Assessing information security maturity in an industrial company

Ekaterina Rudina

Critical Infrastructure Defense

KL ICS-CERT

industrial internet CONSORTIUM

KASPERSKY lab

Contents

Security Facets

Which, when, where, and **to which extent?**

Security policy
Threat modeling
Connected Cities
Privacy & data protection challenge
Cars become smarter
Consumerization & mobility
Internet of Things
Increasing online commerce
Critical infrastructure at risk
Big data
Fragmentation of the Internet
Cloud & virtualization
Asset management
Attacks on Smart Cities
Malware for ATMs
IoT botnets
Commercialization of APTs
Merger of cybercrime and APTs
Supply chain attacks
Ransomware in Targeted Attacks
Increasing cost of APTs
Targeted attacks
Hacktivism
Vulnerabilities connected cars
Access control
Internet of Things
Mobile threats
Online banking attacks
Massive data leaks
Cyber-espionage
Ransomware
Incident response
Patch management
"Wipers" & cyber-sabotage
Targeting hotel networks
Financial phishing attacks
Attacks on POS terminals
Threats to Smart Cities
Risk attitude
Vulnerability assessment

Difference between Security Level and Security Maturity Level

SECURITY LEVEL

is a degree for the implementation of security practices, mechanisms, and procedures

Consistency in the implementation

Assurance on the implementation

Confidence in assurance cases

SECURITY MATURITY LEVEL

is a degree of understanding of the current Security Level, its benefits, and cost of its support

Example. Approaches to Threat Modeling facet

++ valid across various IIoT domains.
-- sometimes they cannot be properly applied to the particular domain
-- in some other cases they do not cover the specific risks

Horizontal models:
general (such as STRIDE or CAPEC classification)
technology specific (OWASP Top 10)

Combining the methods and models is the best option

Vertical models:
valid within one domain (LINDDUN, PASTA, template by NCC)

++ take into account the specific risks for the domains
-- may cover the narrow set of technologies
-- some “vertical” models address only certain objectives

General objective:
Stakeholders collaboration in the process of getting the mature state

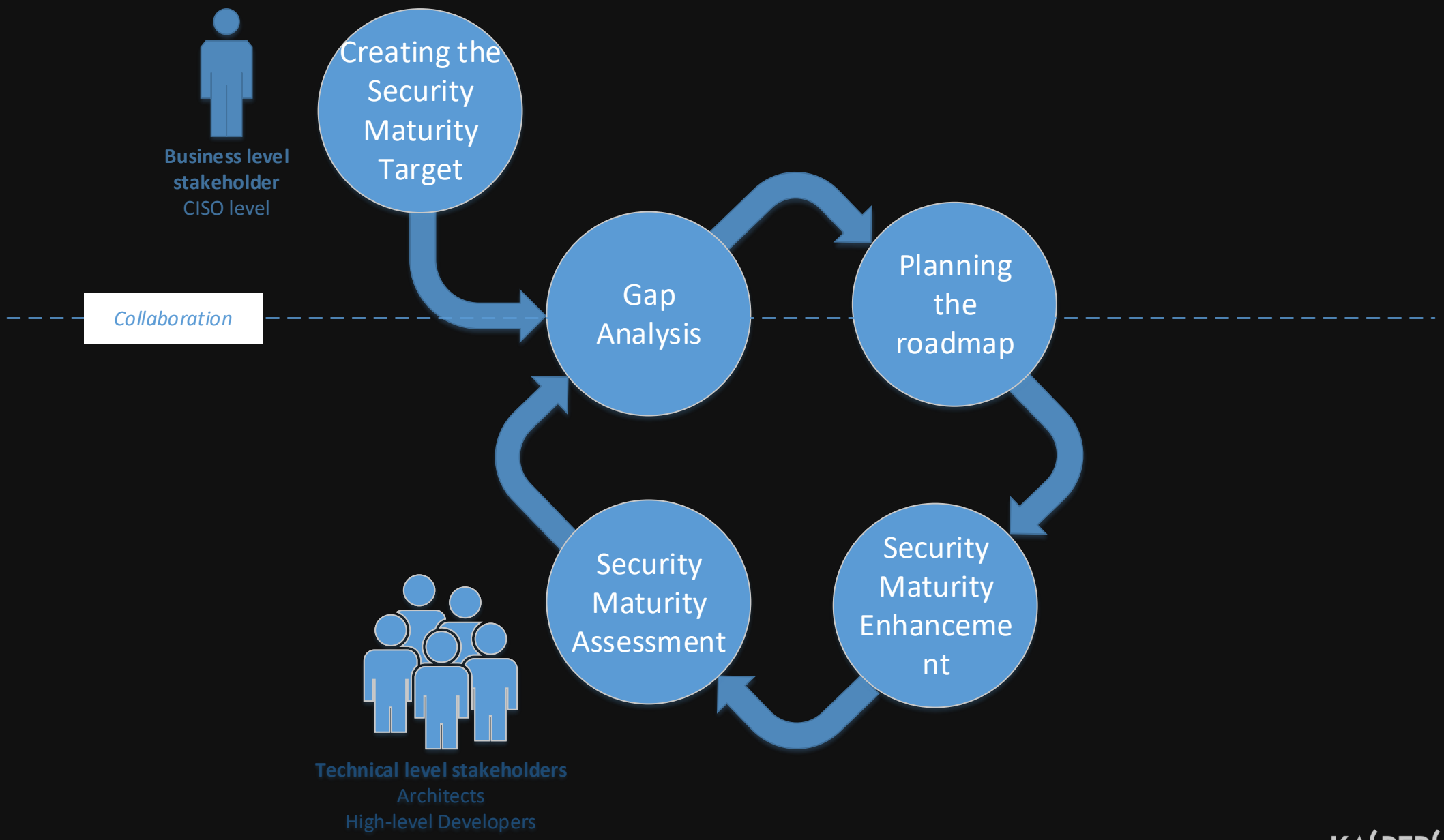
Different stakeholders consider the same aspects from the different viewpoints

