IoT Security Maturity Model

Operating System: How to apply

kaspersky

industrial internet CONSORTIUM

OpenFog

Industrial Internet Consortium

The Industrial Internet Consortium, now incorporating OpenFog, is the world's leading organization transforming business and society by accelerating the Industrial Internet of Things (IIoT).

Our mission is to deliver a trustworthy IIoT in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes.

https://iiconsortium.org/

https://iiconsortium.org/smm.htm

kaspersky

industrial internet CONSORTIUM

OpenFog

RESOURCE HUB

SEARCH MEMBERS

FOUNDING & CONTRIBUTING MEMBERS

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A
451 Research
A*STAR Research Entities (“ARES”)
Aalto University
AASA Inc.
ABB
Accenture

F
Fathom Solutions Inc.
First Line Software, Inc
FogHorn
Fraunhofer Gesellschaft
FreeWave Technologies
Fuji Electric Co., Ltd.

N
National Chiao Tung University
National Taiwan University
Nanyang Technological University
NEC Corporation
NetApp
NIST

T
Tampere University of Technology,Finland
Tata Consultancy Services
Technische Hochschule Mittelhe
Technische Universität Darmsta
Telecommunications Technology

Agenda

IoT Security Maturity Model

How it appeared

The core: Practices hierarchy

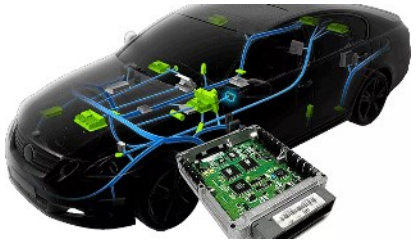
Comprehensiveness and scope

How to measure and present

How to apply to operating system

What does it mean “to be secure”…

For a production line



For an automotive ECU

For a surveillance camera

For a fitness bracelet

For a nuclear facility

kaspersky

industrial internet CONSORTIUM

OpenFog

The Mature Security Solution in IoT addresses

Business Context

Size and coverage, project timing, competing solutions…

Threats and risks

Known threats, threat sources, worst threat impact …

Expectations and priorities

Objectives, indicators, extent of improvement

Available and already implemented practices

What has been done

Industry and System Constraints

Safety, service continuity, type of lifecycle

kaspersky

industrial internet CONSORTIUM

OpenFog

The Internet of Things (IoT) Security Maturity Model (SMM) builds on the concepts identified in the Industrial Internet Security Framework (IISF) and provides a path for IoT providers to understand where they need to be, make intelligent choices about which mechanisms to use and how to invest in the mechanisms to meet their needs.

