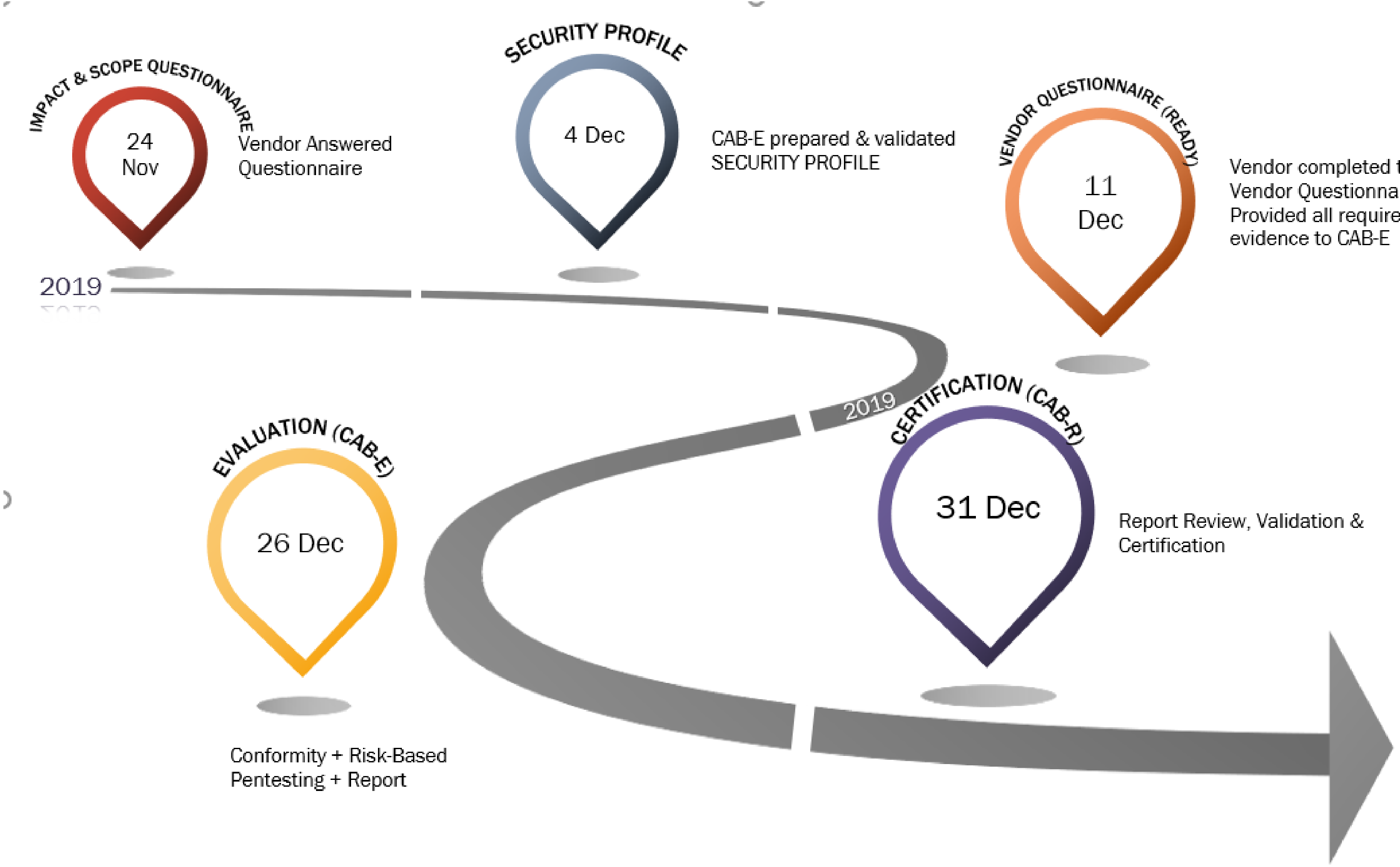
CERTIFICATION EXPECTED DURATION BASIC

0 MAN/DAYS (e.g. ETSI..)	• Security Profile Baseline (could be by domain => consumer, enterprise, industrial…)
1-2 MAN/DAYS	• Vendor Questionnaire Analysis • Conformity Analysis (docs)
0.5-1 MAN/DAYS	• Vulnerability Scanning • Evaluation Report Creation (Template) • Certificate Issuance