Business level stakeholders define the security goals*

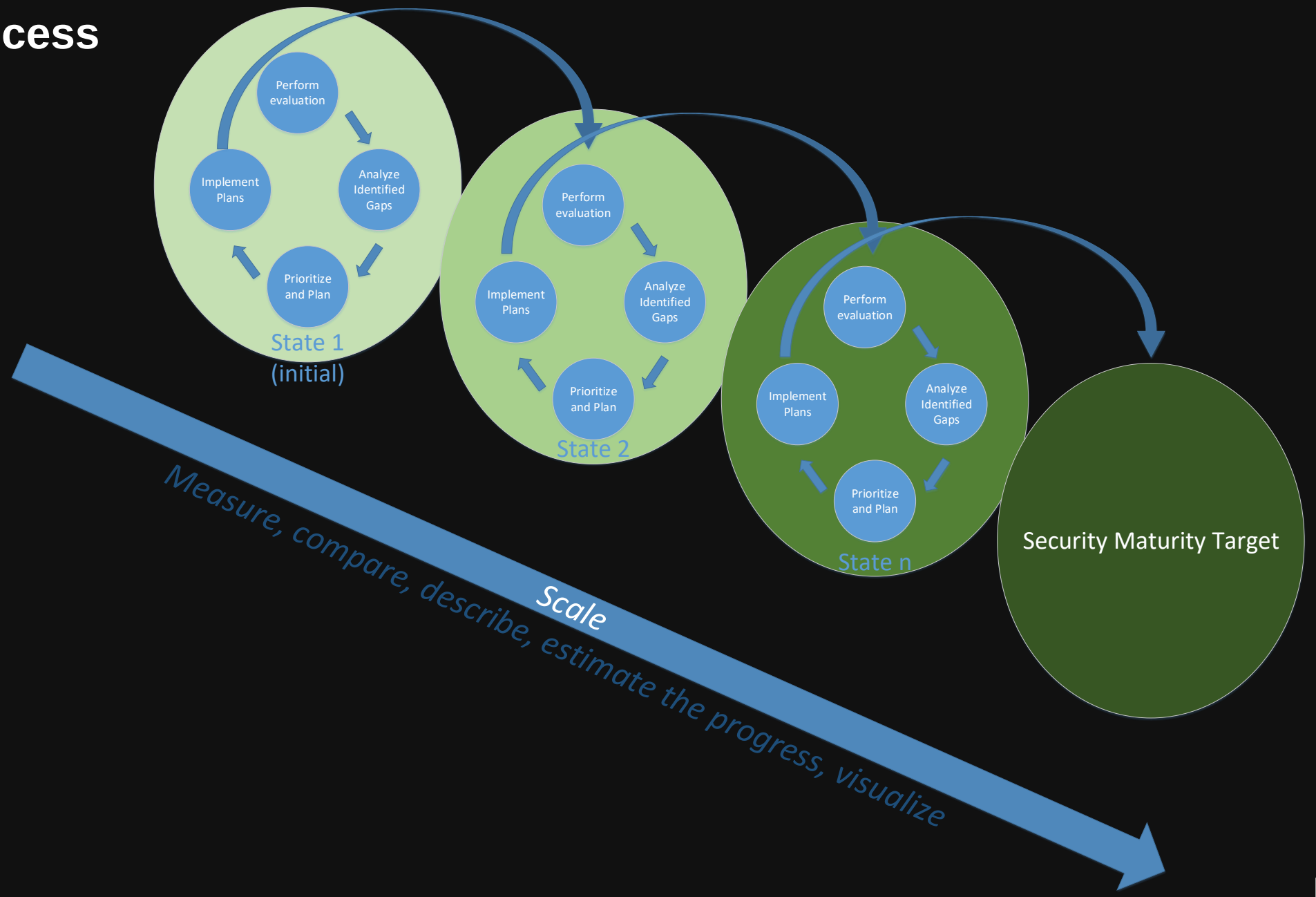
Technical level implements the mechanisms and procedures**

* Business level here means security aware stakeholders (not CEO but CISO)