kaspersky

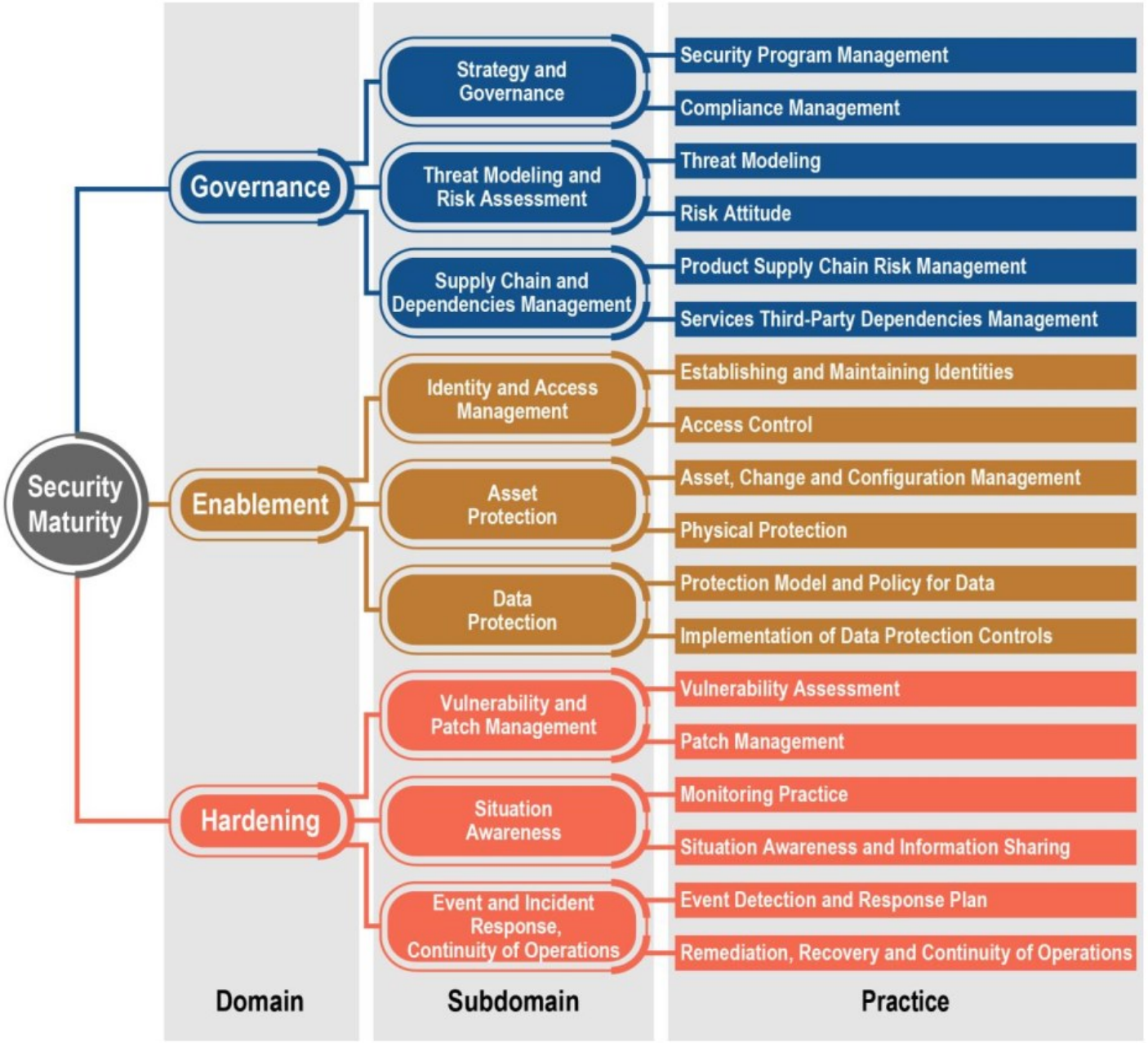
Security maturity is a measure of the understanding of the current security level, its necessity, benefits and cost of its support.

Security level, on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner.

Those using the Security Maturity Model should be able to determine and clearly communicate to management the answers to the following questions:

- Given the organizational requirements and threat landscape, what is my solution's target maturity state?
- What is my solution's current maturity state?
- What are the mechanisms and processes that will take my solution's maturity from its current state to its target state?

The Core:
Hierarchy of Security Practices



industrial internet CONSORTIUM

OpenFog

The Hierarchy: Domains, Subdomains, Practices

Domains are pivotal to determining the priorities of security maturity enhancement at the strategic level.

At the domains level, the stakeholder determines the **priorities** of the direction in improving security

Subdomains reflect the basic means of obtaining these priorities at the planning level.

At the sub domains level, the stakeholder identifies the typical **needs** for addressing security concerns.

Practices define typical activities associated with sub domains and identified at the tactical level.

At the practices level, the stakeholder considers the **purpose** of specific security activities.