0 + 1.5-3 MAN/DAYS

Depending on **the domain**

JOIN
THE PILOT CERTIFICATION PHASE (EXTENDED)



Vendor Answered Questionnaire

CAB-E prepared & validated SECURITY PROFILE

Vendor completed the Vendor Questionnaire & Provided all required evidence to CAB-E

Conformity + Risk-Based Pentesting + Report

Report Review, Validation & Certification

JOIN → https://www.eurosmart.digital/eurosmart-iot-certification-scheme/

R

All Documents are FREE for Download Online

https://www.eurosmart.digital/eurosmart-iot-certification-scheme/

OPEN SOURCES

The END…

Don't forget to buy milk!
In your dreams… Go get Certified first !

THANK YOU

R

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Red Alert Labs

3 rue Parmentier | 94140 Alfortville | FRANCE

contact@redalertlabs.com
Tel. +33 9 53 55 54 11
www.redalertlabs.com
@RedAlertLabs

Eurosmart

Rue de la Science 14b | 1040 Brussels | BELGIUM

pierrejean.verrando@eurosmart.com
Tel. +32 2 880 36 35
www.eurosmart.com
@Eurosmart_EU

RED ALERT LABS
IoT Security

2019 INTERNATIONAL CONFERENCE ON THE EU CYBERSECURITY ACT

ANNEX

EUROSMART
The Voice of the Digital Security Industry

E-IoT-SCS Core Documentation

Reference	Name/Description
[TR-e-IoT-SCS-Part-1]	E-IoT-SCS Process & Policy - This document defines the policies and processes that govern the IoT device certification scheme.
[TR-e-IoT-SCS-Part-2]	E-IoT-SCS Generic Protection Profile + Security Requirements Methodology - This document is a generic representation of common security requirements on IoT devices. It is based on a security risk analysis approach of an IoT Device operating in a typical infrastructure without considering a specific type of data or a context for risk calculation. The main output of this document is a list of security goals and requirements qualifying the need to counter security threats identified on a typical IoT device.
[TR-e-IoT-SCS-Part-3]	E-IoT-SCS Evaluation Methodology - Document defining the evaluation activities to be performed by an evaluator and links between them in order to conduct properly an evaluation. It lists evaluation evidences required to perform actions as defined in the security assurance requirements. It defines way to report evaluation results in Evaluation technical report and observation report. It also provides rules to define verdict and criteria of failure.

E-IoT-SCS Documentation

CABs Accreditation

Reference	Name/Description
[TR-e-IoT-SCS-Part-4]	CABs Agreement - Guidelines listing the rules for setting up agreement between CABs and Certification Scheme stakeholders (e.g. other CABs – CAB reviewer, CAB evaluator, NABs, etc.)
[TR-e-IoT-SCS-Part-5]	CABs Accreditation Policy - Guidelines describing policy for CABs accreditation

Certification Secure Life-Cycle Management

Reference	Name/Description
[TR-e-IoT-SCS-Part-6]	Vulnerability Management, Maintenance & Continuous Assurance Policy: Document describing vulnerability management procedures and the life-cycle management of the Certificate after issuance
[TR-e-IoT-SCS-Part-7]	Mark & Certificate Usage Policy for e-IoT Certification Scheme: Document describing the procedure and conditions which govern the use of the e-IoT SUBSTANTIAL mark and certificate by IoT device vendors, CABs and end-users
[TR-e-IoT-SCS-Part-8]	The Metadata Certification Policy for e-IoT Certification Scheme: Document describing the Metadata Certification Concept and Requirements guaranteeing the relevancy and Authenticity of the Certificates.