** Technical level – not codewriters but architects, high-level developers, etc.



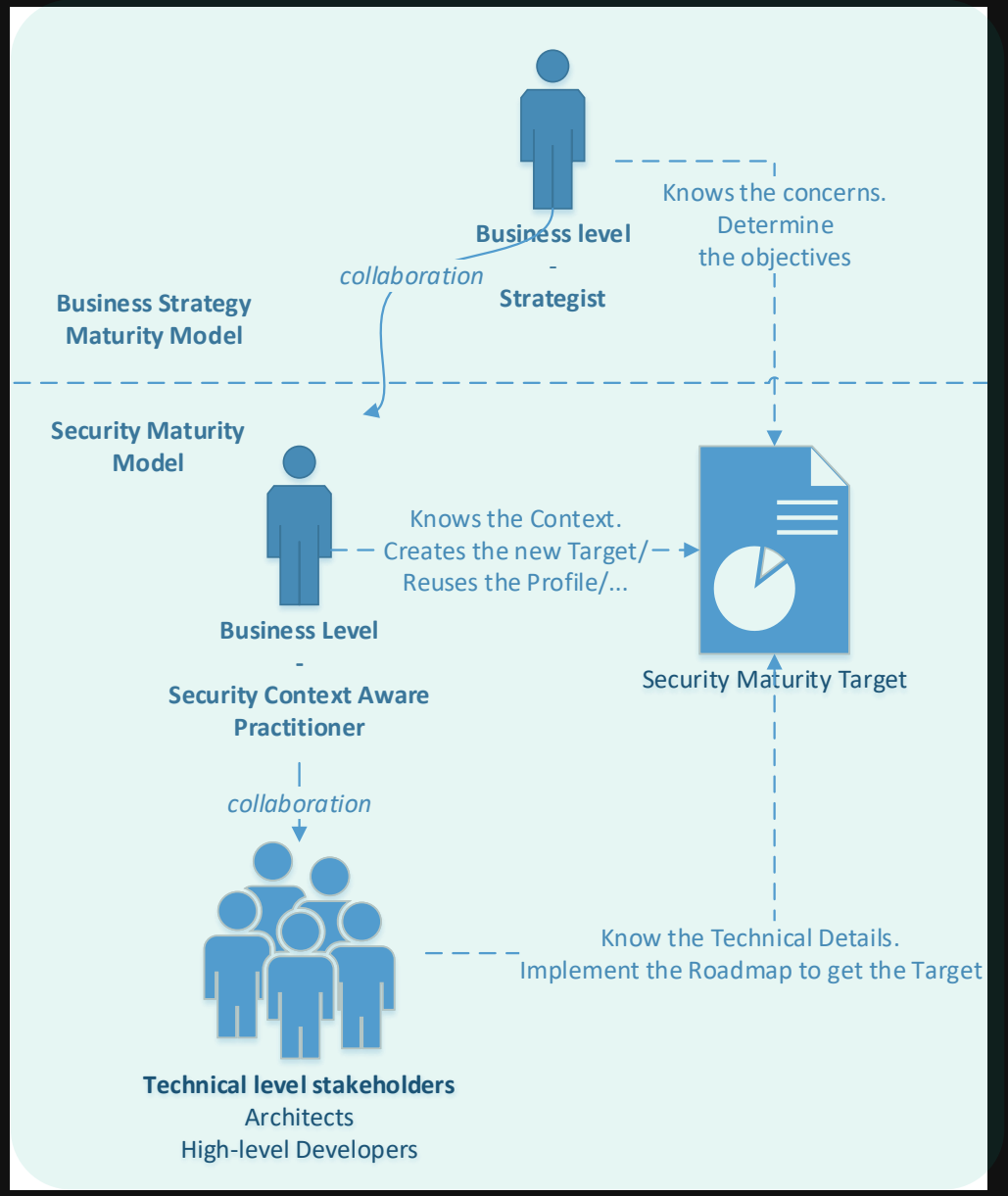
The Process

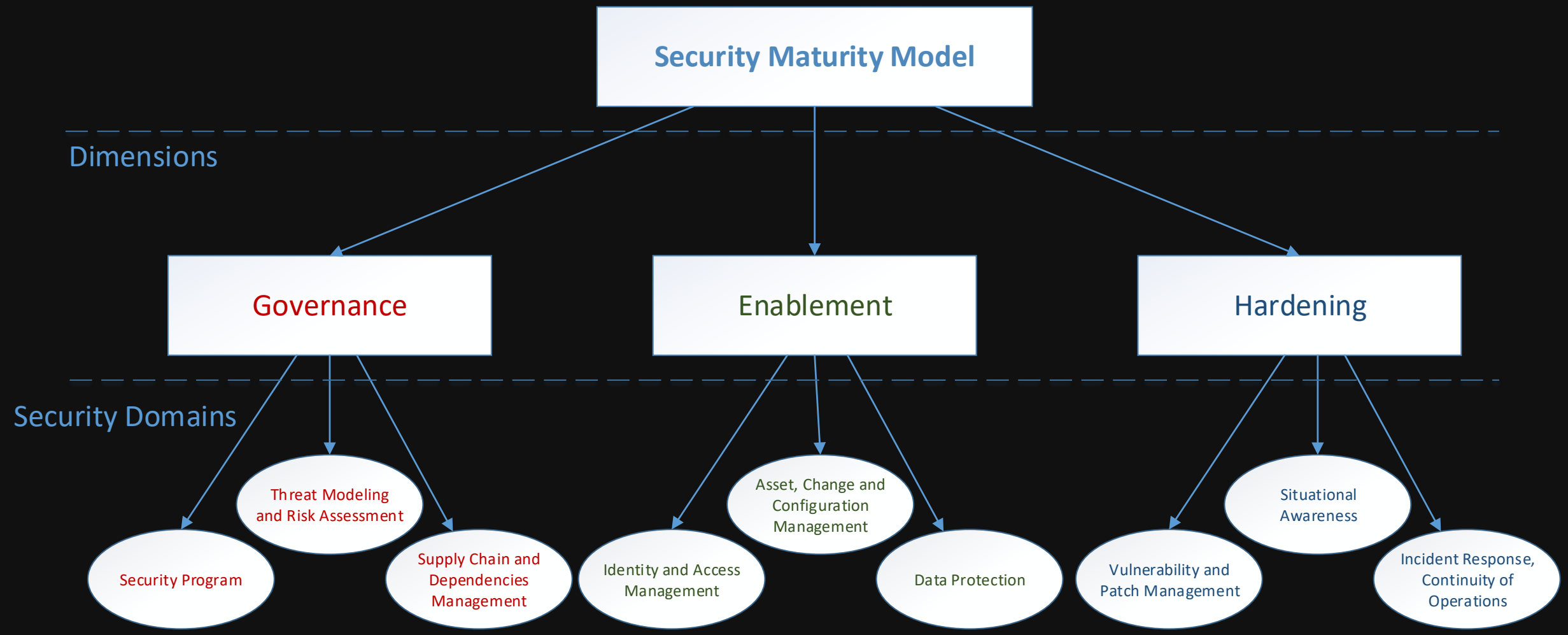


KASPERSKY lab

Security Maturity Target

SM Target defines what the 100% Security Maturity for the system is

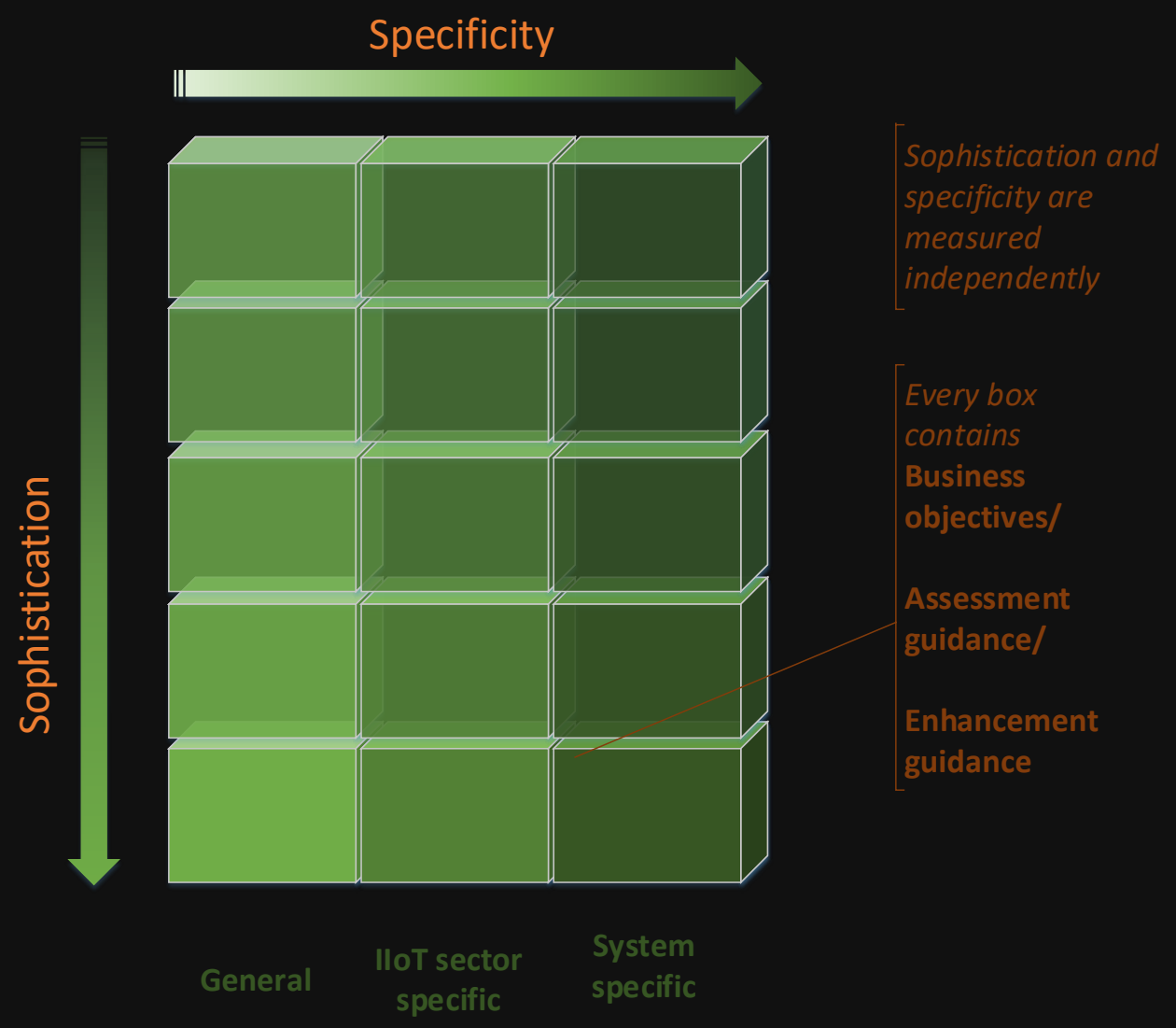




Security Practices

Security Program Management	Compliance Management	Threat Modeling	Risk Attitude	Supply chain Risk Management	Third-Party Dependencies Management	Establishing and Maintaining Identities	Access Control	Asset Management	Change and Configuration Management	Security Model and Policy for the Data	Implementation of Data Protection Controls	Vulnerability Assessment	Patch Management	Auditing	Information Sharing and Communication	Event and Incident Response	Remediation, Recovery and Continuity of Operations

Measuring scale for the Security Facet