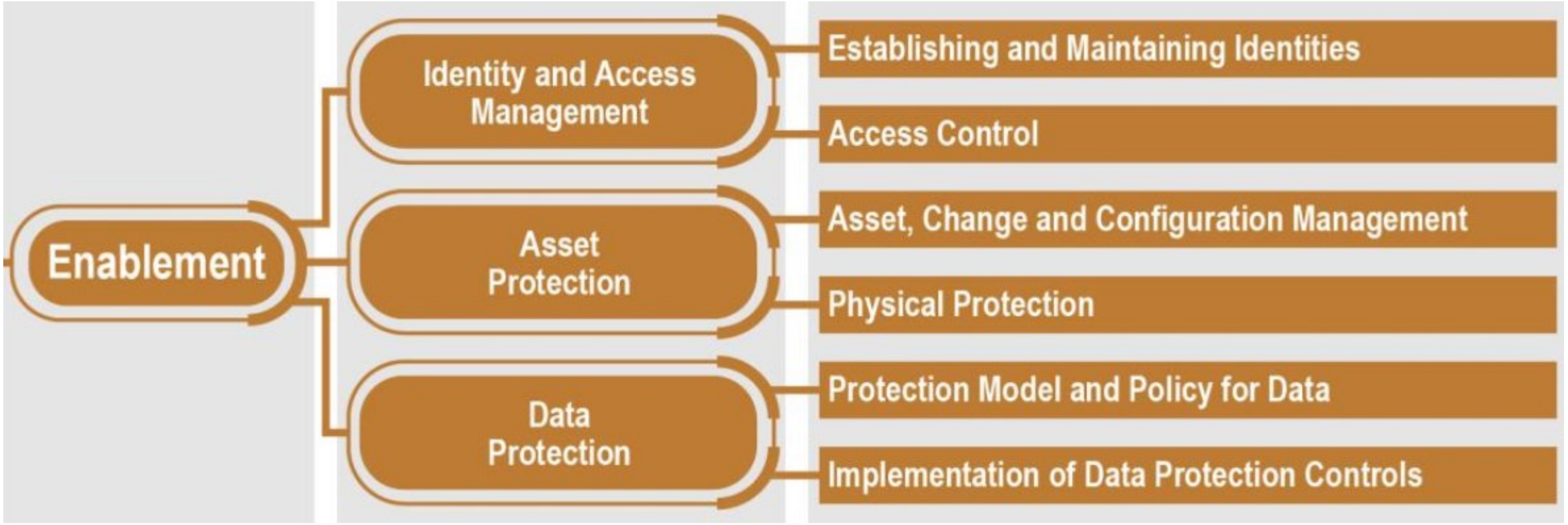
kaspersky

industrial internet CONSORTIUM

OpenFog

Governance Domain

Enablement Domain



Hardening Domain

kaspersky

industrial internet CONSORTIUM

OpenFog

Security challenges for (not only) IoT

Rigid requirements

to the security levels describing the comprehensiveness of security measures

Specificity of some areas and particular systems

in regard to security may constrain the implementation of security measures or require some that are out-of-scope for the standard/regulatory requirements

“Good enough” security

As a result, it is hard to understand what is required to guarantee that the system is secure enough but not more

kaspersky

industrial internet CONSORTIUM

OpenFog

Scoring. Comprehensiveness

Level 0, None:

There is no common understanding of how the security practice is applied and no related requirements are implemented

Level 1, Minimum:

The minimum requirements of the security practice are implemented. There are no assurance activities for the practice implementation

Level 2, Ad hoc:

The requirements for the practice cover main use cases and well-known security incidents in similar environments. The assurance measures support ad hoc reviews of the practice implementation to ensure baseline mitigations for known risks

Level 3, Consistent:

The requirements consider best practices, standards, regulations, classifications, software and other tools. The assurance validates the implementation against security patterns, secure-by-default designs and known protection approaches and mechanisms

Level 4, Formalized:

A well-established process forms the basis for practice implementation, providing continuous support and security enhancements. The assurance on the implementation focuses on the coverage of security needs and timely addressing [illegible] threaten the system of interest.

kaspersky

industrial internet CONSORTIUM

OpenFog

Scoring. **Scope**

Level 1, General

This is the broadest scope. The security practice is implemented in the computer systems and networks without any assessment of its relevance to the specific IoT sector, equipment used, software or processes to be maintained. The security capabilities and techniques are applied as they were in the typical environment.