Supporting Documents

Reference	Name/Description
[TR-e-IoT-SCS-Part-9]	Templates (Vendor Questionnaire, Impact Analysis Report, Security Profile, Evaluation Report, Mapping Table Concept)
[Informative Annexes]	A set of informative annexes complementing the e-IoT Security Certification Scheme deliverables such as the "e-IoT-SCS Candidate Certification Scheme Pre-Study – v1.0 RELEASE", or "Risk Assessment Methodologies".

KEY DEFINITIONS

Generic Protection Profile (GPP)

This General Protection Profile (GPP) is a technical report which is based on a generic security risk analysis approach of an IoT Device reference architecture without considering a specific type of data or a context for risk calculation. The main output of this document is a list of security goals and requirements qualifying the need to counter threats identified on a typical IoT device.

[TR-e-IoT-SCS-Part-2]

VENDOR QUESTIONNAIRE

A Vendor Questionnaire (VQ) is a technical document including questions and instructions addressed to the vendor who's implementing the ToE. Responses to these questions are considered as evidence materials and must be provided by the vendor to support the evaluation process.The goal: allow the Vendor to reformulate and refine the security requirements of a Security Profile.

It will draw a list of questions and actions for both the Vendor and the CAB

- VA = actions addressed for the Vendor
- CA = actions addressed for the CAB

EUROSMART
The Voice of the Digital Security Industry

[TR-e-IoT-SCS-Part-9]

SECURITY PROFILE

A refinement of the GPP to address specific problem definition of a type of ToE (thermostat, smart cam, etc.) while considering the type and sensitivity of data and the context of the operational environment (e.g. Consumer, Enterprise, Industrial) and the risk factor.

They help to scale security controls and security-related process activities in accordance to the identified risks

A standardized security profile saves a detailed risk analysis for every new product instance.

3 step approach (collect, define and decide)

Risk-based Methodology

[TR-e-IoT-SCS-Part-2]

KEY DEFINITIONS

IoT SERVICE PROVIDER

The IoT Service Provider (IoTSP) could be the IoT device vendor itself or a third-party service provider such as IoT Cloud Platforms (e.g. Azure, AWS IoT, GE Predix, Oracle IoTCS, Google Cloud IoT, IBM Watson IoT, Microsoft Azure IoT Suite, PTC ThingWorx, Kaa Platform, Overkiz IoT Platform, etc.)

METADATA CERTIFICATION STATEMENT

An IoT Metadata Certification Statement (MCST) is a document containing information about a device's characteristics, features and capabilities arranged in a structured manner that can be read and understood by IoT service providers. The reporting format of the metadata statement is generic and therefore can be used to describe any device from any vendor