Sophistication and specificity are measured independently

Every box contains **Business objectives/**

Assessment guidance/

Enhancement guidance

The detailed scale

The rows describe the measure of the comprehensive, consistent, and highly assured implementation of security controls

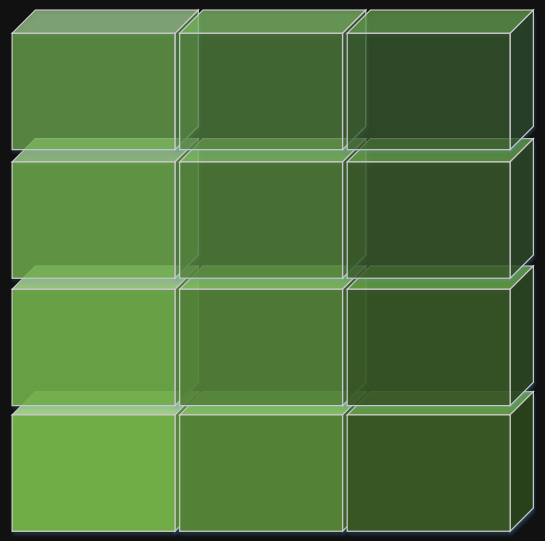
The columns relate to the customized, technically appropriate approach to the implementation of security controls

Sophistication/Specificity measured independently	General	IIoT Sector specific	System specific
No information on of how the Security Facet is applied			
The Security Facet is implemented somehow			
The Security Facet is implemented with taking into account the main use cases			
The Security Facet employs the generally accepted methods, classifications, tools, software, etc.			
The Security Facet is implemented consistently, using the process-oriented approach			