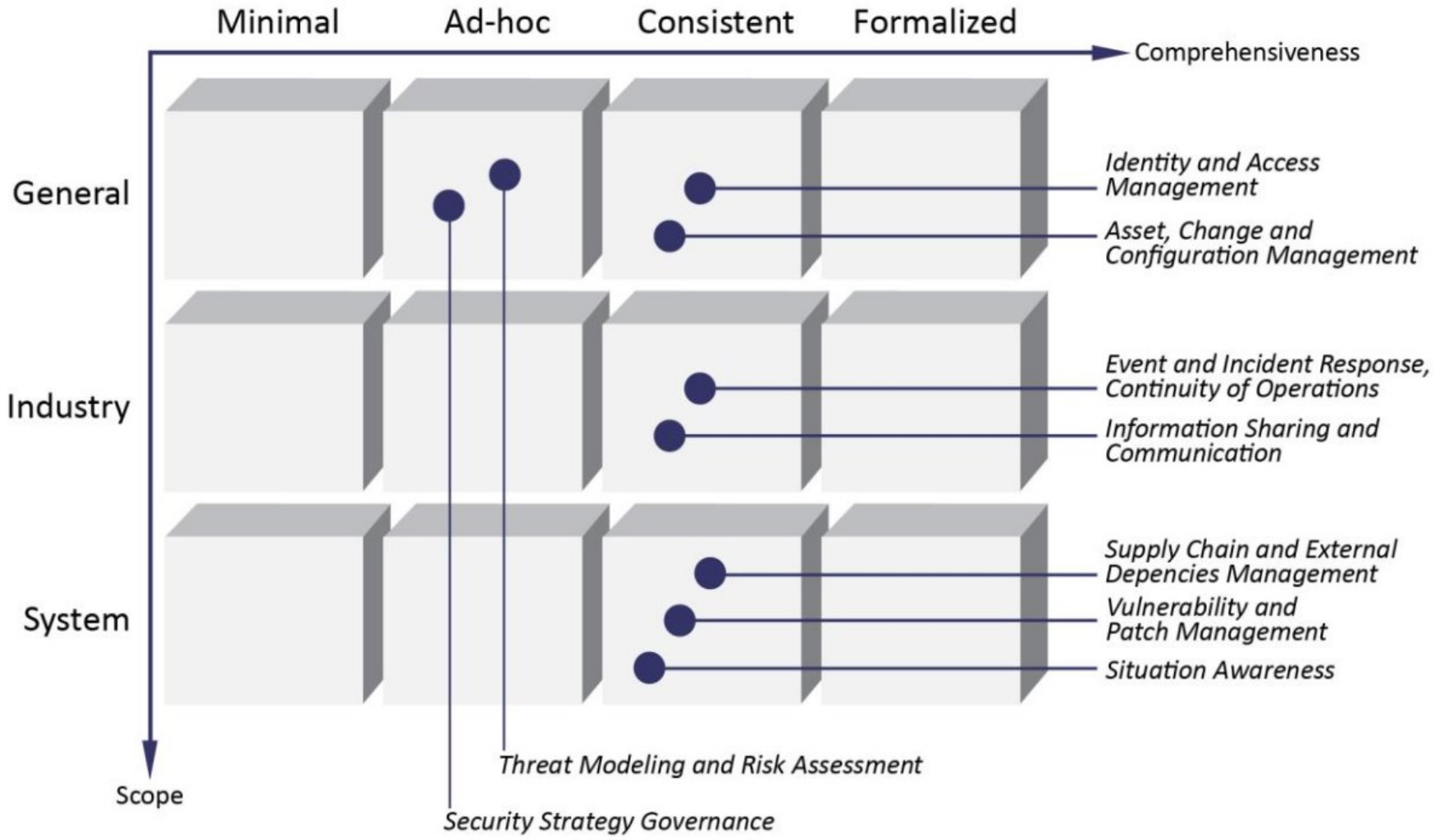
Level 2, Industry specific

The scope is narrowed from the general case to an industry-specific scenario. The security practice is implemented considering sectaor-specific issues, particularly those regarding components and processes that are prone to certain types of attacks, and known vulnerabilities and incidents that took place.

Level 3, System specific

This is the narrowest scope. The security practice implementation is aligned with the specific organizational needs and risks of the system under consideration, identified trust boundaries, components, technologies, processes and usage scenarios. Combining the general and domain specific objectives in a unique manner sets the requirements of this implementation.