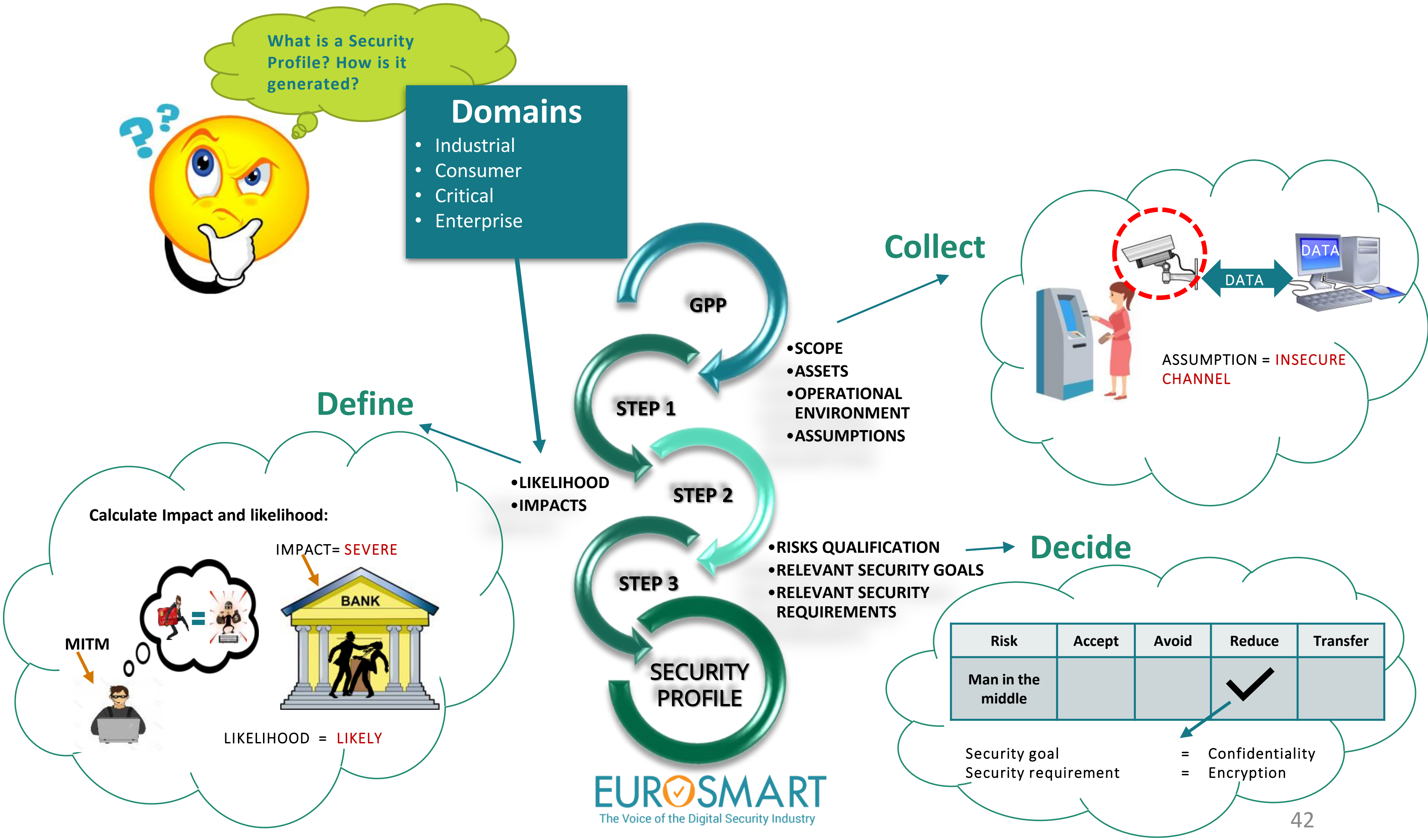
[TR-e-IoT-SCS-Part-8]

METADATA CERTIFICATION SERVICE

The IoT Metadata Certification Service (MCSE) is a web-based tool where CABs can, on behalf of IoT device vendors, upload signed metadata statements for IoT service providers to access and use as a source of trusted information about a specific device model. Service Providers for IoT Devices will naturally want to be able to trust a device that attempts to make use of their services this makes the deployment of "device metadata service" very useful, secure and scalable in quickly determining if a specific device model is trustworthy to access a resource.

[TR-e-IoT-SCS-Part-8]

SECURITY PROFILE ?



What is a Security Profile? How is it generated?

Domains

- Industrial
- Consumer
- Critical
- Enterprise

- SCOPE
- ASSETS
- OPERATIONAL ENVIRONMENT
- ASSUMPTIONS

Collect

ASSUMPTION = INSECURE CHANNEL

- LIKELIHOOD
- IMPACTS

Define

Calculate Impact and likelihood:

IMPACT= SEVERE

LIKELIHOOD = LIKELY

- RISKS QUALIFICATION
- RELEVANT SECURITY GOALS
- RELEVANT SECURITY REQUIREMENTS

Decide

Risk	Accept	Avoid	Reduce	Transfer
Man in the middle			✓	

Security goal = Confidentiality
Security requirement = Encryption

EUROSMART
The Voice of the Digital Security Industry

Example of Security Goals

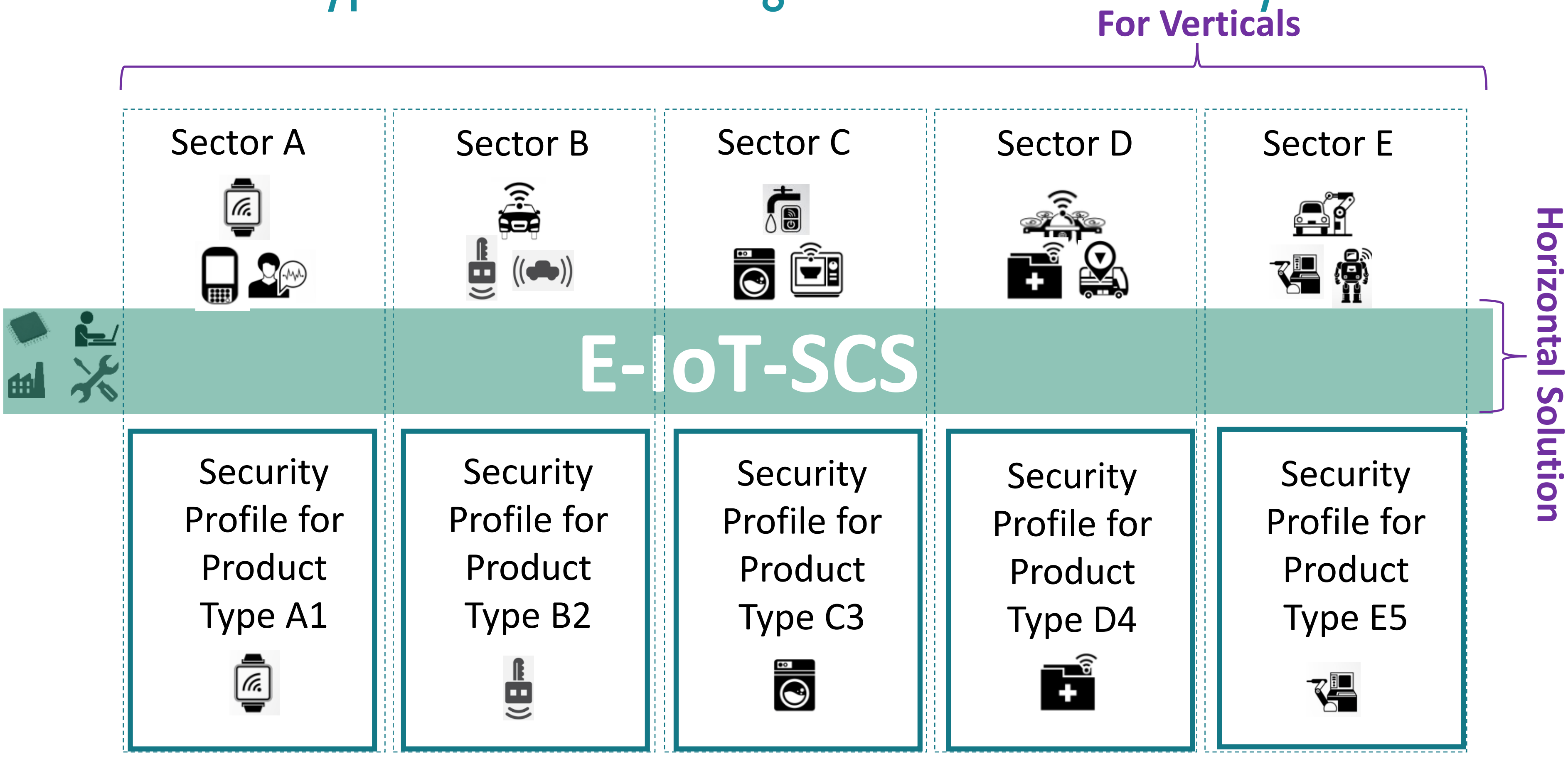
Security Goal (Sample)	Basic	Substantial	High
Strong Authentication		X	X
Firmware Integrity			X
Communication Integrity			X
Strong Encryption		X	X
Data Confidentiality		X	X
IP Protection	X	X	X
Data Availability		X	X
Data Privacy	X	X	X
Human Safety			X

Example of Security Requirements

Requirements (sample)	Basic	Substantial	High
Secure Manufacturer-based Identity & Certificate Storage		X	X
Secure Storage (Tamper Resistant)			X
RNG (FIPS or AIS)		X	X
SHA-256 at least		X	X
Secure Onboarding		X	X
Secure Firmware/SW update (digital signature)		X	X
Secure Event Logging		X	X
Limited Data Collection	X	X	X
End User Data Removal	X	X	X
Secure Cloud-Based Management Services		X	X
Active Product Incident Response Team		X	X
Secure Development Lifecycle (SDLC)			X
Data Privacy (Manufacturing)	X	X	X

IOT Devices may operate in different Operational Environments

➔ each type of IoT device might have several Security Profiles



For Verticals

Sector A

Sector B

Sector C

Sector D

Sector E

E-IoT-SCS

Horizontal Solution

Security Profile for Product Type A1

Security Profile for Product Type B2

Security Profile for Product Type C3

Security Profile for Product Type D4

Security Profile for Product Type E5

Ref. based on ECSO WG1 sources

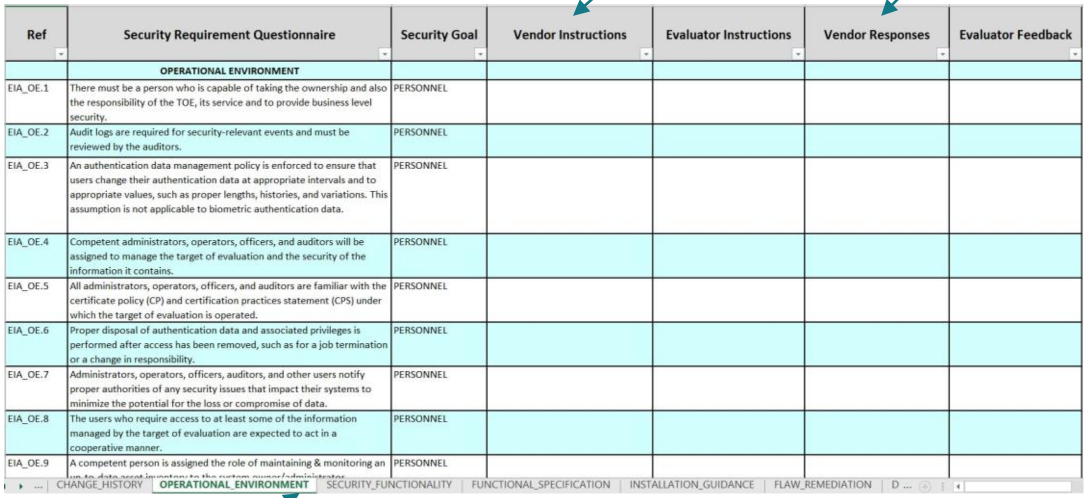
Vendor Questionnaire ?

A Vendor Questionnaire (VQ) is a technical document including questions and instructions addressed to the vendor who's implementing the ToE. Responses to these questions are considered as evidence materials and must be provided by the vendor to support the evaluation process.

Each requirement has an associated instruction which the vendor must follow while providing responses. (explains how to respond)

You will provide your responses inside this column corresponding to each requirement.

VQ looks like this:



Ref	Security Requirement Questionnaire	Security Goal	Vendor Instructions	Evaluator Instructions	Vendor Responses	Evaluator Feedback
	OPERATIONAL ENVIRONMENT					
EIA_OE.1	There must be a person who is capable of taking the ownership and also the responsibility of the TOE, its service and to provide business level security.	PERSONNEL				
EIA_OE.2	Audit logs are required for security-relevant events and must be reviewed by the auditors.	PERSONNEL				
EIA_OE.3	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values, such as proper lengths, histories, and variations. This assumption is not applicable to biometric authentication data.	PERSONNEL				
EIA_OE.4	Competent administrators, operators, officers, and auditors will be assigned to manage the target of evaluation and the security of the information it contains.	PERSONNEL				
EIA_OE.5	All administrators, operators, officers, and auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the target of evaluation is operated.	PERSONNEL				
EIA_OE.6	Proper disposal of authentication data and associated privileges is performed after access has been removed, such as for a job termination or a change in responsibility.	PERSONNEL				
EIA_OE.7	Administrators, operators, officers, auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.	PERSONNEL				
EIA_OE.8	The users who require access to at least some of the information managed by the target of evaluation are expected to act in a cooperative manner.	PERSONNEL				
EIA_OE.9	A competent person is assigned the role of maintaining & monitoring an up-to-date asset inventory to the system owner/administrator	PERSONNEL				

You will find the list of requirements here

Different tabs for each aspect of evaluation. You have to select corresponding tab for providing the responses

The Security Profile contains pointers to all ToE relevant requirements (from the exhaustive list contained in the reference VQ) that must be considered by the Vendor.

What Else ?

IOT SECURITY CERTIFICATION SCHEME COMPARISION

CRITERIA	SESIP L1+	E-IOT-SCS	ARM PSA L2
MARKET	ENTREPRISE, INDUSTRIAL	CONSUMER, ENTREPRISE, INDUSTRIAL	ENTREPRISE, INDUSTRIAL
USERS	IoT Chip Vendor, IoT ROE/RoT Dev, IoT OS/FW Dev	IoT ROE/RoT Dev, IoT OS/FW Core Dev, IoT Application Dev, IoT Product Integrator, Vendor IoT Service Provider	IoT Chip Vendor, IoT RoT Dev
TARGET OF EVALUATION	Chip Level, RoT Level, OS Level	Chip Level, RoT Level, OS Level, Application Level	Chip Level, RoT Level,
OPERATIONAL ENVIRONMENT CONSIDERATION	No	Yes	No
GOVERNANCE	Private	Public	Private
CERTIFICATION VALIDITY	2 years	No limitation (with change management process)	No limitation?

What Else ?

IOT SECURITY CERTIFICATION SCHEME COMPARISION

CRITERIA	SESIP L1+	E-IOT-SCS	ARM PSA L2
VULNERABILITY MNGT PROCESS	Partially	Yes	Partially
CERTIFICATE MAINTENANCE	Yes	Yes	Yes
COMPARABLE CERTIFIED PRODUCTS	Partially	Yes	Partially
RISK MANAGEMENT PROCESS	Partially?	Yes	No
RISK-BASED EVALUATION METHODOLOGY	No	Yes	No
METADATA CERTIFICATION SERVICE	No	Yes	No
ASSESSMENT STYLE	3rd Party	3rd Party	3rd Party
PENTESTING STYLE	Time-Limited	Risk-Base + Time-Limited (per Profile)	Time-limited
CERTIFICATION LEVELS	Pre-defined Substantial Level (one size fits all)	Risk-based Substantial Level (per security profile)	Pre-defined Substantial Level (one size fits all)

What Else ?

IOT SECURITY CERTIFICATION SCHEME COMPARISION

CRITERIA	SESIP L1+	E-IOT-SCS	ARM PSA L2
SECURITY/PROTECTION PROFILE	Yes	Yes	Yes
SECURITY/PROTECTION PROFILE CREATION METHODOLOGY	No	Yes	No
ATTACKERS PROFILE	Fixed Attackers Profile per Level	Varies Per Security Profile	Fixed Attackers Profile per Level
COMPOSITION	Yes	Yes	Yes
OTHER SCHEMES EVIDENCE RE-USE	Partially	Yes	?
EVIDENCE FORMALISM	Partially (CC + Natural Language)	Natural Language	Natural Language
EVALUATION COSTS	>20K€ ?	7K-12K€	?
CERTIFICATION COSTS	9,5K€ - 16,5K€	2-4K€	?
SECURITY/PROTECTION PROFILE	Yes	Yes	Yes