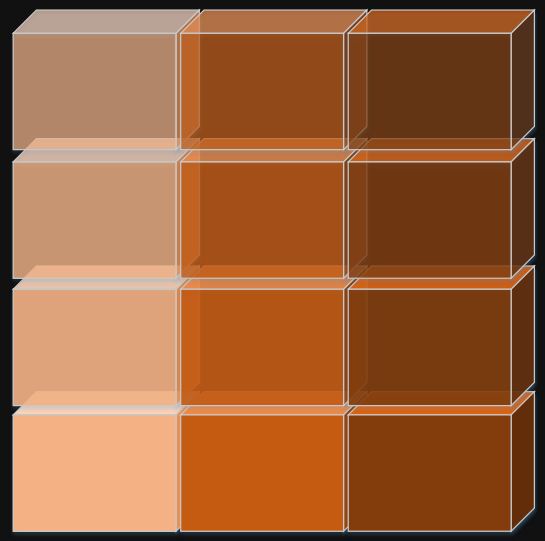
Maturity

Security Facets and their maturity

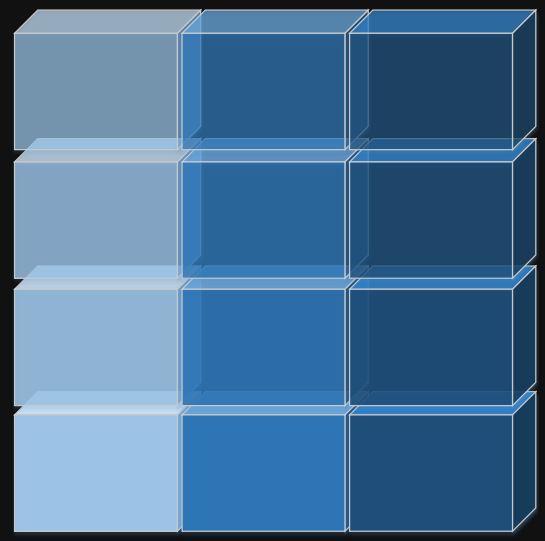
Threat Modeling



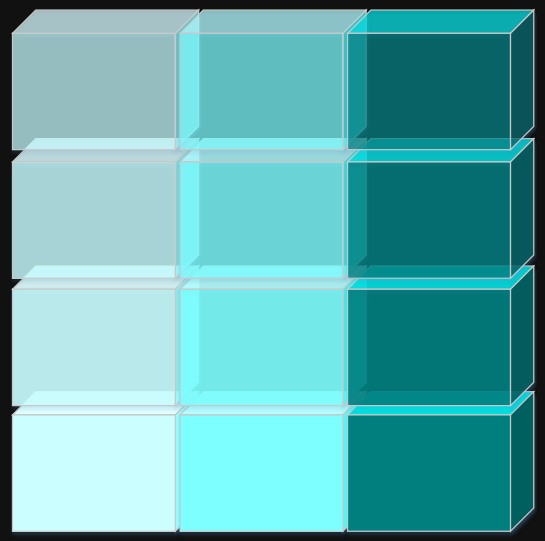
Vulnerability & Patch management



Compliance/conformance assessment



Supply chain management



Secure communications

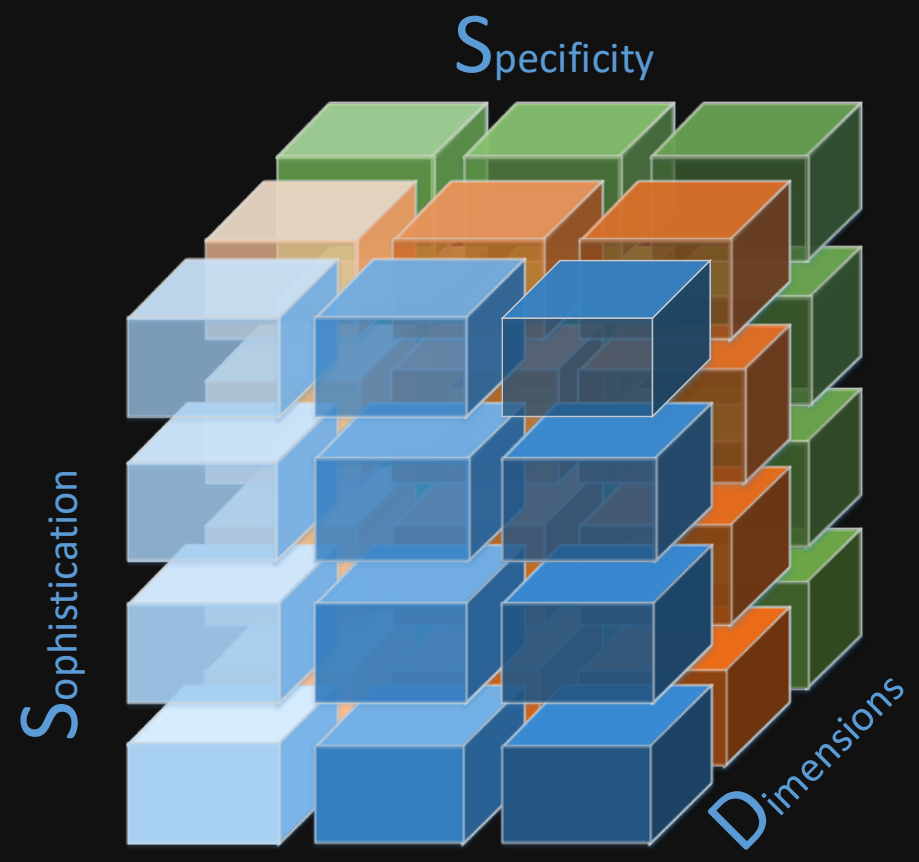
Protection of endpoints

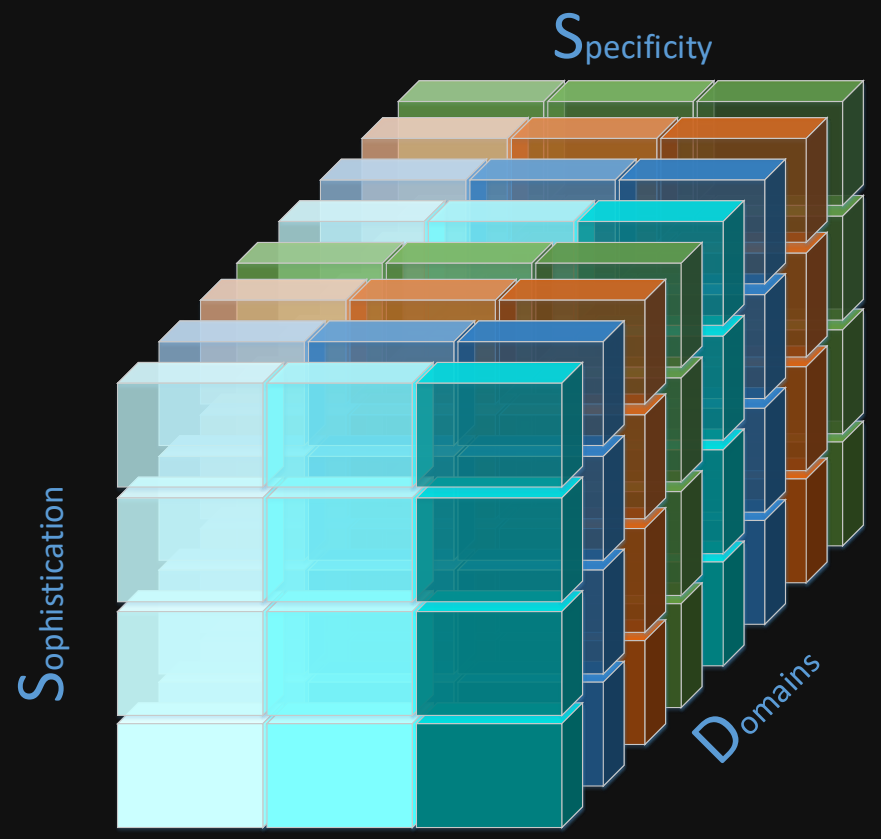
Incident handling

Recovery and remediation

...