Two-dimensional approach

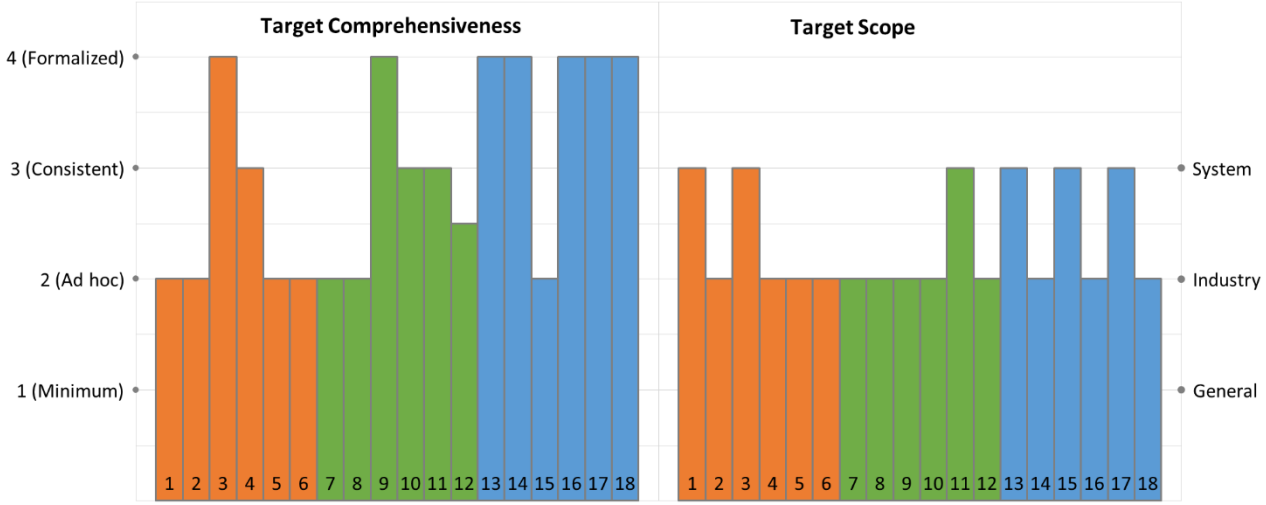


kaspersky

industrial internet CONSORTIUM

OpenFog

Example of Security Maturity Profile

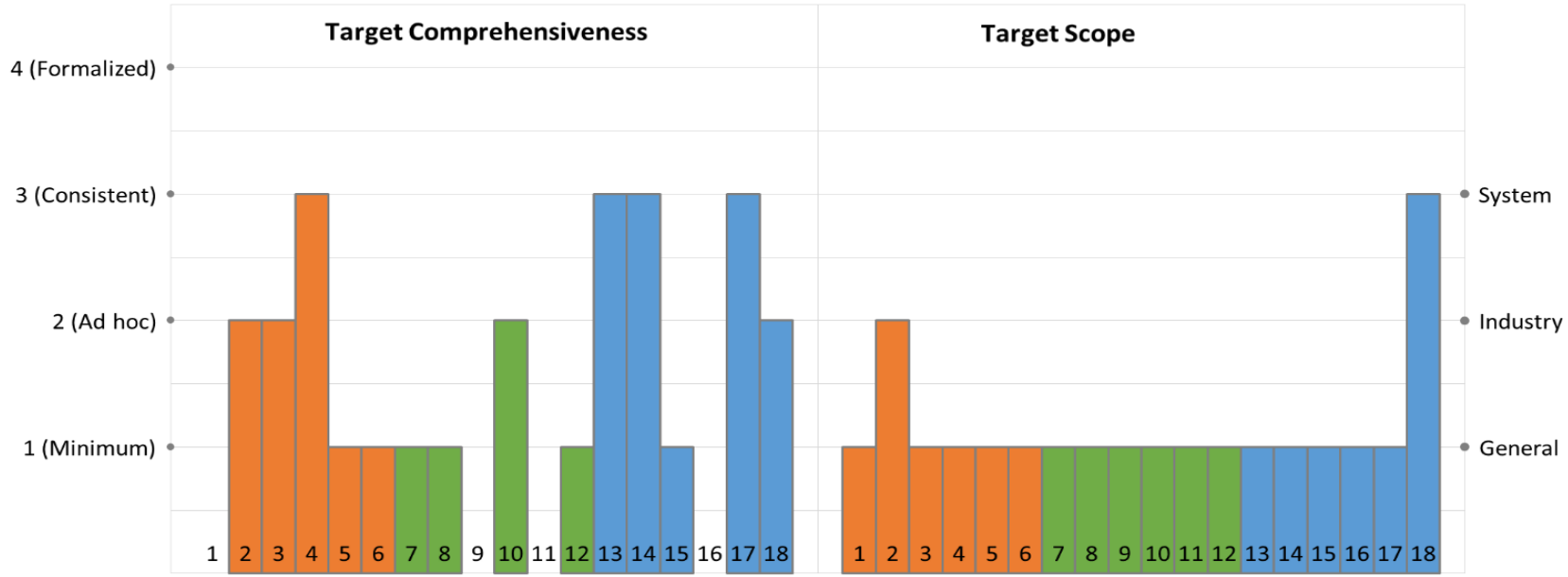


We apply the known techniques to the assessment of required practices and perform gap analysis to demonstrate how the Profile is covered in the current implementation

The quantitative result is also considered (method is under research)

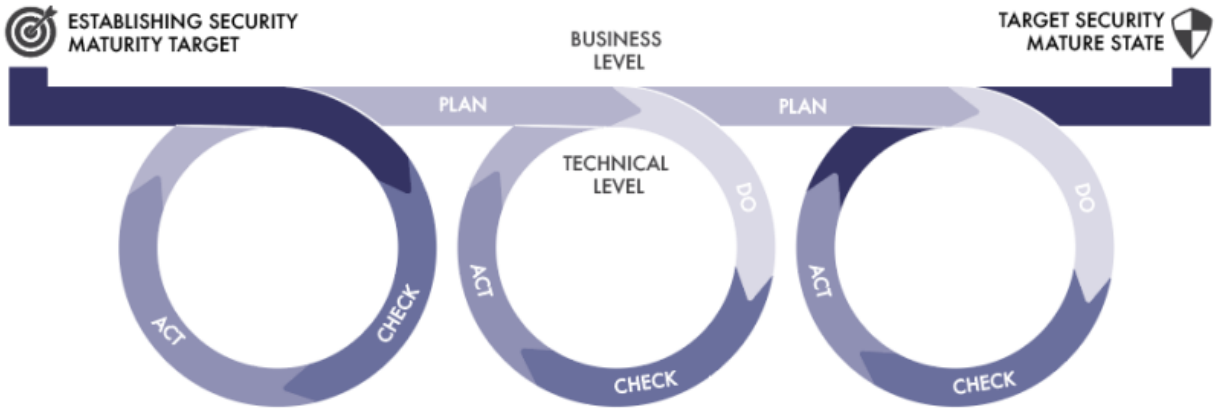
HVAC control system

Security Maturity Target: Detailed Target for Security Pratices



- 1 Security Program Management
- 2 Compliance Management
- 3 Threat Modeling
- 4 Risk Attitude
- 5 Supply Chain Risk Management
- 6 Third-Party Dependencies Management
- 7 Establishing and Maintaining Identities
- 8 Access control
- 9 Asset, Change and Configuration Management
- 10 Physical Protection
- 11 Security Model and Policy for Data
- 12 Implementation of Data Protection Controls
- 13 Vulnerability Assessment
- 14 Patch Management
- 15 Audit
- 16 Information Sharing and Communication
- 17 Event Detection and Response Plan
- 18 Remediation, Recovery, and Continuity of Operation

The advantages of using IoT SMM Approach



The **Security Maturity Profile** plays a role of the security standard for the solution and helps the stakeholders to align their security concerns and appropriate measures to address these concerns

Security requirements can be tailored to the **specific needs** of particular solution and organized according to the recognized framework

Scoring and roadmap planning are covered by the method. Lifecycle-based approach helps with setting the priorities and enhancement of Security Maturity for the selected security practices.

Assessment for Security Maturity fosters the collaboration of potential users, business stakeholders and high-level technicians/security specialists

We do not have to waste the time on assuring the requirements that make no sense in regard to the solution

The method does not separate security enhancement and security certification, thus making the process much more effective

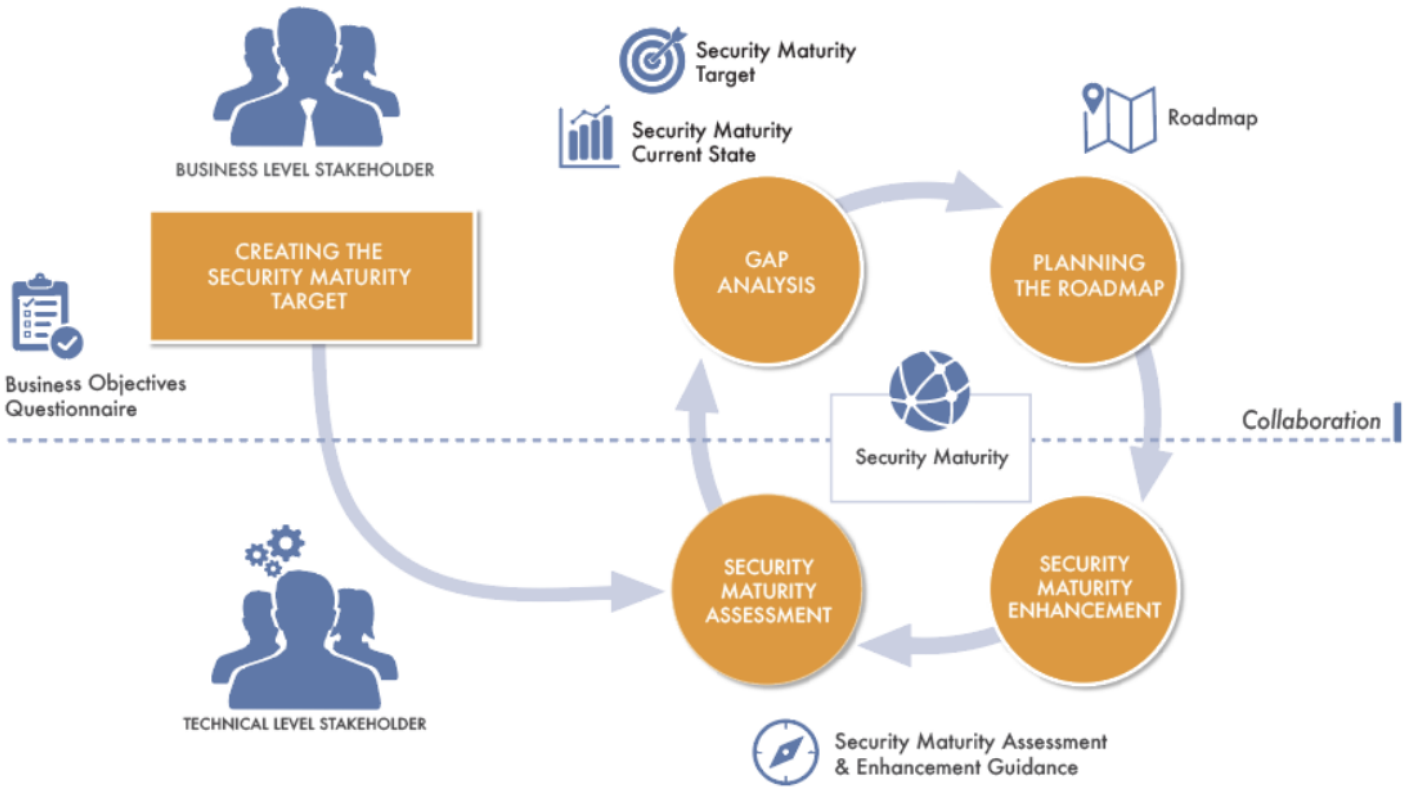
kaspersky

industrial internet CONSORTIUM

OpenFog

Security Maturity Model for Strategy and Priority setting

The process of security maturity assessment and enhancement



Where to apply Security Maturity Assessment

Establishing scope of work

going from business to technical proposal

Certification of devices/software

not for the absence of vulnerabilities but for mature process to fix the discovered ones

As a separate service

for planning the roadmap for security enhancement

kaspersky

industrial internet CONSORTIUM

OpenFog

kaspersky

OS Security Maturity

kaspersky

industrial internet CONSORTIUM

OpenFog

Applying IoT SMM to operating system

Relying on basic OS security features

Minimum or ad hoc comprehensiveness level

+ Secure SDLC and supporting best practices

Consistent comprehensiveness level

+ OS architectural design facilitating security assurance

Formalized comprehensiveness level

kaspersky

industrial internet CONSORTIUM

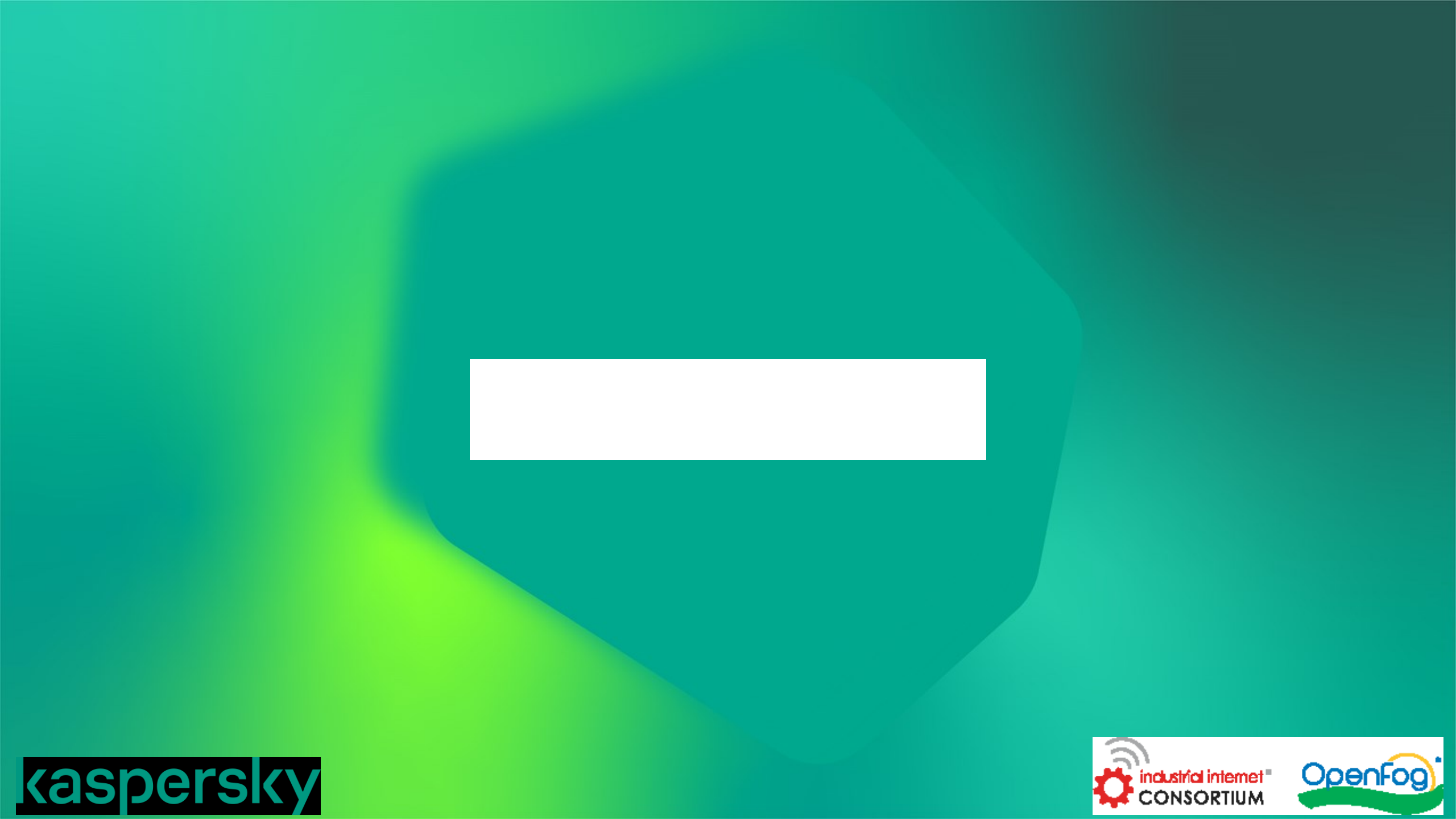
OpenFog

Thank you!

kaspersky

industrial internet CONSORTIUM

OpenFog


kaspersky
industrial internet CONSORTIUM
OpenFog