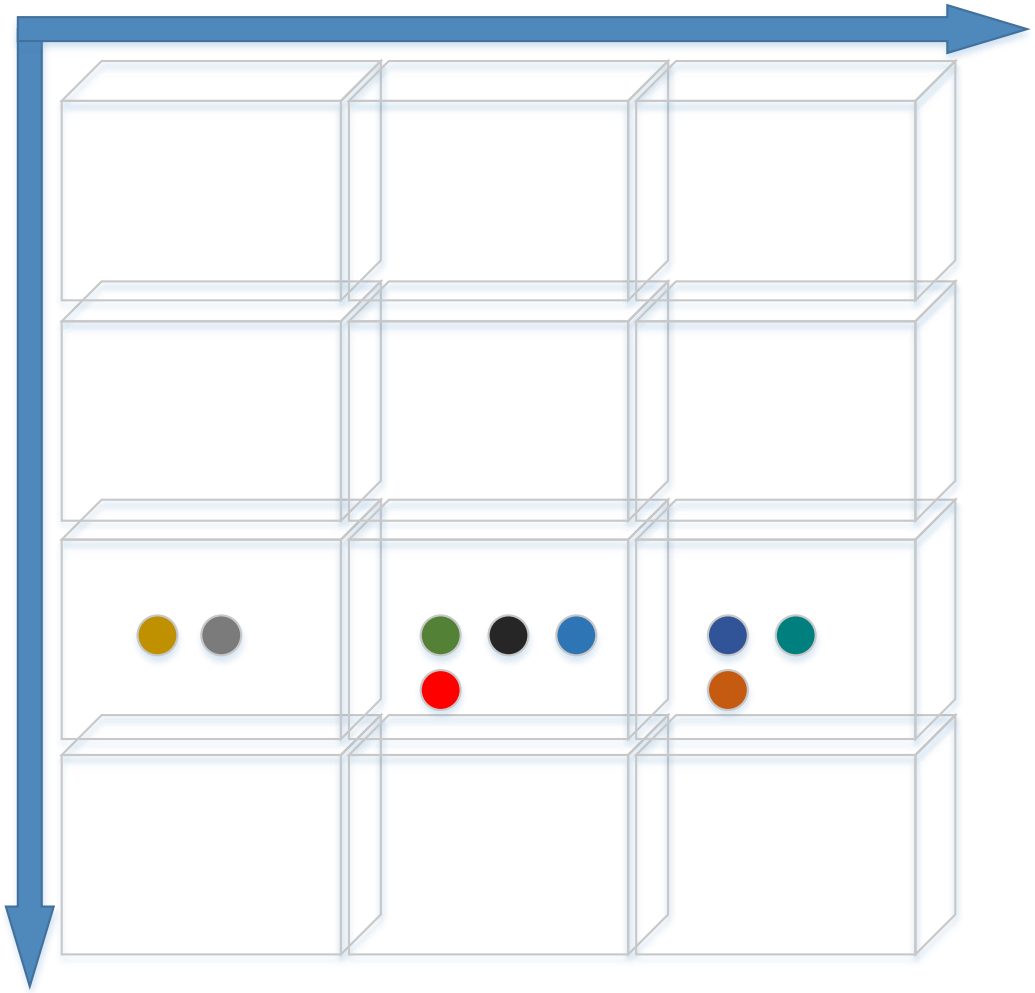
The Security Maturity Model





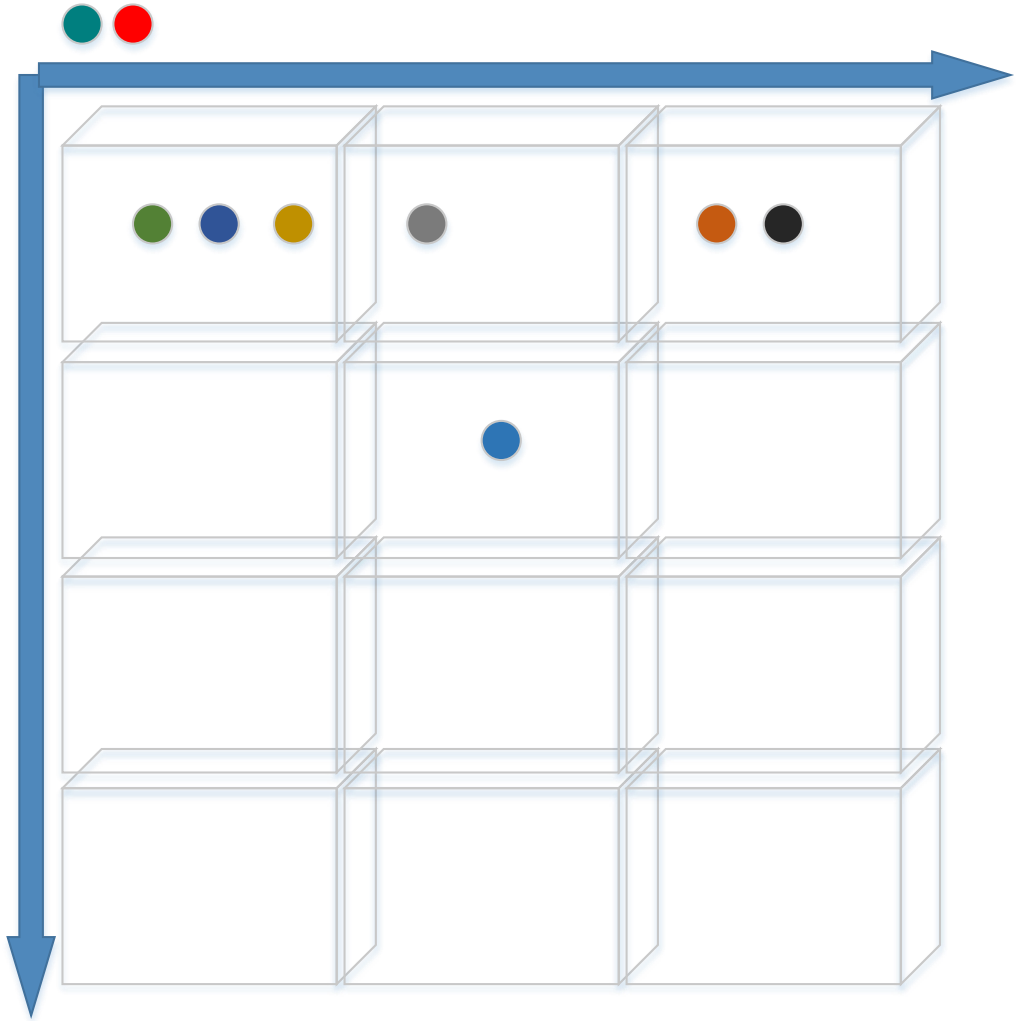
EXAMPLE. SM Target

- Security strategy and Governance
- Threat Modeling and Risk Assessment
- Supply Chain and External Dependencies Management
- Identity and Access Management
- Asset, Change and Configuration Management
- Vulnerability and Patch Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations
- Information Sharing and Communication



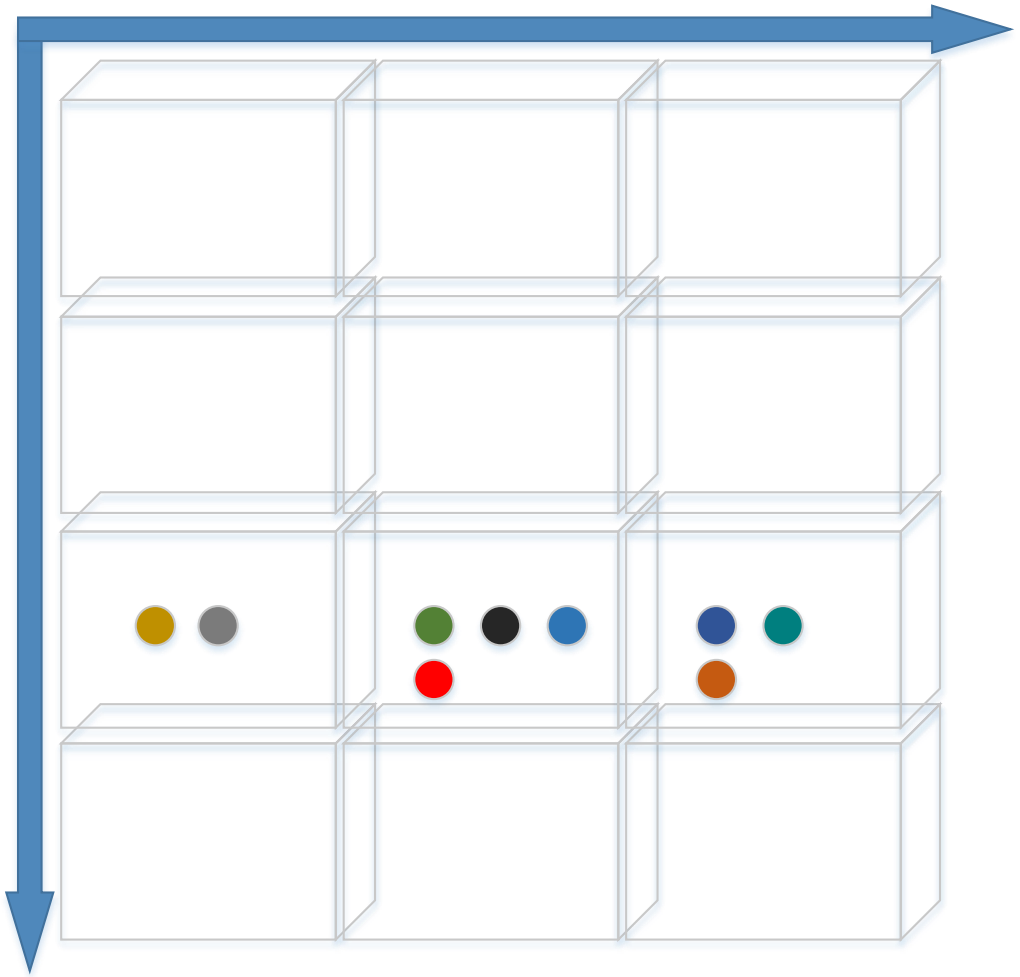
EXAMPLE. SM State

- Security strategy and Governance
- Threat Modeling and Risk Assessment
- Supply Chain and External Dependencies Management
- Identity and Access Management
- Asset, Change and Configuration Management
- Vulnerability and Patch Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations
- Information Sharing and Communication



EXAMPLE. How to get the Target?

- Security strategy and Governance
- Threat Modeling and Risk Assessment
- Supply Chain and External Dependencies Management
- Identity and Access Management
- Asset, Change and Configuration Management
- Vulnerability and Patch Management
- Situational Awareness
- Event and Incident Response, Continuity of Operations
- Information Sharing and Communication

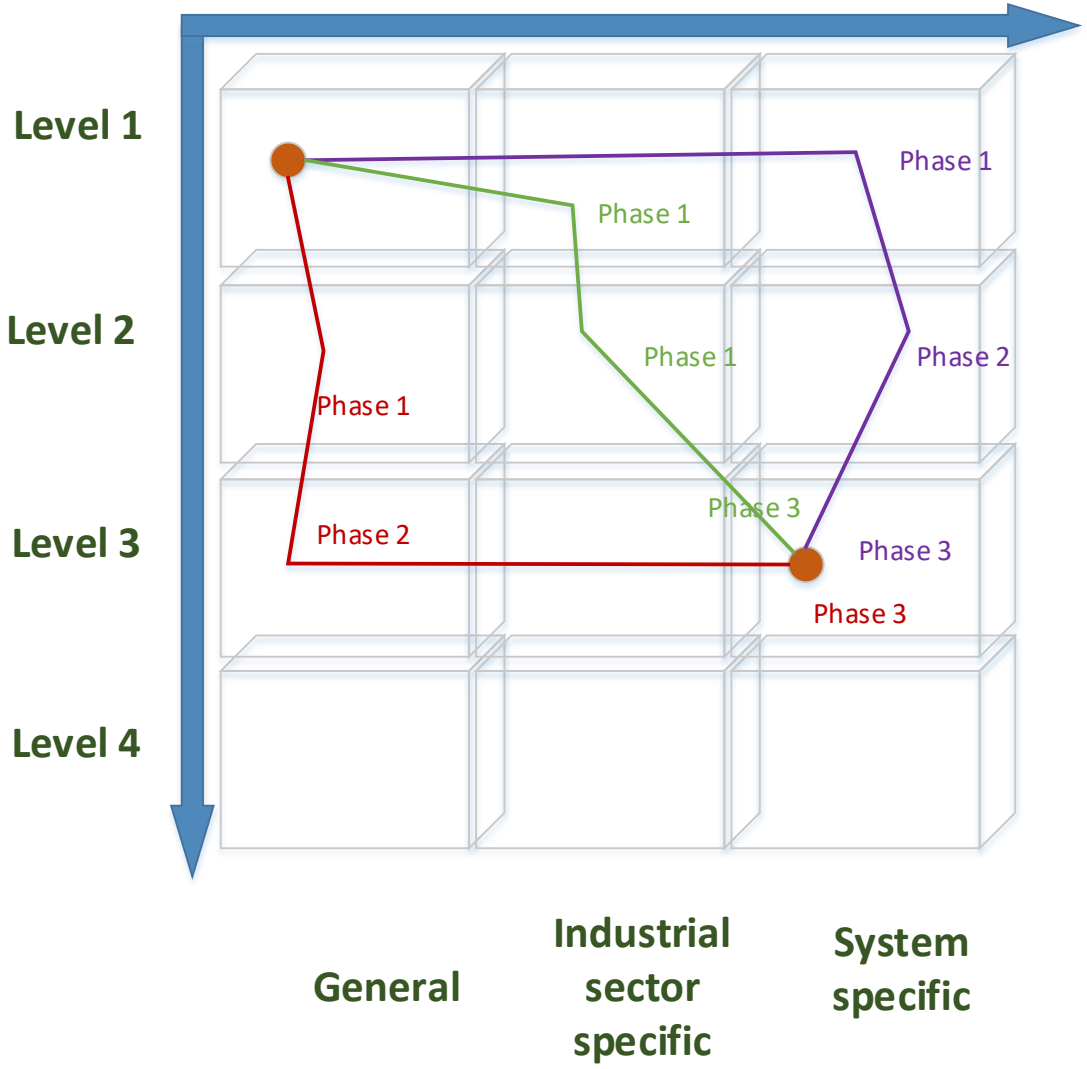


The Roadmap

- Asset, Change and Configuration Management

- *SMM allows choosing the direction and the strategy:*

- *use known security practices (increase maturity)*
- *tailor the security processes to the system (increase specificity), or*
- *step-by-step increase both parameters*



Conclusions, current and further work

Two documents describing the SMM and its use

1. SMM description and intended use
2. SMM details and how to apply

The tool (currently Excel-based) to support the process of setting the SM Target

1. Questionnaire for the business level stakeholders
2. Visualization of SM Target and SM State

Work continues in the Security Applicability WG of Industrial Internet Consortium

A lot of IIC members are already interested in the results

Contributions, comments, reviews are welcomed!

industrial internet CONSORTIUM

KASPERSKY lab

LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab