Sicherheit im IoT: IoT-Sicherheitskennzeichen, Sicherheitslücken, Einfallstore – Wie können neue Standards helfen?

Moderation und Begrüßung

Cornelia Schildt

Senior Projektmanagerin IT-Sicherheit

cornelia.schildt@eco.de

eco - Verband
der Internetwirtschaft e.V.

Tatjana Hein

Projektmanagerin IoT & Mobility

tatjana.hein@eco.de

eco - Verband
der Internetwirtschaft e.V

Wie Sie an diesem Webinar teilnehmen können

- Wir zeichnen das Webinar auf
- Sie sind während des ganzen Webinars stumm geschaltet
- Stellen Sie Ihre Fragen **schriftlich über den Chat** in Ihrem Control Panel
- Die Fragen werden jeweils im Anschluss der Präsentationen besprochen
- Sie können **Ihre Frage auch gerne mündlich** stellen
  - ➢ Nutzen Sie bitte die **„Hand heben" Funktion** in Ihrem Control Panel
  - ➢ Wir werden Ihre Stummschaltung dann aufheben
  - ➢ Bitte nennen Sie dann kurz Ihren Namen und Ihre Firma und stellen Sie Ihre Frage
- Falls Sie lieber anonym bleiben möchten, können Sie natürlich weiterhin Ihre Frage schriftlich im Tool stellen

Agenda

10:00 **Begrüßung und Einleitung**

Cornelia Schildt, Sr. Projektmanagerin IT-Sicherheit, eco Verband der Internetwirtschaft e. V. und Tatjana Hein Projektmanagerin IoT & Mobility, eco Verband der Internetwirtschaft e. V.

10:10 **IoT-Sicherheitslücken und Einfallstore, Auffälligkeiten und Beispiele unserer Labortests**

Eric Clausing, Laborleitung Internet of Things, AV-TEST GmbH

10:40 **IoT Security & Compliance automatisieren – Risiken & Kosten minimieren**

Jan Wendenburg, CEO, IoT Inspector GmbH

11:10 **Let's talk about security in IoT: Von Security-by-Design bis zur Prüfung und Zertifizierung**

Pablo Endres, Managing Director / Lead Security Consultant, SevenShift GmbH

11:40 **Security by Design – Der ARENDAR**

Rudolf Preuss, Geschäftsführer, ARENDAR IT-Security GmbH

12:10 **Offene Diskussion**

12:30 **Ende**

Sicherheit im IoT – Auffälligkeiten und Beispiele unserer Labortests 2021

Eric Clausing
Director IoT-Lab
AV-TEST Institute
https://www.av-test.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST

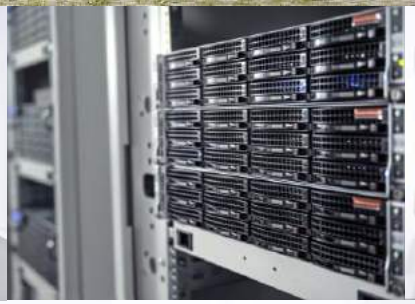
The Independent IT-Security Institute

Magdeburg Germany

- Mehr als 30 IT-Spezialisten
- Mehr als 15 Jahre Expertise im Bereich Antiviren-Forschung
- Unternehmensgründung 2004

- Eine der größten Viren-Datenbanken der Welt
- 500 Client- und Server-systeme
- 2.500 TB Testdaten
- Mehr als 5.000 Einzel- und Vergleichstests pro Jahr

- Analyse, Testing, Development, Consulting & Services für AV-Hersteller, Fachmagazine, Behörden und Unternehmen



AV-TEST

The Independent IT-Security Institute

Magdeburg Germany

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

- **150+** getestete **Systeme** aus den Bereichen **Smart Home**, **Smart Locks**, **IP-Kameras**, **Smarte Beleuchtung**, **eHealth**, **Haushaltsroboter**, **Sicherheitssysteme**…

- **Zertifizierungen** und **Kurztests** bestehend aus **vier Haupttestkategorien**:
  - Lokale Kommunikation
  - Online Kommunikation
  - Applikation
  - Datenschutz und Privatsphäre

https://www.iot-tests.org/

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

ABUS
Security Tech Germany

somfy

T

NUKI

BOSCH
Technik fürs Leben
Smart Home

tedee

LUPUS
ELECTRONICS

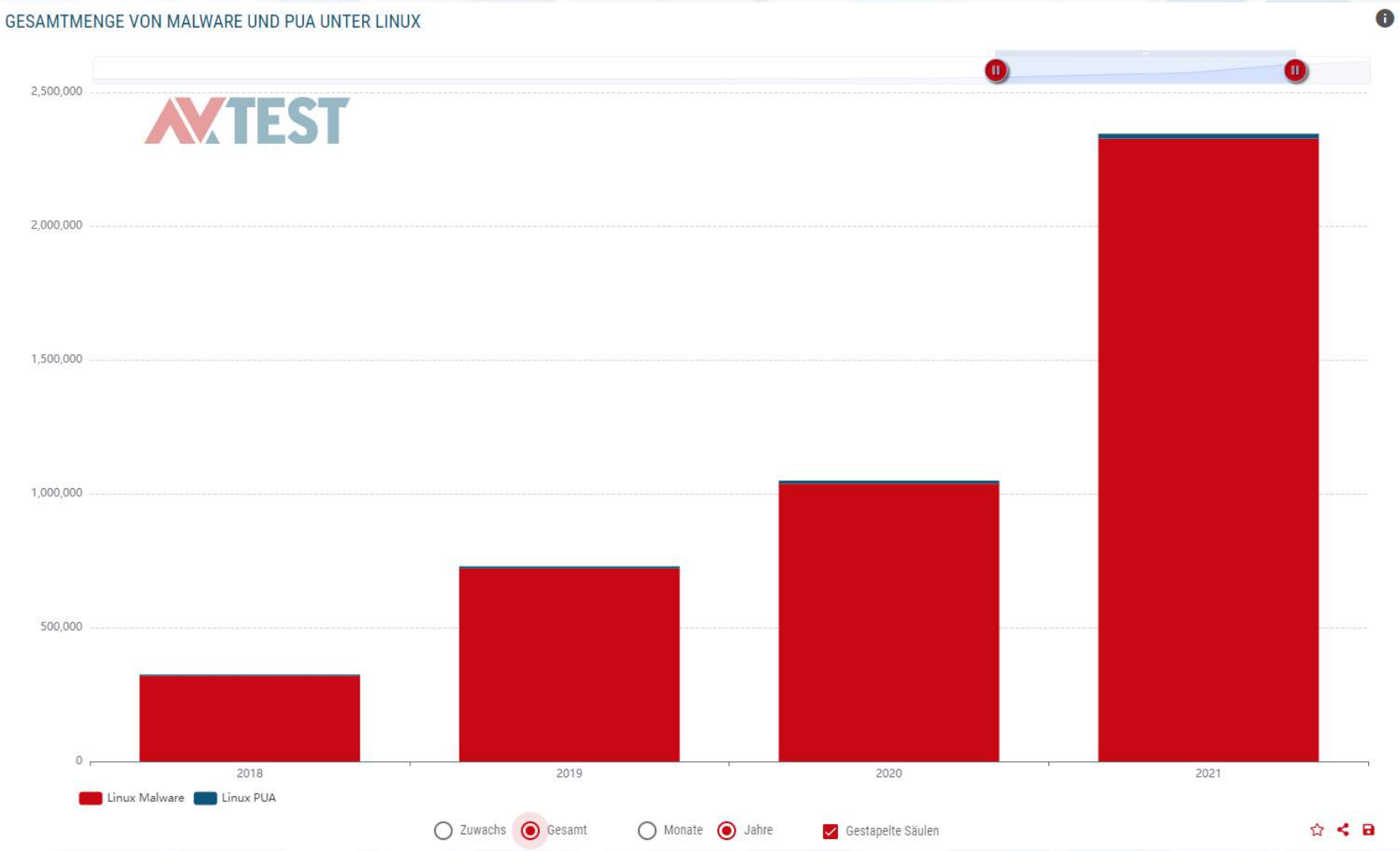
eQ-3

Prowise

AV-TEST

The Independent IT-Security Institute

Magdeburg Germany

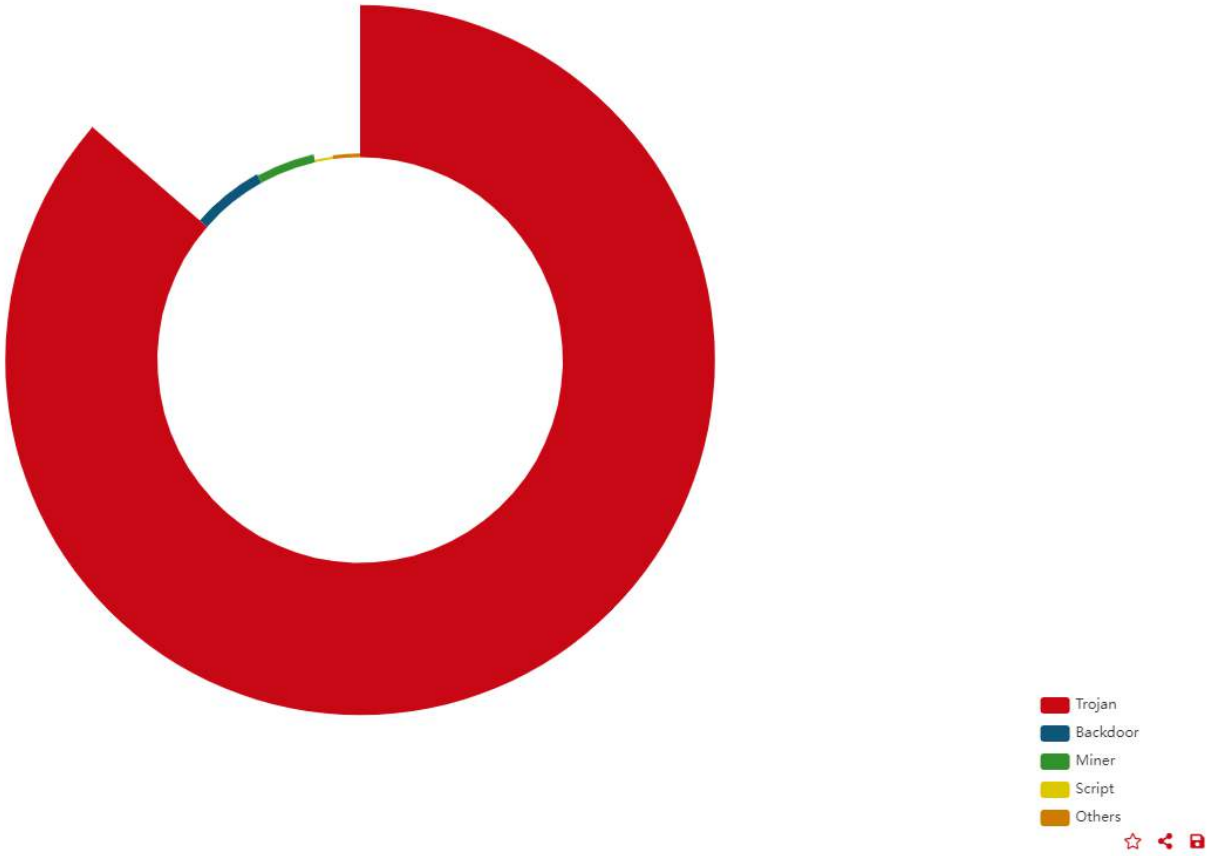


av-atlas

www.av-atlas.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

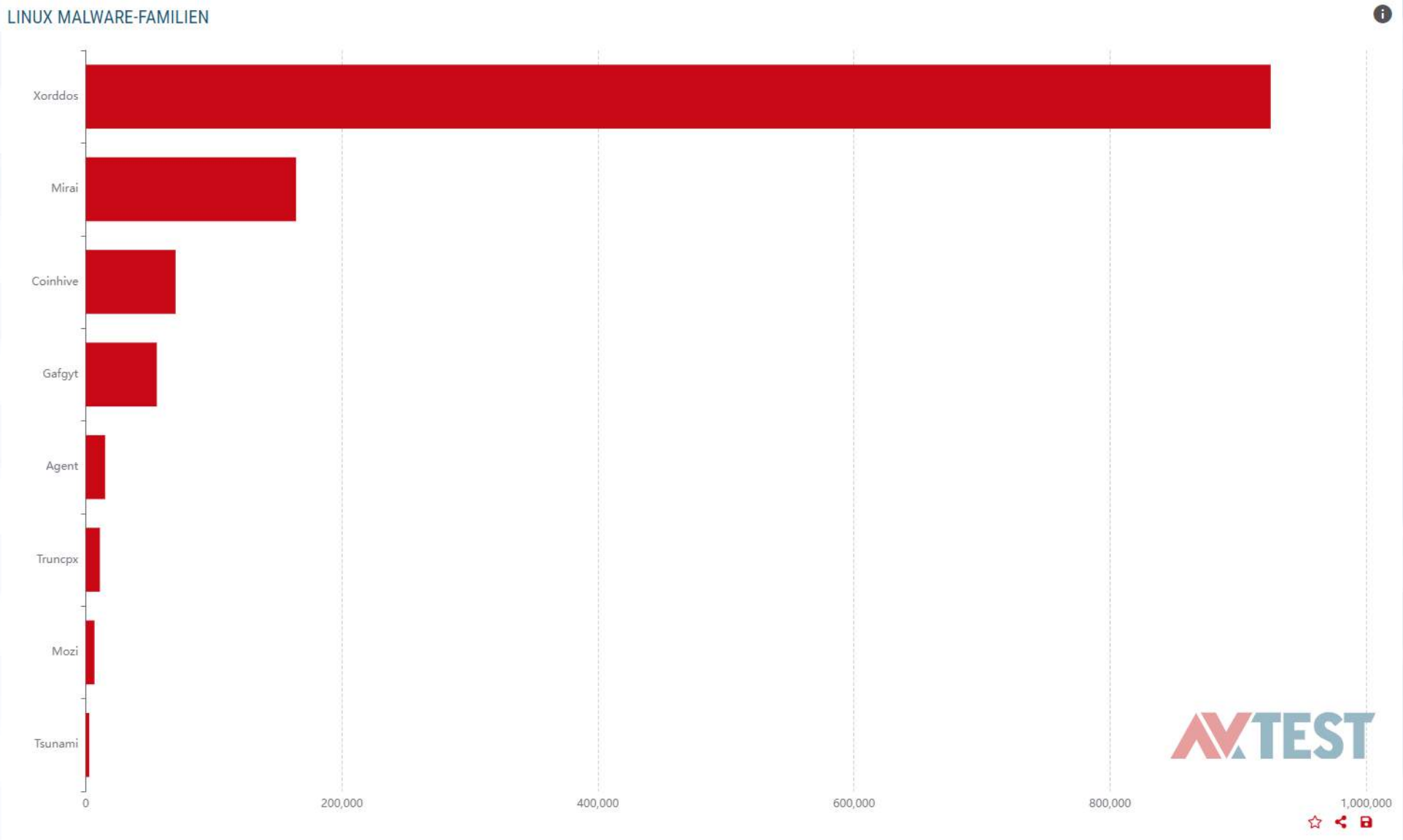
LINUX MALWAREKATEGORIEN



av-atlas

www.av-atlas.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany



avatlas www.av-atlas.org

AV-TEST

The Independent IT-Security Institute

Magdeburg Germany

Registrierte Angriffe	Nutzernamen erfasster Angriffe	Von Angreifern ausgeführte Befehle	Ursprungsland der meisten Attacken
4,334,696	root	66,942,514	Niederlande
In den letzten 14 Tagen	In den letzten 14 Tagen	In den letzten 14 Tagen	In den letzten 14 Tagen

avatlas www.av-atlas.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

- In **2021 über 20 Produkte** zertifiziert + weitere initiative und interne Tests
- Produkte u.a. aus den Kategorien **Smart Lock, Smart Home- und Alarmsystem, IP Camera, Entertainment**
- Darunter Hersteller, wie ABUS, Telekom, Bosch, Somfy, NUKI uvm.

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

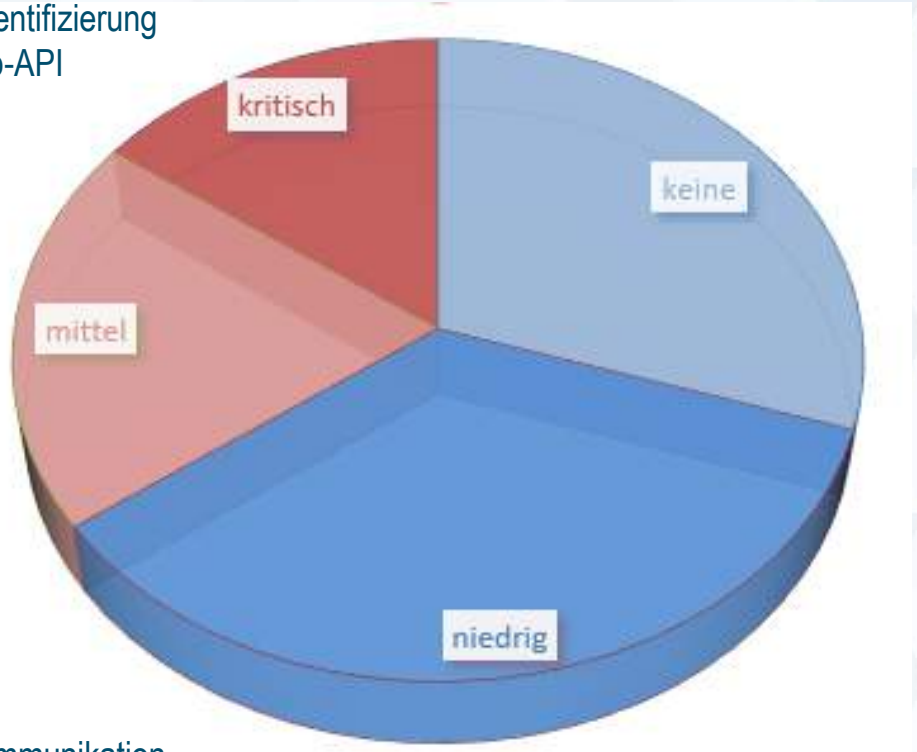
Online-Kommunikation

- **Internetbasierte Kommunikation zwischen Systemkomponenten und der mobilen Applikation und der Cloud**
- **Angriffsfläche dem Internet gegenüber**
  - **Topppriorität**, da naturgemäß schwerwiegendstes Einfallstor
  - Analyse **sämtlichen Online-Traffics** auf potentielle Schwachstellen bzgl. Verschlüsselung und Authentifizierung
  - Im Fokus: Mobile Applikation, IoT-Gerät, Hersteller-Server/-Cloud

The Independent IT-Security Institute
Magdeburg Germany

15% kritische Probleme:

- Fehlende / schwache Verschlüsselung
- Veraltete TLS-Versionen verwendet
- Zertifikats-Handling
- Fehlende Authentifizierung
- Unsichere Web-API



30% adäquat abgesichert

55% mit kleinen oder mittelschweren Problemen:

- Unverschlüsselte, unkritische Kommunikation
- Offene Ports / Schnittstellen
- Veraltete TLS-Versionen unterstützt (aber nicht aktiv verwendet)

AV-TEST The Independent IT-Security Institute Magdeburg Germany

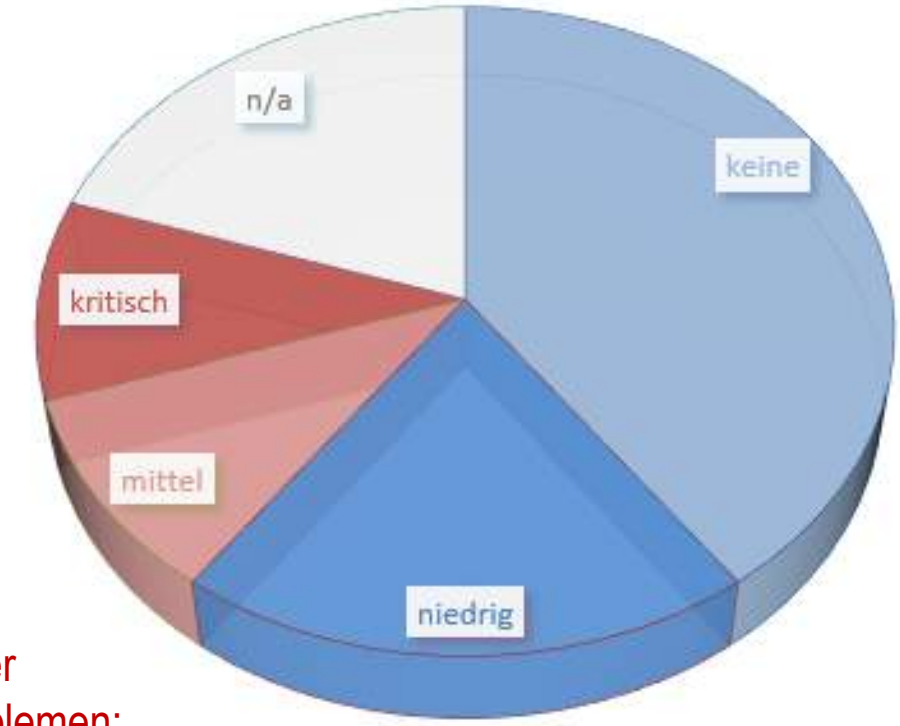
Lokale Kommunikation

- **Offline-Kommunikation zwischen Systemkomponenten und Smartphone (bspw. per LAN, Bluetooth, NFC, …)**
  - Lokale Verschlüsselung und Authentifizierung **oft aufgrund falscher Sicherheitsannahmen** und/oder zur Aufwandseinsparung **vernachlässigt**
  - Im Fokus: Mobile Applikation, IoT-Gerät, ggf. weitere Komponenten
  - Schwachstellen naturgemäß weniger kritisch, **ABER**:

Regel #1 IoT-Security: **Assume a hostile edge!**

The Independent IT-Security Institute
Magdeburg Germany

20% keine lokale Kommunikation



40% adäquat abgesichert

15% kritische Probleme:

- Fehlende / schwache Verschlüsselung
- Fehlende Authentifizierung
- Unsichere lokaler Zugang

30% mit kleinen oder mittelschweren Problemen:

- Statusinformationen
- Offene Ports / Schnittstellen
- Unverschlüsselte, unkritische Kommunikation

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Applikation

- **Sicherheitsrelevante Aspekte in Konzept und Implementation der zum Produkt gehörigen mobilen Applikation**
  - Alle 2021 getesteten Produkte mit mobiler Applikation
  - **Statische und dynamische Analyse**
  - Gerade auf **Android** ist das Reverse-Engineering meist unkompliziert und Schwachstellen treten dadurch leichter ans Tageslicht
  - Im Fokus: Mobile Applikation (Android & iOS)

AVTEST
The Independent IT-Security Institute
Magdeburg Germany

10% mittelschwere und kritische Probleme:

- Hardcoded Secrets
- Unzureichende Passwortsicherheit
- Unsichere Speicherung

90% mit kleinen Problemen:

- Suboptimale Konfigurationen
- Unsichere Methodenaufrufe
- Fehlende Speicherzugriffsschutzmechanismen (u.a. ASLR)

AV-TEST The Independent IT-Security Institute Magdeburg Germany

Datenschutz und Privatsphäre

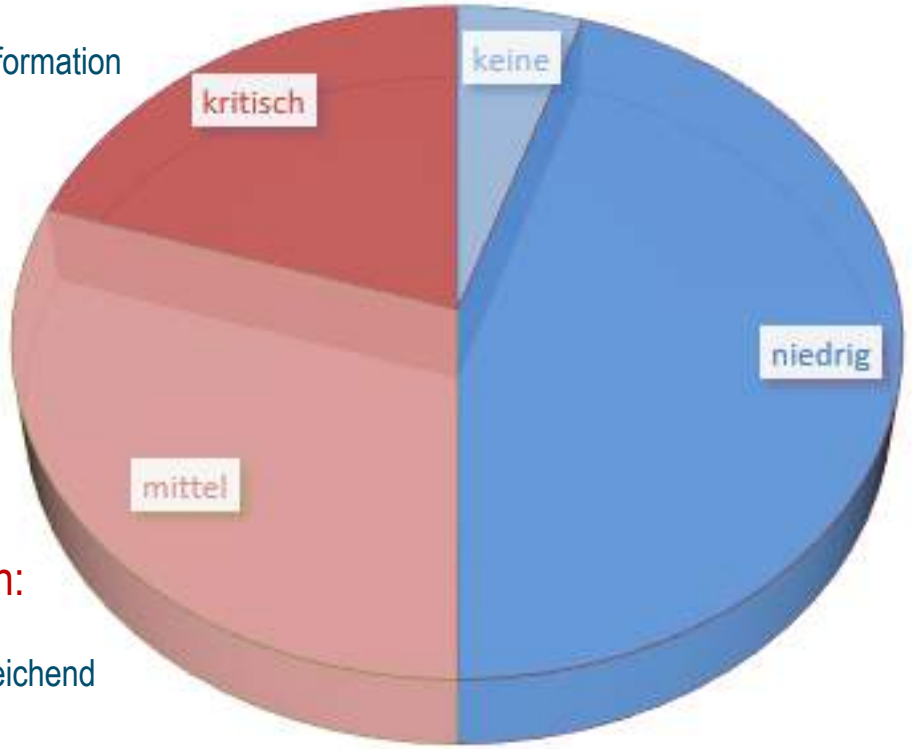
- **Schutz der personenbezogenen Nutzerdaten auf dem Übertragungsweg und in der Cloud**
- **Sammlung personenbezogener Nutzerdaten**
  - **Datenerfassungsmöglichkeiten** (Sensorik, Tracker) VS. **Geräteverhalten/-kommunikation** VS. **Datenschutzerklärung**
  - Vom Hersteller **angenommenes** Verhalten VS. **tatsächliches** Verhalten
  - (relativ) junge DSGVO (und neu TTDSG)
  - Im Fokus: Datenschutzerklärung, mobile Applikation, IoT-Gerät

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

5% ohne Probleme

20% mit kritischen Problemen:

- Schwere Inkonsistenz Verhalten vs. Information
- Fehlende Datenschutzerklärung
- Nicht dokumentierte Tracker



45% mit kleinen Problemen:

- Leichte Inkonsistenzen
- Ausbaufähige Transparenz
- Formalitäten

30% mit mittelschweren Problemen:

- Inkonsistenz Verhalten vs. Information
- Detailgrad Datenschutzerklärung unzureichend
- Menge Werbe-/Analyse-Tracker

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Fazit

- Jährlich **steigendes Sicherheitsniveau**, ABER auch jährlich **steigendes Bedrohungspotential**
- Immer noch teilweise **unnötige und „ausgestorben“ geglaubte Schwachstellen**
- **Datenschutz und Privatsphäre** immer weiter im Fokus
- **Datenklau** vs. **Datensammlung**

Vielen Dank für Ihre Aufmerksamkeit!

Follow us on Twitter @avtestorg

Find us at facebook.com/avtestorg

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

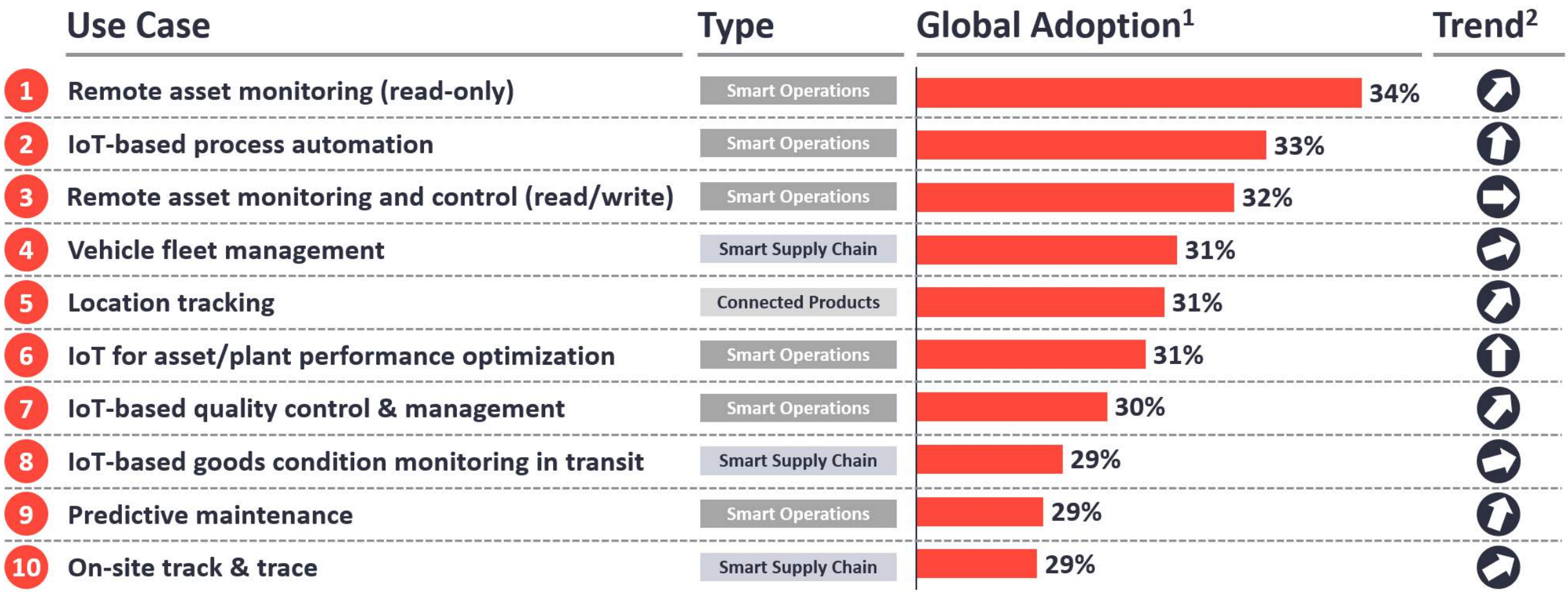
Automate IoT Security & Compliance – Risk & Cost Reduction

IoT Inspector | March 2022 | Jan C. Wendenburg, CEO

eco
ASSOCIATION OF THE INTERNET INDUSTRY

The Top 10 IoT Use Cases

N= 1,640 IoT Projects



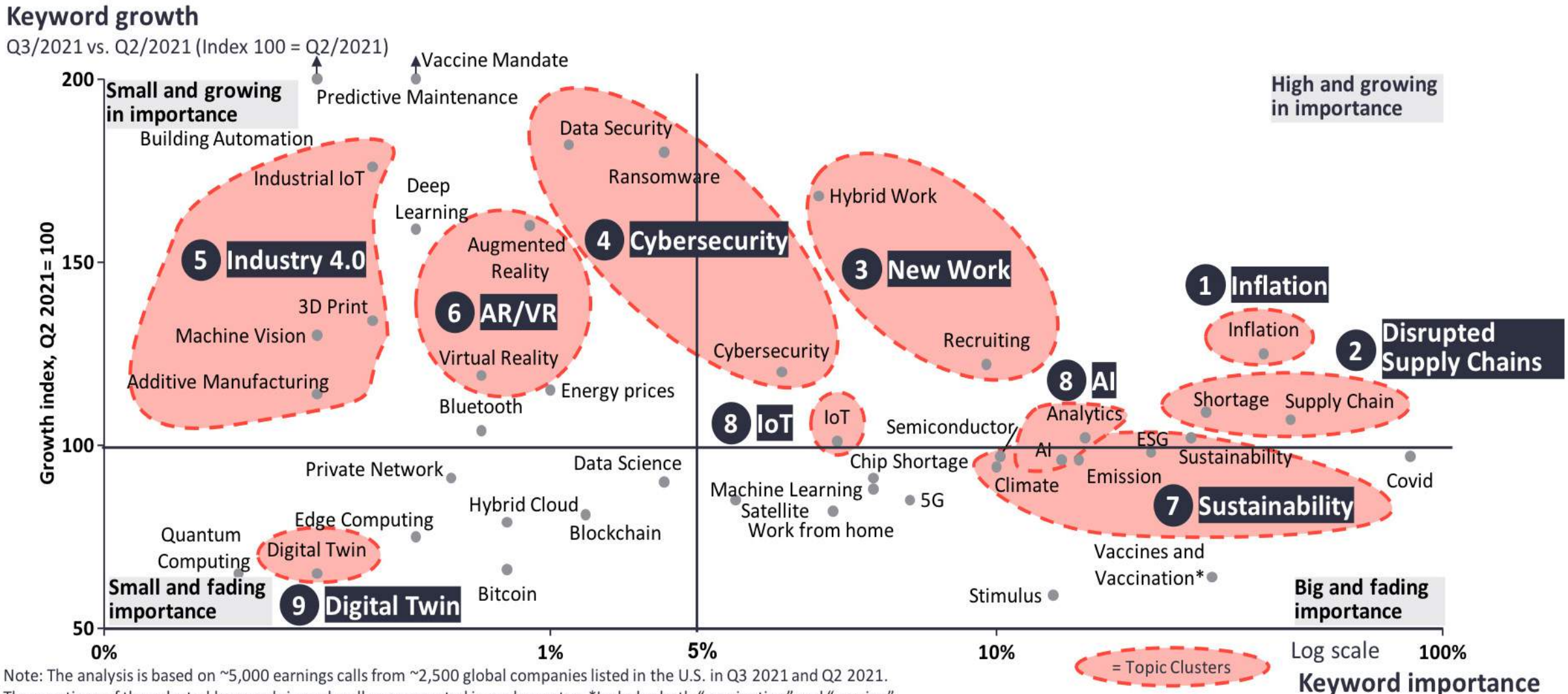
... of 48 use cases analyzed in total

Note 1: Share of companies that have at least partially rolled-out the use case **Note 2:** Based on respondents' indication of investment plan in in the next 2 years
Source: IoT Analytics Research 2021, Conditions for republishing: Source citation with link to original post and company website; Non-commercial purposes only

Very strong investments expected in next 2 years

Moderate investments expected in next 2 years

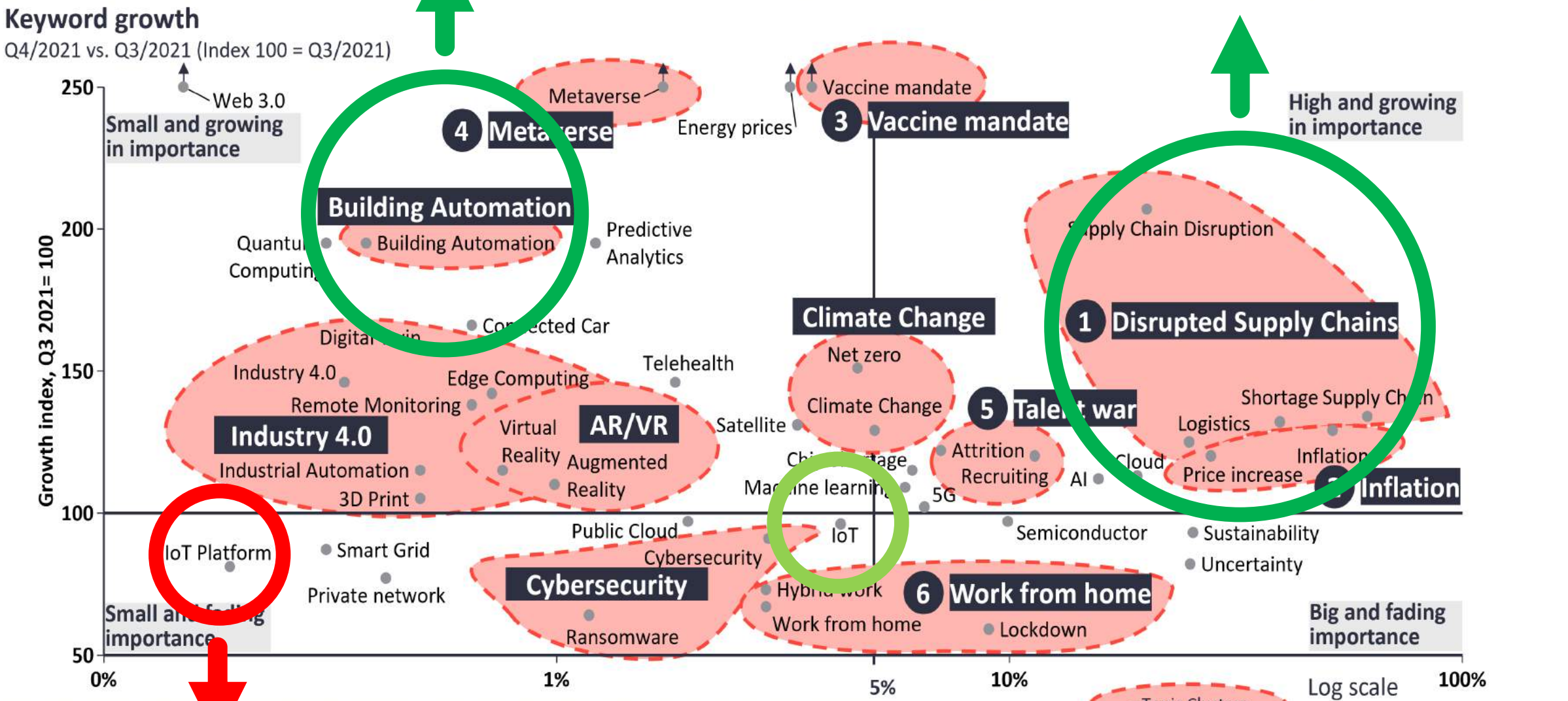
What CEOs talked about in Q3/2021 (vs. Q2/2021)



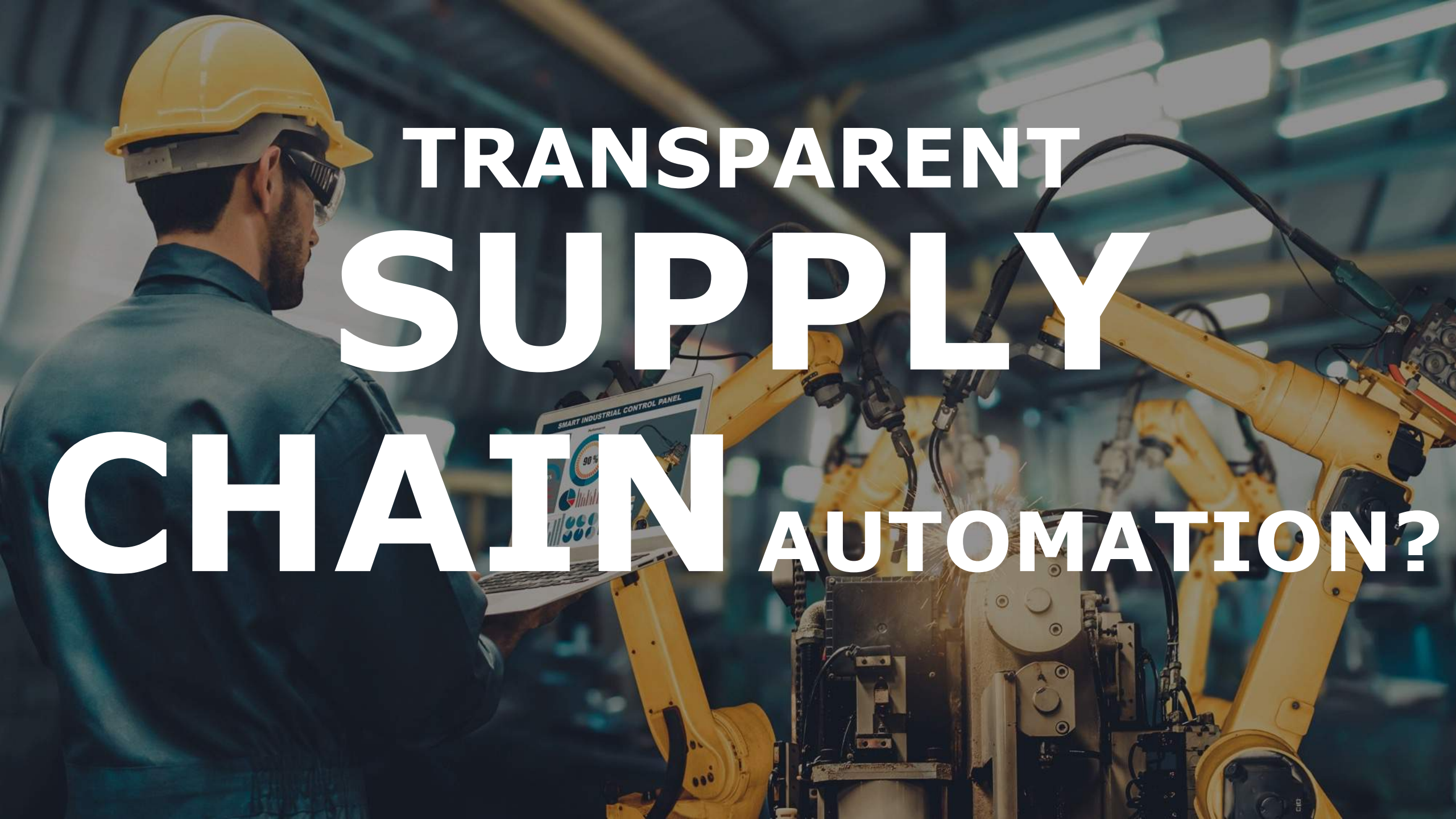
Note: The analysis is based on ~5,000 earnings calls from ~2,500 global companies listed in the U.S. in Q3 2021 and Q2 2021. The mentions of the selected keywords in each call were counted in each quarter. *Includes both "vaccination" and "vaccine"

Source: IoT Analytics Research 2021

What CEOs talked about in Q4/2021 (vs. Q3/2021)



Note: The analysis is based on 5,000 earnings calls from ~2,500 global companies listed in the U.S. in Q4 2021 and Q3 2021.
The mentions of the selected keywords in each call were counted in each quarter.
Source: IoT Analytics Research 2022



TRANSPARENT SUPPLY CHAIN AUTOMATION?

SECURITY IN FAST GROWTH IOT MARKETS

CHALLENGE

Challenge

- Over 25 bn IoT devices in 2030 and further growing*
- Vast heterogenous IoT/IIoT/OT technology stacks
- Manual analysis are time consuming & expensive
- Shortage of more than 3.1m cybersecurity professionals*

Limited resources, time consuming, expensive!

Market Demand

- Continuous 24/7/365 visibility of IoT/IIoT/OT risks
- Transparent software supply chains
- Continuous supply chain risk monitoring
- Realtime alerts for new vulnerabilities on IoT/IIoT/OT devices

Full risk transparency & 24/7/365 alerts!

Solution

- Automated pen-testing services automating the effort of a manual penetration test in minutes (30 minutes vs. 5 days)
- Full software supply chain transparency
- Highly scalable and available 24/7/365.
- Continuous monitoring & auto risk alerts 24/7/365

Automation is key!

IOT INSPECTOR

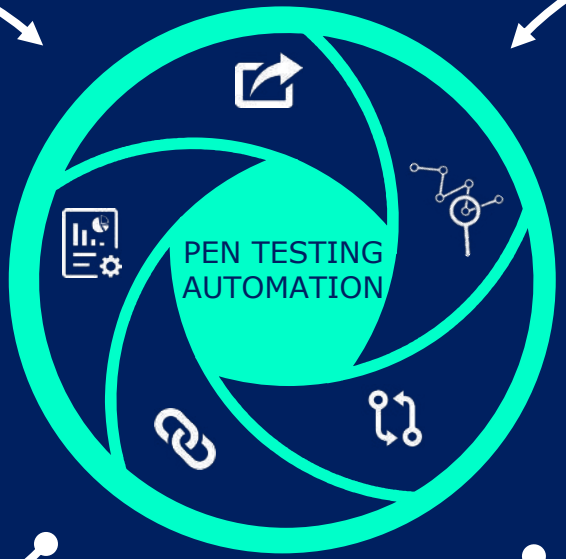
*Source: Statista 10/2021, ISC2.ORG Cybersecurity Workforce Study

PROCESS AUTOMATION & INTEGRATION

CONTINUOUS SECURITY & COMPLIANCE

Device Vendors

Enabling "Security By Design" through instant security feedback to developers



"Security & Compliance Quality Gate" for software & device supply chain

Device Buyers

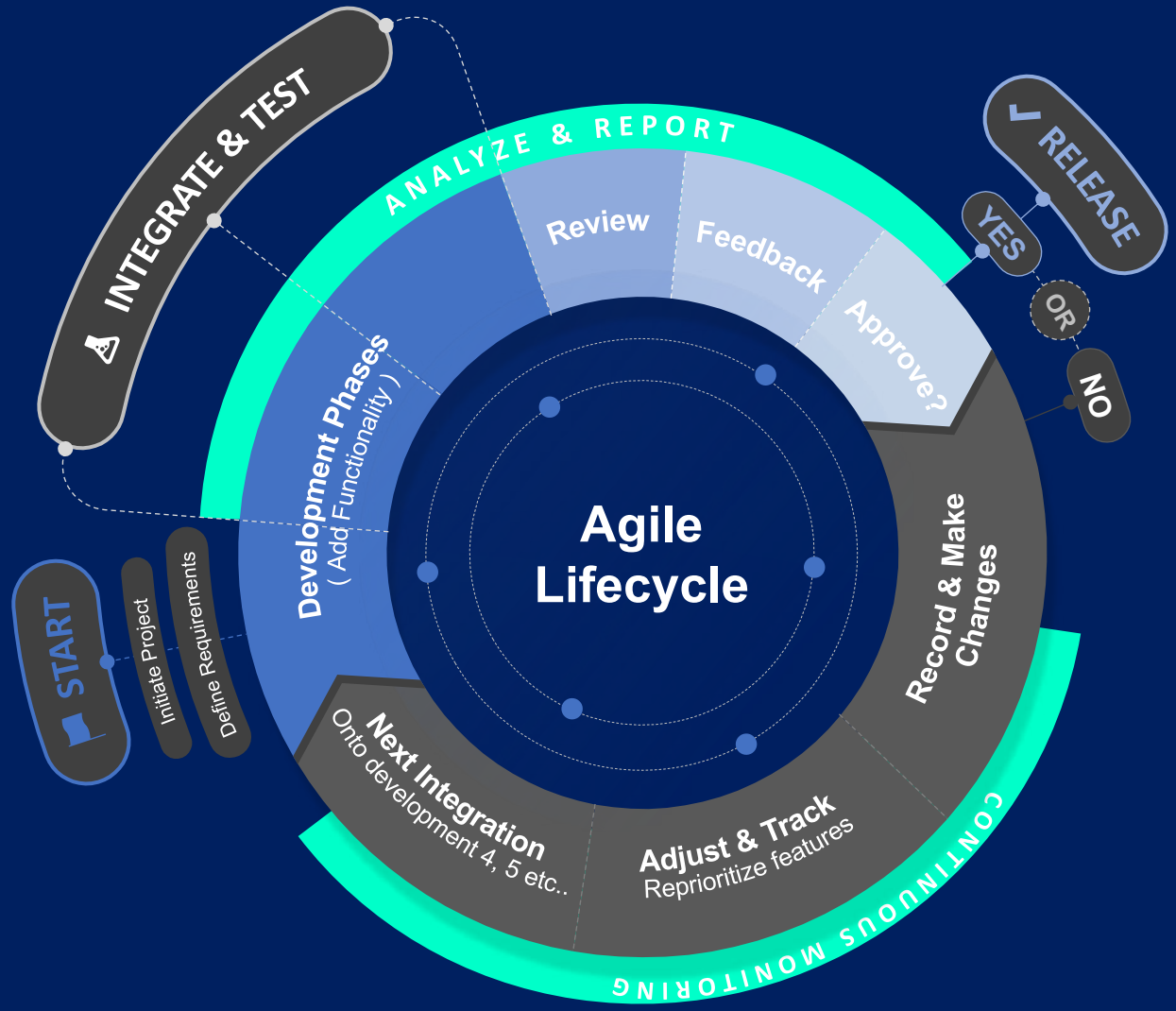
IOT INSPECTOR

SAMPLE DEV PROCESS INTEGRATION

CONTINUOUS SECURITY & COMPLIANCE

(Pen)testing shall be integrated into the **daily** development process – not only before releasing software.

"Upgrading" agile SDLC processes with **instant** audits on security & compliance.

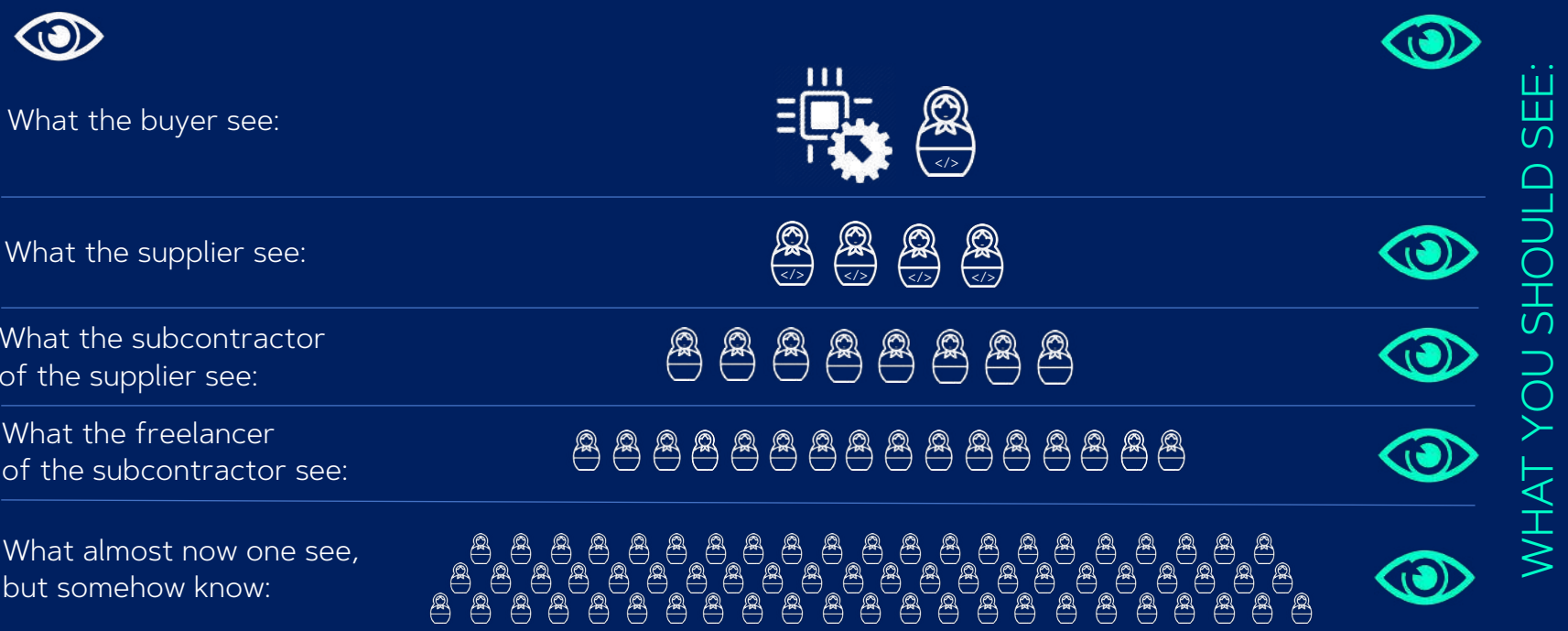


IOT INSPECTOR

BUYER'S SUPPLY CHAIN TRANSPARENCY

SOLVING THE MATRYOSHKA (RUSSIAN DOLL) PROBLEM

Automated software composition analysis enables organizations to verify & check supplier's supply chain transparency on binary code level.



IOT INSPECTOR

KEY BENEFITS – IOT VENDORS

REDUCED DEVELOPMENT EFFORTS, INCREASED QUALITY & COMPLIANCE

- Reduces software development cost & resources
- Reduces software development time
- Consistent level & quality of security & compliance testing
- Reduces total software development project risks
- Continuous security & compliance check of installed devices

IOT INSPECTOR

KEY BENEFITS – IOT CORPORATE BUYERS

INDEPENDENT QUALITY GATE ENSURES SECURITY & COMPLIANCE

Independent procurement quality gate for security & compliance

- enables organizations to carry out automated security and compliance checking of purchased devices (quality gate & SBOM)
- Enables predictive security testing before production

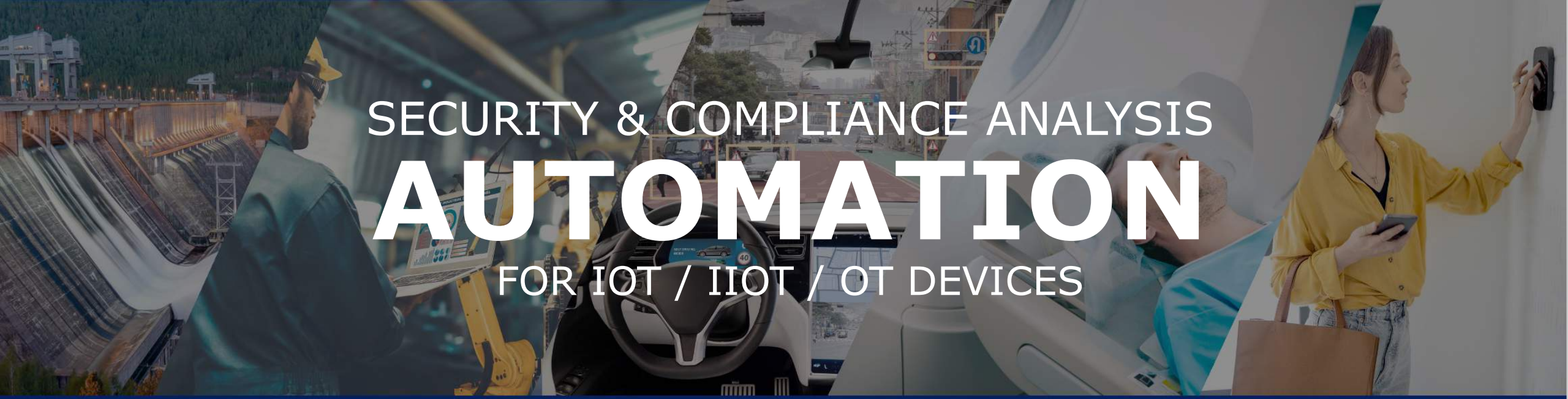
Continuous security & compliance check of installed devices

- the “Digital IOT Twin” monitoring enables a fully automated checking of the installed IoT/OT/IIoT devices, without the need of network or physical access

Reduces total procurement project risks

- reduced costs and resources for procurement security & compliance checks resulting in reduced procurement project risks

IOT INSPECTOR



SECURITY & COMPLIANCE ANALYSIS

AUTOMATION

FOR IOT / IIOT / OT DEVICES

THANK YOU

IOT INSPECTOR GMBH
Kaiserswerther Straße 45
40477 Düsseldorf / Germany
+49 211 158 741 04
info@iot-inspector.com
www.iot-inspector.com

JAN C. WENDENBURG, CEO
Mobile: +49 171 5555312
jan.wendenburg@iot-inspector.com

SecurITy made in Germany

SevenShift

Let's talk about security in IoT

from security-by-design to testing

SevenShift

ABOUT SevenShift

SevenShift is a boutique security consulting firm with a wealth of experience in the worlds of Cybersecurity and Internet of Things (IoT).

CONTACT

SevenShift GmbH

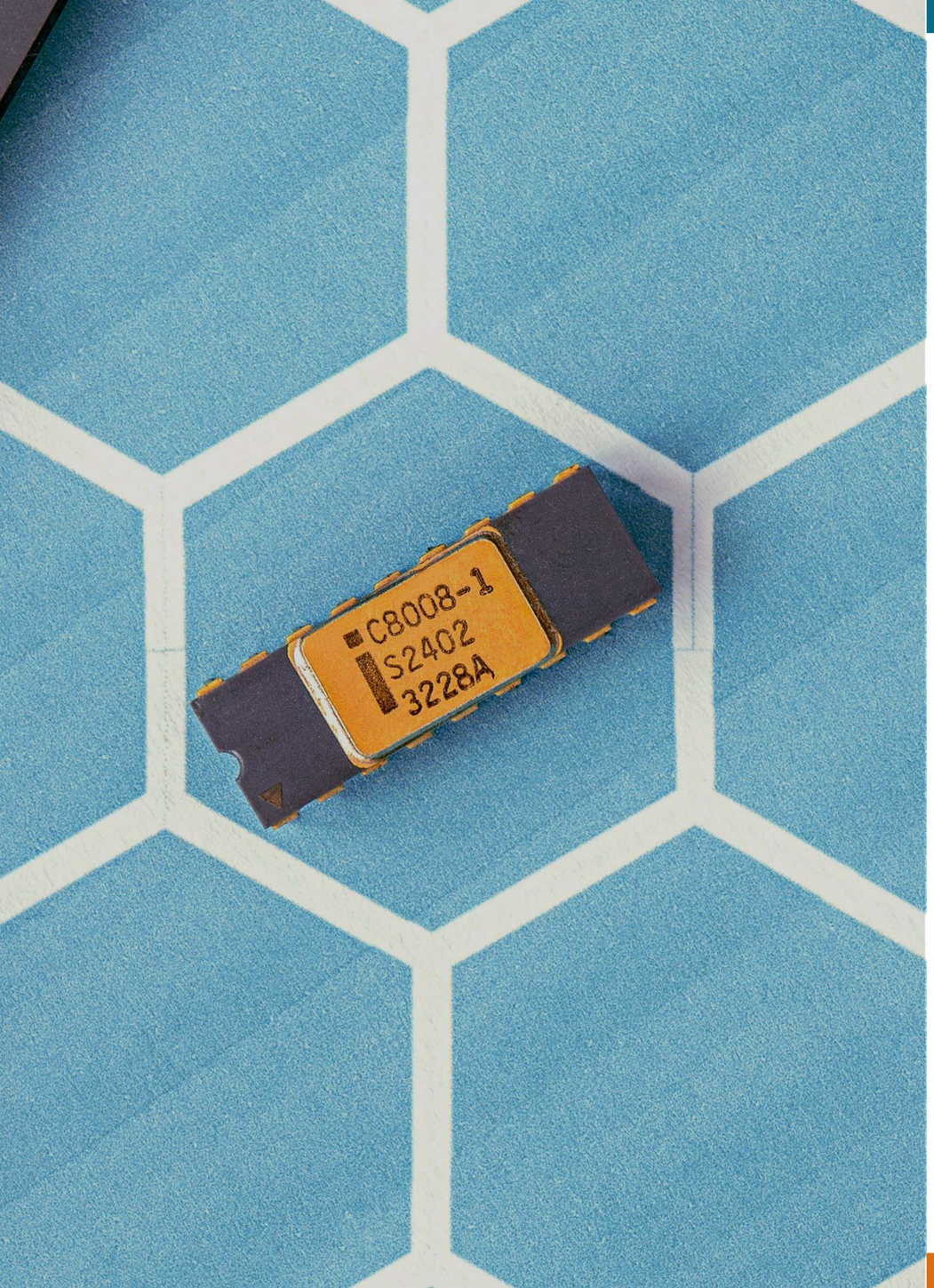
Im Mediapark 5, 50670 Köln

+49 221 952 609 12

info@sevenshift.de

Web: sevenshift.de

@SevenShift_de



Our Services

Security Testing

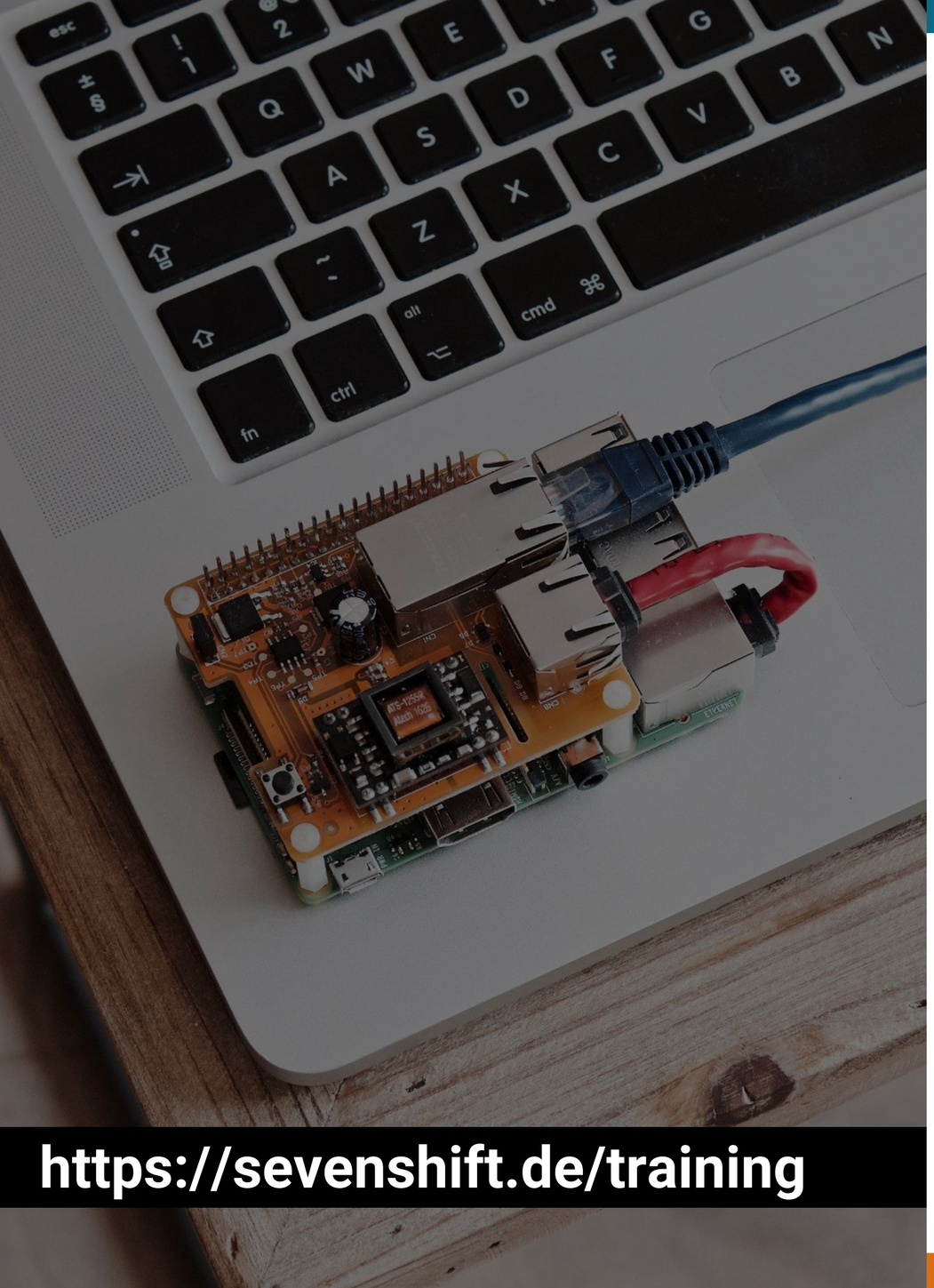
- IoT devices, applications, networks, mobile apps …

Engineering and Consulting

- Security-by-design
- Certification support
- Automation

Training

- Public and private
- Online or onsite



Trainings

- IoT Security Master Class
- IoT Security Bootcamp
- Assessing and Exploiting Control Systems & IIoT
- Security Awareness

Next Trainings

- Take place **in spring and winter**
- Check dates on our website
- **All live and online**

Pablo Endres

Managing Director
Lead Security Consultant

epablo@sevenshift.de

@epablosensei

https://www.linkedin.com/in/pabloendres

Experienced security consultant,
Professional Hacker and
Trainer

- Professional Hacker and Security Trainer
  - IoT Security {Bootcamp, Strategy} ICS or IIoT
- Penetration and security testing (design, planning and execution)
  - IoT, IIoT, ICS, Infrastructure, Cloud, Web, Mobile …
- Security consulting: architecture, secure-by-design, programs..
- Project management
- Certified: CISSP, OPSA, OPST
- Special interest: Karate and slacklining

Agenda

01 – IoT Security

02 – Security-by-design

03 – Security Testing

Photo by Paul Frenzel on Unsplash

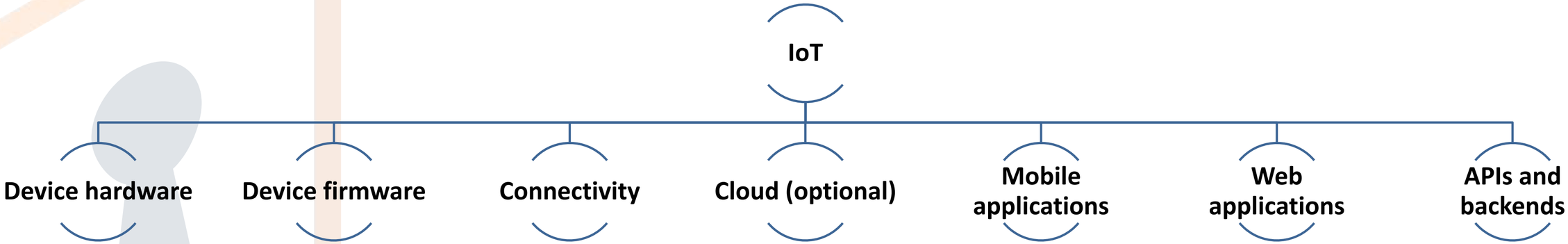
What is IoT

What is IoT

- Internet of Things
- Connected objects interacting with the physical world (sensors / actors)
- Used for automation, monitoring, and data collection purposes
- Consumer IoT: smart watches, plugs, home, etc
- Automotive
- IIoT: smart city (parking), ICS, SCADA, smart grid

https://en.wikipedia.org/wiki/Smart_meter#/media/File:Intelligenter_zaehler-_Smart_meter.jpg

IoT is complex



We must deal with ..

- Complexity
- Interactions
- Weaknesses

of all the layers and components if we want to make this **secure**

Status of IoT Security?

Most companies are more focused on the time to market and the price than security

Attack surface for IoT devices

Can be split into 4 categories :

- Device security vulnerabilities
- Firmware based vulnerabilities
- Mobile, Web, Cloud and Infrastructure, and Network security issues
- Radio communication-based vulnerabilities

Basic security principles

- Secure all data in motion and at rest
- Use secure defaults
- Least privilege
- Trust, but verify
- Use only secure components
- Upgrades and factory resets must be possible
- Defense-in-depth
- Define security requirements

Security-by-design

Let's talk about design

"Design adds value faster than it adds costs."

-- Joel Spolsky, web programmer, writer, and creator of Trello

"Design is not just what it looks like and feels like. Design is how it works."

-- Steve Jobs, co-founder of Apple, Inc.

"The alternative to good design is always bad design.

There is no such thing as no design."

-- Adam Judge, author

Secure by design

From Wikipedia, the free encyclopedia

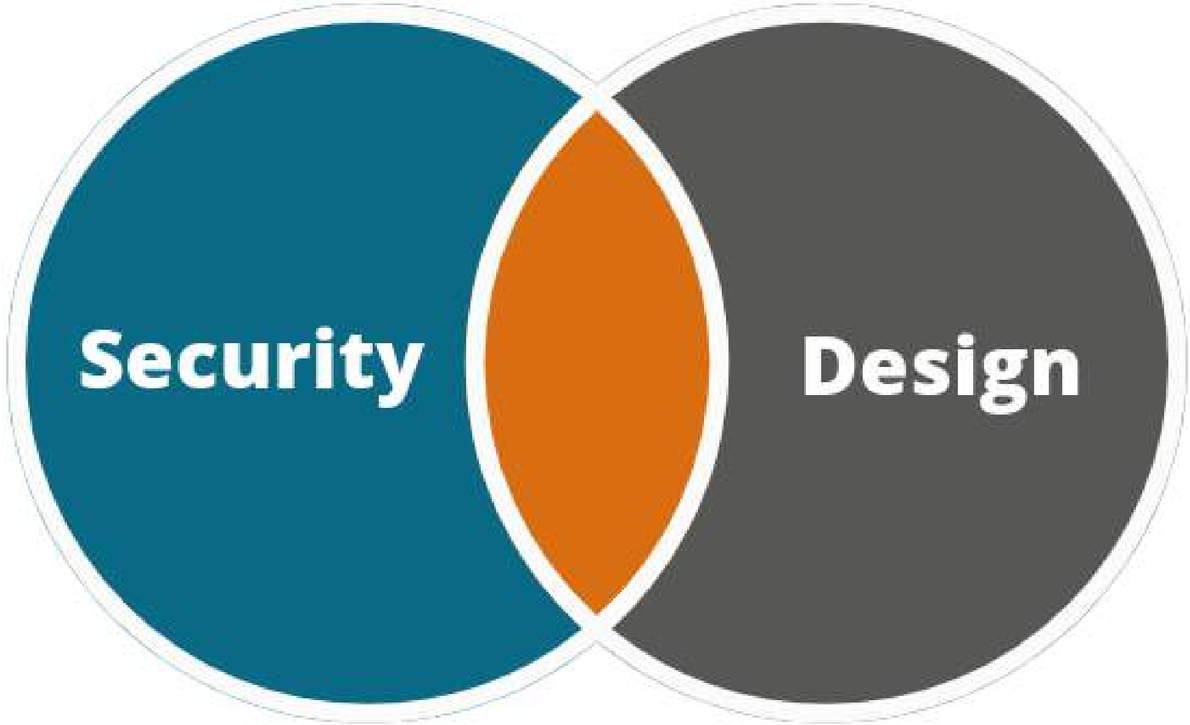
Secure by design, in software engineering, means that software products and capabilities have been designed to be foundationally secure.

Alternate security strategies, tactics and patterns are considered at the beginning of a software design, and the best are selected and enforced by the architecture, and they are used as guiding principles for developers.

Security-by-design

Make security part of your SDLC

- Iterative process
- Part of the design
- Plan into each sprint
- Fail early and adapt
- DevSecOps

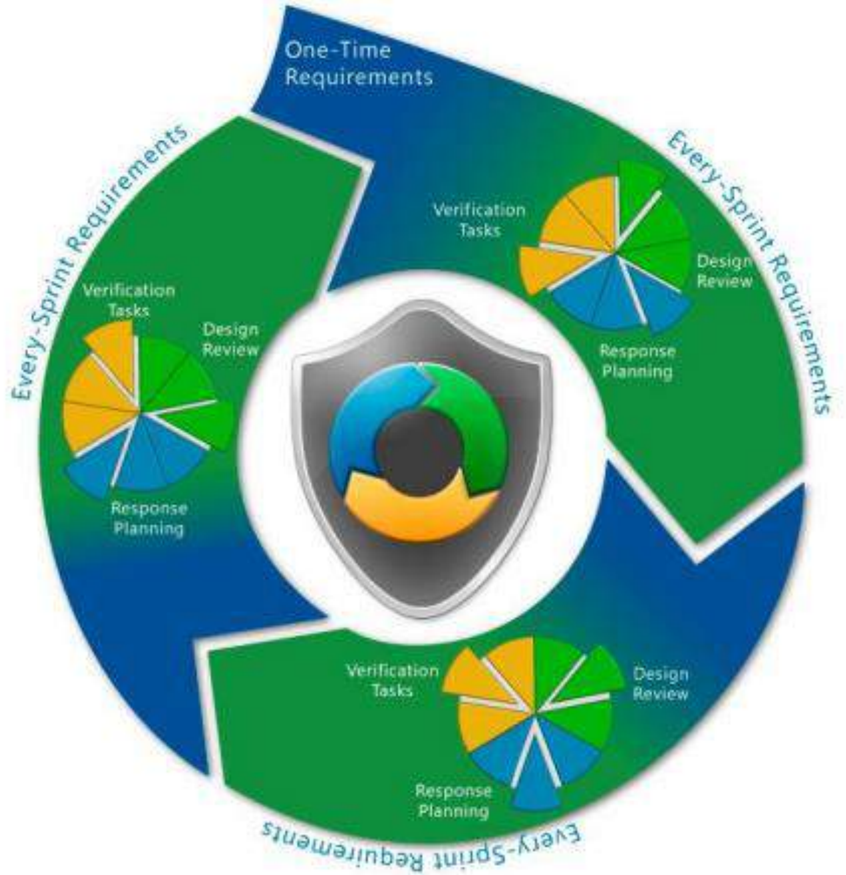


Reduce costs 20 - 100x

Agile Secure Development Lifecycle

SDL Requirement Categories:

- Every-Sprint
- Bucket
  - Verification Tasks
  - Design Review Tasks
  - Response Planning Tasks
- One-Time



Microsoft SDL for Agile development
https://owasp.org/www-pdf-archive/OWASP_AppSec_Research_2010_Microsoft_SDL_Agile_by_Coblentz.pdf

Agile SDL: Every Sprint

Essential tasks that must be done each sprint

Examples:

- Update the threat model
- Communicate privacy impacting design changes to the team's privacy advisor
- Fix all issues identified by code analysis tools for unmanaged code
- Follow input validation and output encoding guidelines to defend against cross-site scripting attacks

Microsoft SDL for Agile development
https://owasp.org/www-pdf-archive/OWASP_AppSec_Research_2010_Microsoft_SDL_Agile_by_Coblentz.pdf

Agile SDL: Bucket Requirements

- Teams prioritize the pool of tasks over many sprints
- Each sprint, one task from each bucket completed
- Each tasks must be completed at least every 6 months

Examples:

- Security Verification Tasks
  - Run fuzzing tools
  - Manual and automated code review
- Design Review Tasks
  - Conduct privacy review
  - In-depth threat model
- Response Planning Tasks
  - Define security/privacy bug bar
  - Create support documents

Microsoft SDL for Agile development
https://owasp.org/www-pdf-archive/OWASP_AppSec_Research_2010_Microsoft_SDL_Agile_by_Coblentz.pdf

Agile SDL: One-Time Requirements

Why?

- Repetition not necessary
- Must occur at the beginning of the project
- Not possible at the beginning of the project

Examples:

- Setup bug tracking system (3 m)
- Identify sec./privacy experts (1 m)
- Baseline threat model (3 m)
- Establish a security response plan (6 m)

Microsoft SDL for Agile development
https://owasp.org/www-pdf-archive/OWASP_AppSec_Research_2010_Microsoft_SDL_Agile_by_Coblentz.pdf

Security Testing

Security Testing

- Complex
- Many domains
- Hard to standardize
- Requires security and technical expertise
- Follow methodologies or standards

OWASP

- Open Web Application Security Project® (OWASP)
- Non-profit foundation
- Community-led open-source software projects, tools and resources
- Focus: web applications (Top Ten)
  - Covers mobile apps, IoT, and more!
- Evaluates the top vectors and security
- Technical and business impact

OWASP

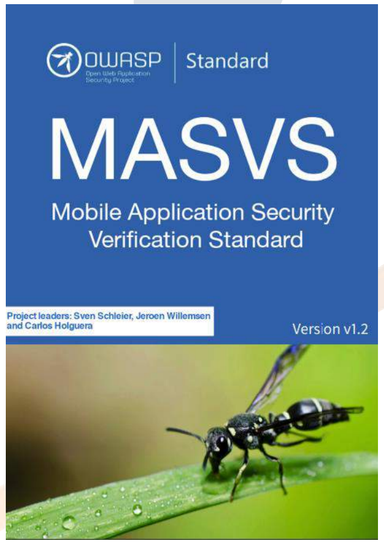
- Provides instructions on how to test, verify, and remediate each vulnerable part of an application

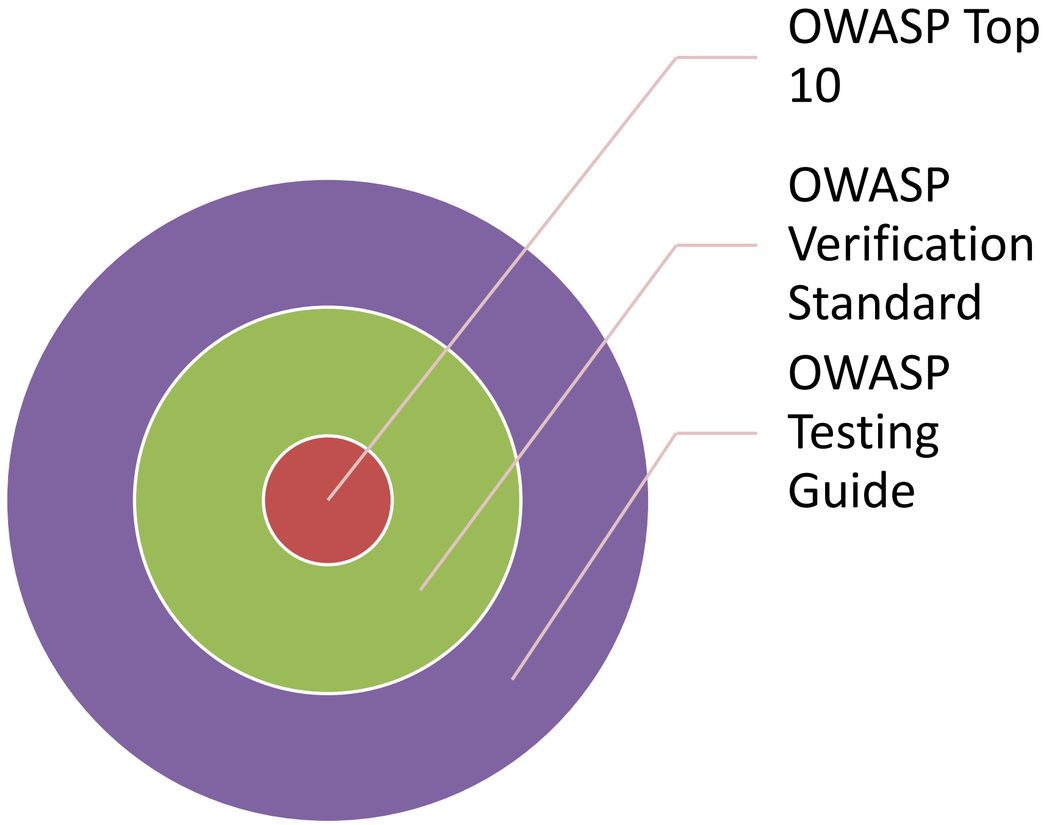
- Ensures that the most common attacks and weaknesses are avoided
  - CIA triad (Confidentiality, integrity and availability) of an application is maintained

- Provides technology specific assessment details
  - Oracle database is different than MySQL

OWASP Top 10s

- OWASP Top 10 is just that
  - Tip of the iceberg
  - Don’t stop there
  - Get professional help





OWASP Web Top 10 2021

Photo by Richy Great on Unsplash

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

OWASP API Security Top 10 2019

API1:2019 Broken Object Level Authorization

API2:2019 Broken User Authentication

API3:2019 Excessive Data Exposure

API4:2019 Lack of Resources & Rate Limiting

API5:2019 Broken Function Level Authorization

API6:2019 Mass Assignment

API7:2019 Security Misconfiguration

API8:2019 Injection

API9:2019 Improper Assets Management

API10:2019 Insufficient Logging & Monitoring

OWASP IoT Top 10

I1. Weak Guessable, or Hardcoded Passwords

I2. Insecure Network Services

I3. Insecure Ecosystem Interfaces

I4. Lack of Secure Update Mechanism

I5. Use of Insecure or Outdated Components

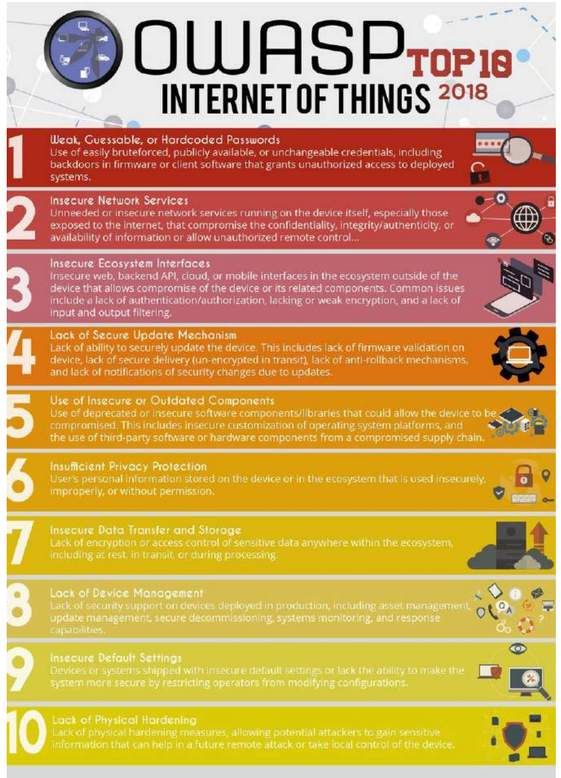
I6. Insufficient Privacy Protection

I7. Insecure Data Transfer and Storage

I8. Lack of Device Management

I9. Insecure Default Settings

I10. Lack of Physical Hardening

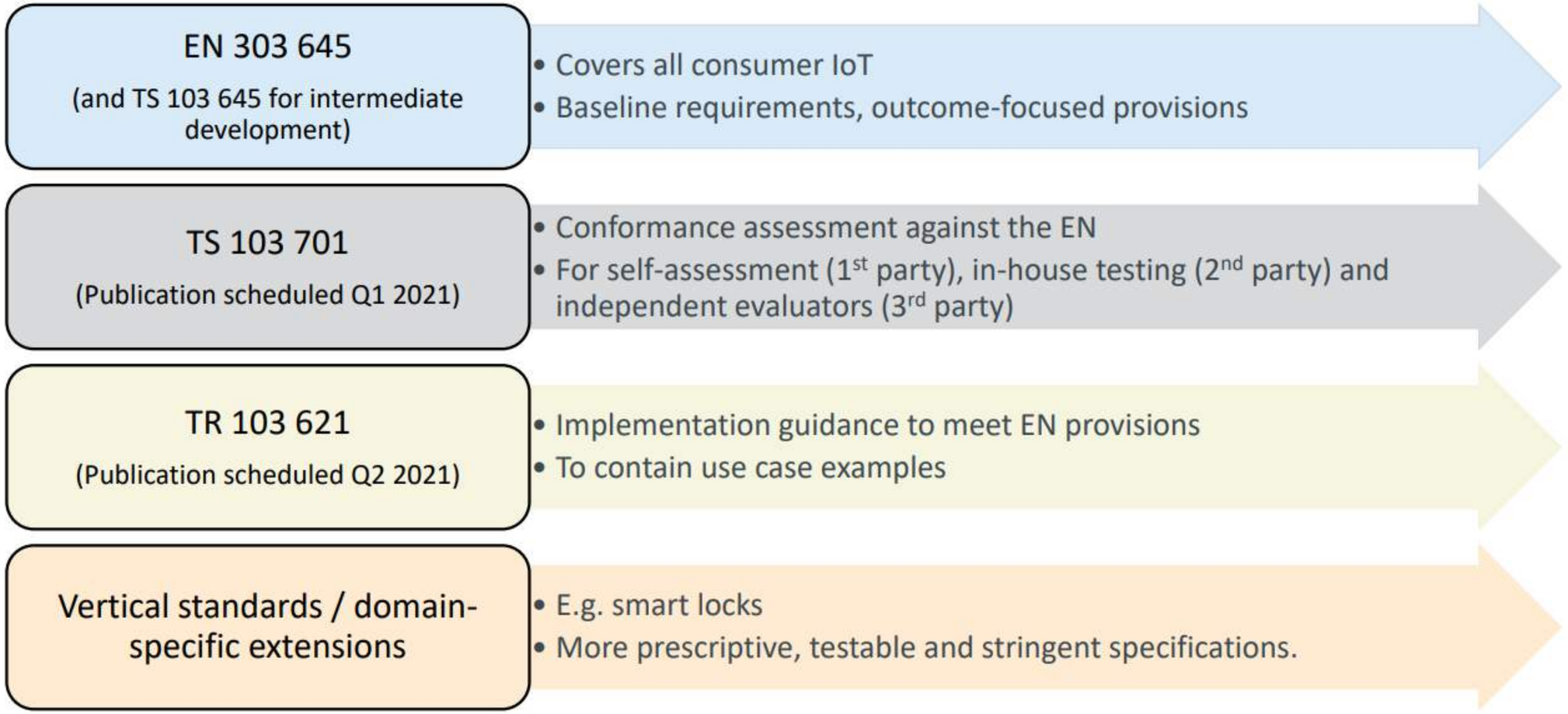


SevenShift

OWASP Security Design Principles

1. Minimise attack surface area
2. Establish secure defaults
3. The principle of Least privilege
4. The principle of Defence in depth
5. Fail securely
6. Don’t trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

ETSI consumer IoT security documents



ESTI EN 303 645

5.1 No universal default passwords
5.2 Implement a means to manage reports of vulnerabilities
5.3 Keep software updated
5.4 Securely store sensitive security parameters
5.5 Communicate securely
5.6 Minimize exposed attack surfaces
5.7 Ensure software integrity
5.8 Ensure that personal data is secure
5.9 Make systems resilient to outages
5.10 Examine system telemetry data
5.11 Make it easy for users to delete user data
5.12 Make installation and maintenance of devices easy
5.13 Validate input data

Norms and enforcement

"IoT security in the consumer industry is not where it needs to be. Many devices on the market can only meet three or four of the 13 recommendations"

-- Alex Leadbeater, the ETSI TC Cyber chairman

Enforcement is a problem

Main drivers:

- Regulation
  - Cybersecurity Act
  - Radio Equipment Directive (RED)
- Market

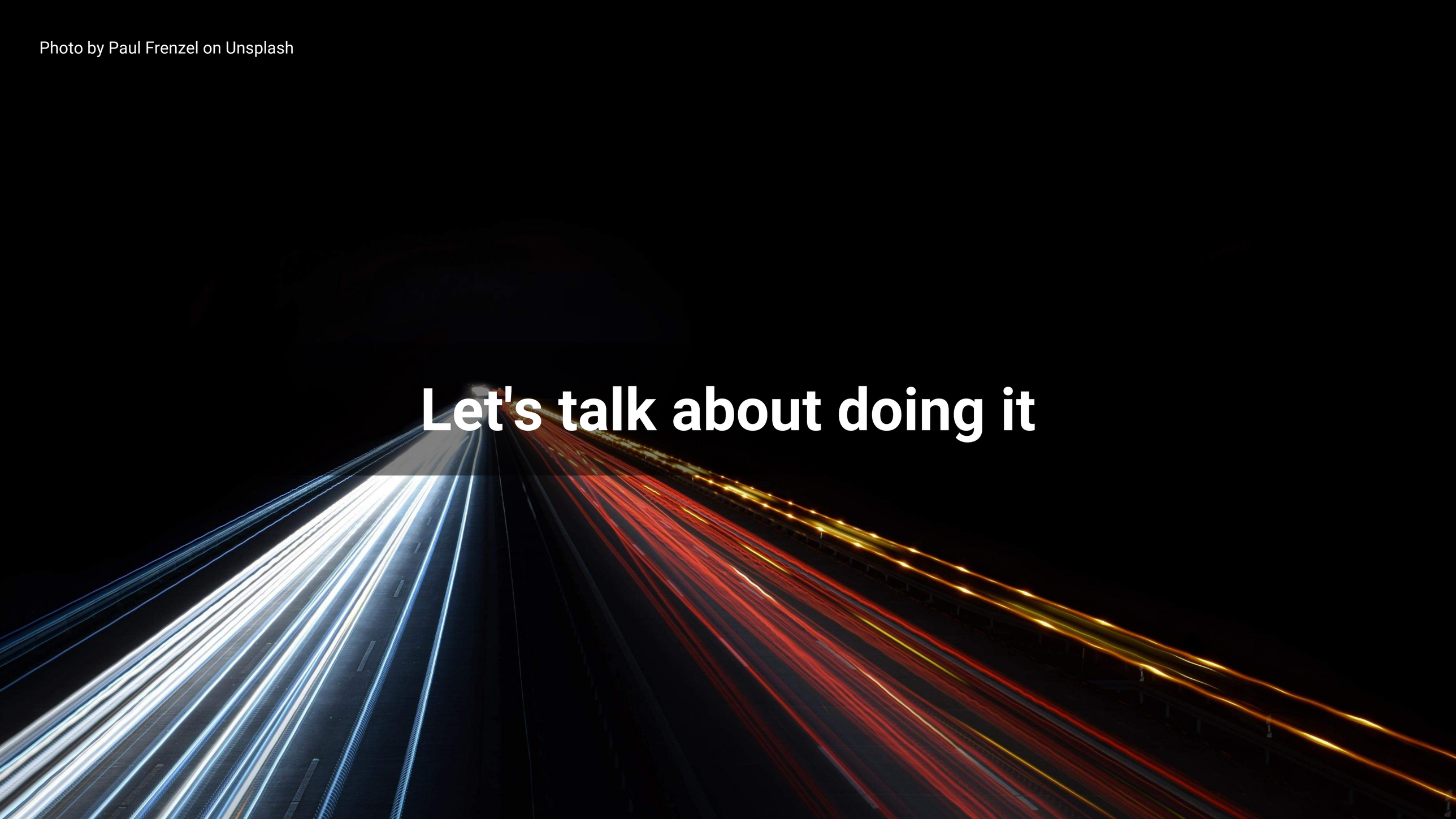


Photo by Paul Frenzel on Unsplash
Let's talk about doing it

Let's talk about doing it

- Most devices are not secure-by-design (nor implementation)
- Security-by-design is effort intensive -> but pays off
  - Set your requirements
  - Bake it into your SDLC
  - Test, test, and test
  - Get professional help

- Cover your basics
  - Password and auth
  - Updates
  - Encryption

Let's talk about doing it

- Remember the design principles

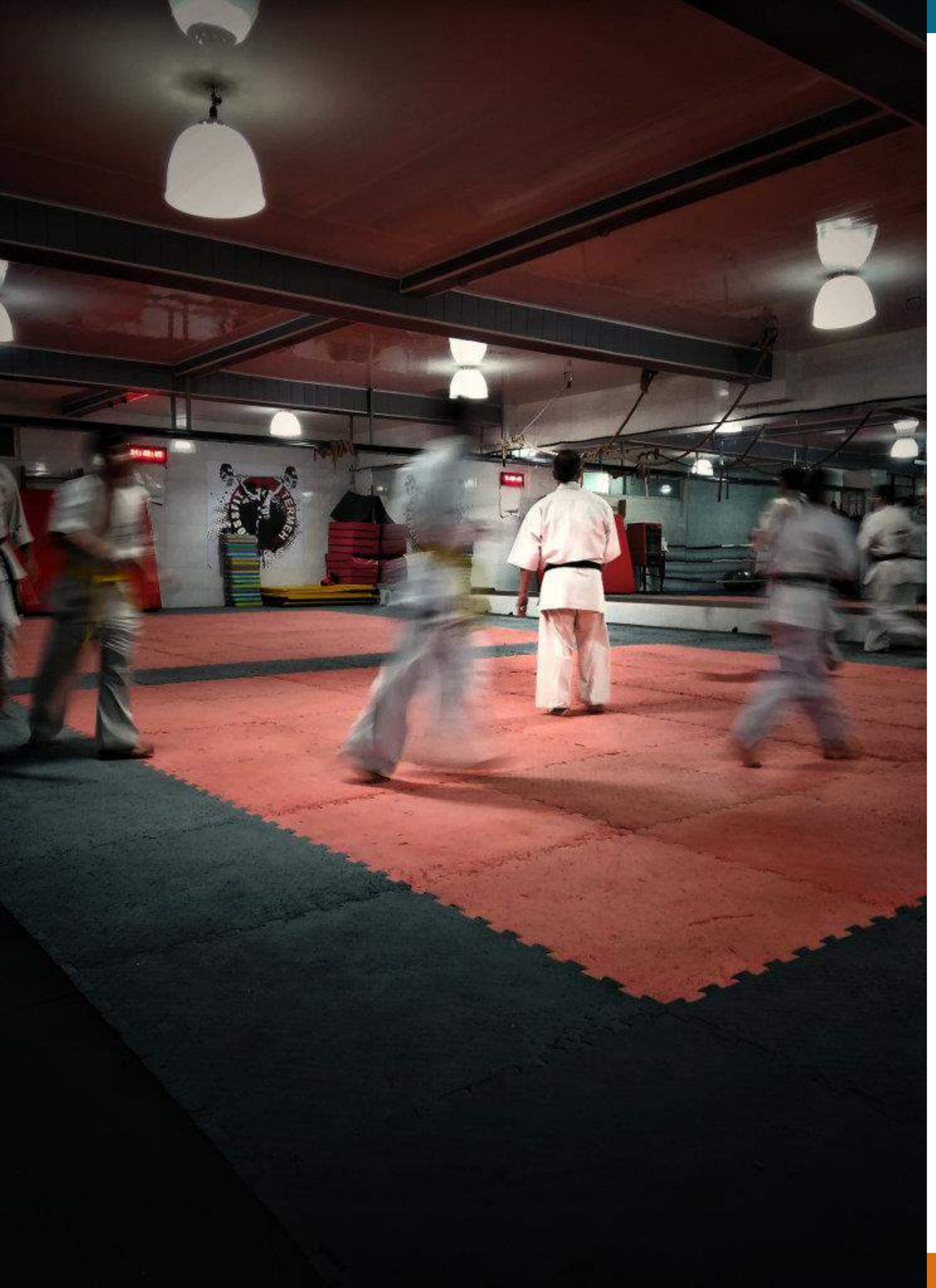
- Cover your basics
  - Password and auth
  - Updates
  - Encryption
  - ...

1. Minimise attack surface area
2. Establish secure defaults
3. The principle of Least privilege
4. The principle of Defence in depth
5. Fail securely
6. Don’t trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

SevenShift

Questions?

Photo by Seth Reese on Unsplash



epablo@sevenshift.de

@epablosensei

https://www.linkedin.com/in/pabloendres

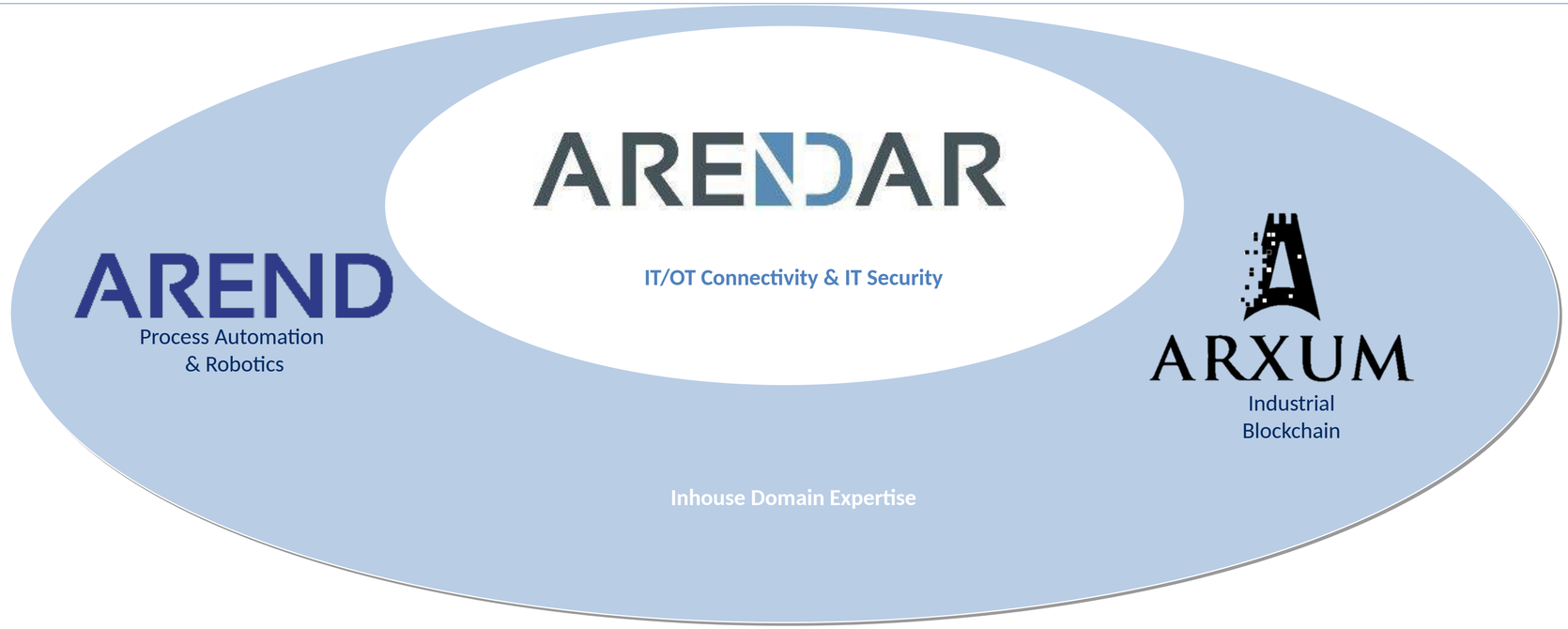
https://pabloendres.com
https://sevenshift.de

Thank you for your time

Integrated Solution Platform for Digitization and Process Connectivity

Sicherheit im IoT: IoT-Sicherheitskennzeichen, Sicherheitslücken, Einfallstore – Wie können neue Standards helfen?

ARENDAR – Teil der AAA-Gruppe



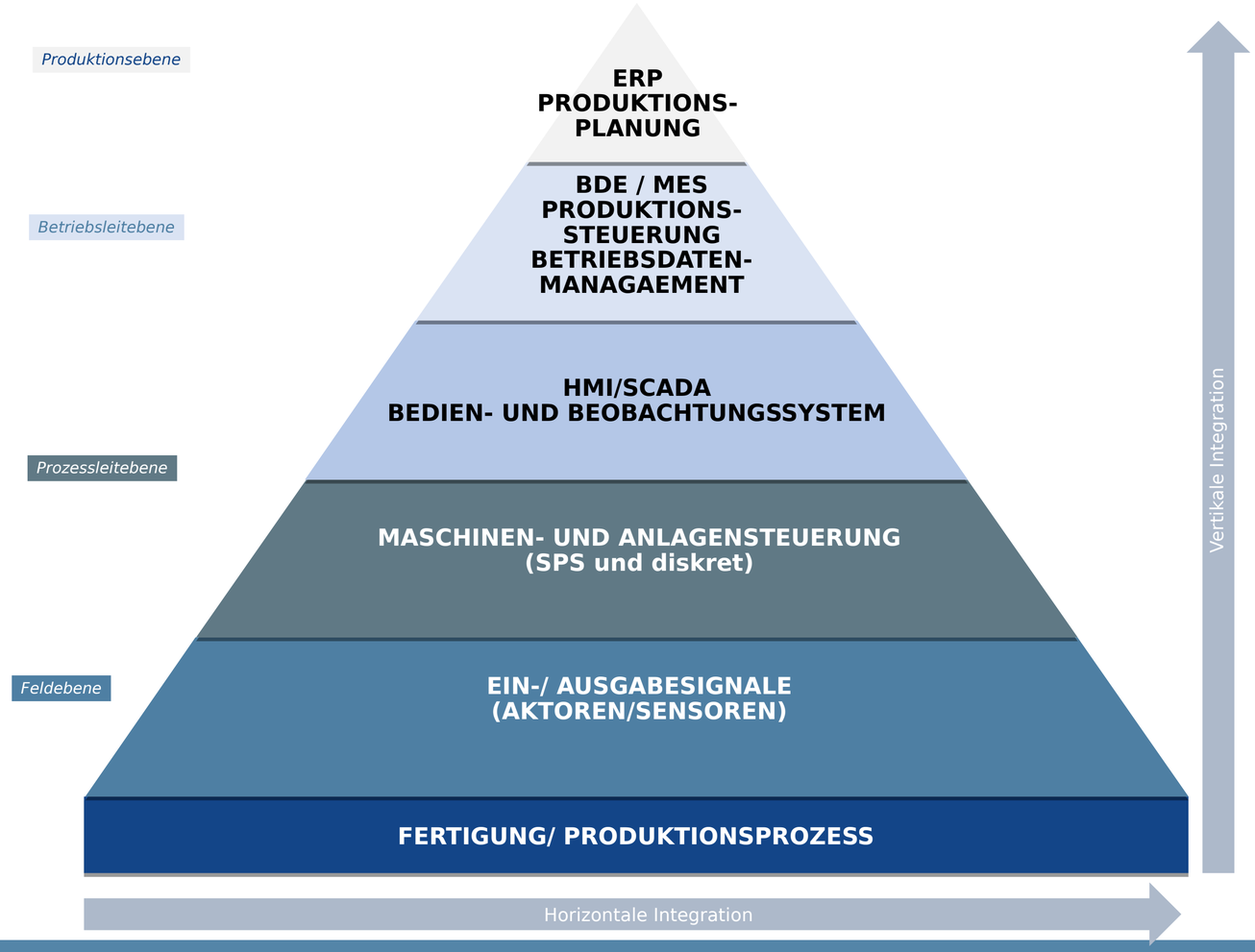
INDUSTRIE 4.0 – Horizontale und Vertikale Integration

Horizontale Integration:

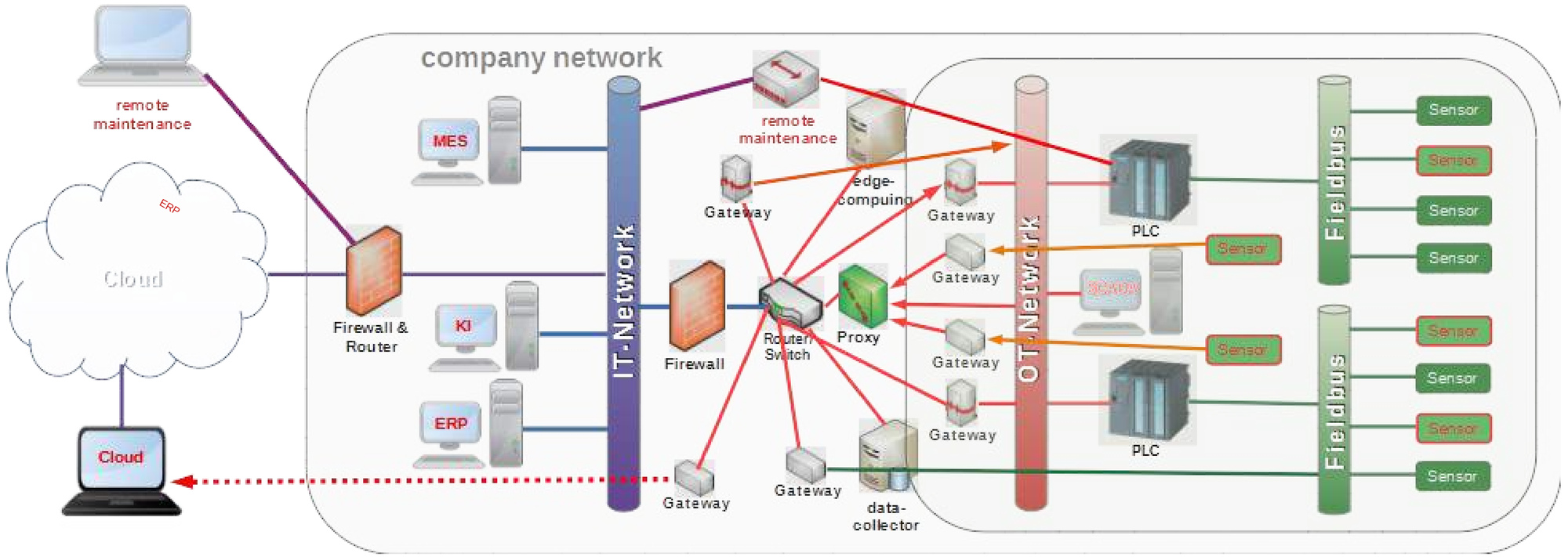
- Vernetzung zwischen Produktionsstätten
- (Einbindung des Kunden in die Prozesse)
- Informationsaustausch während des gesamten Wertschöpfungsprozesses
- Intelligente Systemkommunikation im Bereich Bedarf, Produktion und Logistik

Vertikale Integration:

- Vernetzung innerhalb des Unternehmens von der Produktionsebene bis hin zur Feldebene
- IT-Systeme kommunizieren auf allen Ebenen

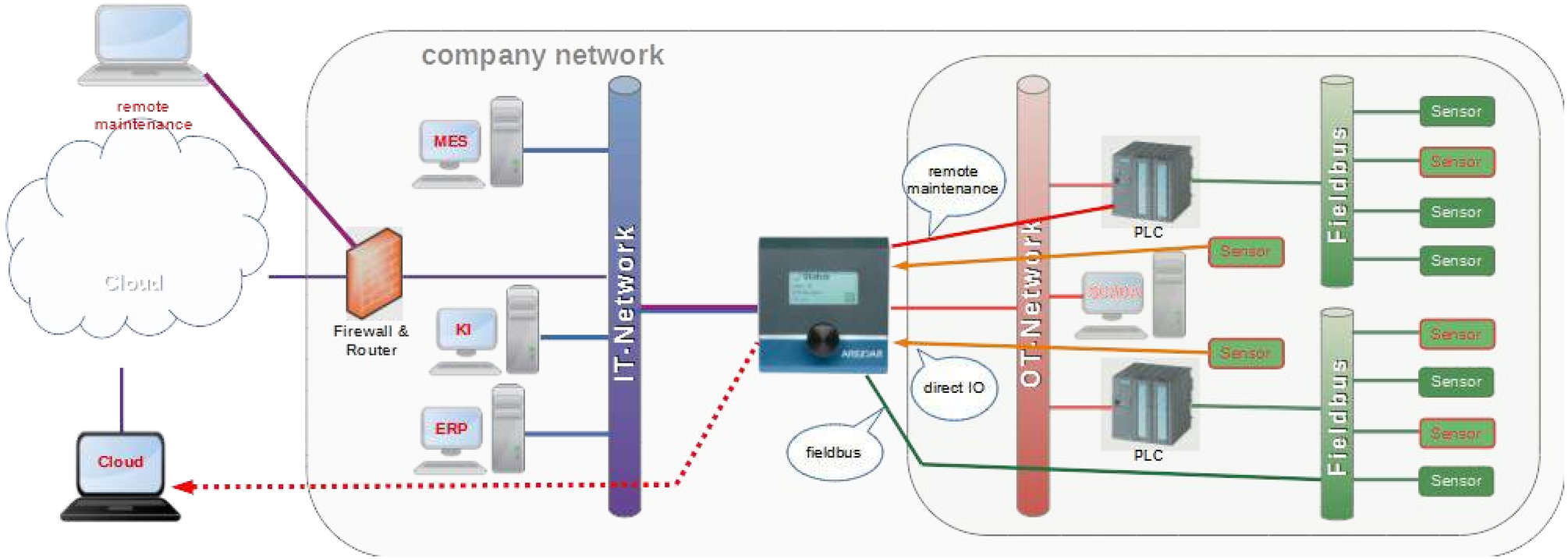


Umsetzung: Konnektivität bedeutet oftmals Komplexität



Heterogene Architektur:
Komplex, Fehleranfällig, diverse Angriffspunkte, anspruchsvoll

Komplexität verbergen – Daten standardisieren – Sicherheit verbessern



ARENDAR:

Firewall, Proxy, Gateway, Remote control, safe inter-process communication, Cloud connectivity, Visualization, Cyber Security …

 Einheitliche Datenlagen, cyber-sichere Lösung

Auch EEG-Anlagen benötigen SCADA!

Die Abkürzung SCADA steht für Supervisory Control and Data Acquisition und beschreibt die grundlegenden Funktionen eines SCADA-Systems.

SEIT ANGRIFF AUF DIE UKRAINE

Fernsteuerung von Tausenden Windkraftanlagen gestört

AKTUALISIERT AM 02.03.2022 - 13:05

Wegen einer gestörten Satellitenverbindung können Tausende Windräder aktuell nicht ferngesteuert werden. Das Problem könnte mit der russischen Invasion in der Ukraine zusammenhängen.

Sind wir überrascht?

Vendor	Product	Vulnerability Class	Service	Severity
Harris	 RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	 9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	 ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	 EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	 SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	 AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	 SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	 SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	 JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	 PilotOpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

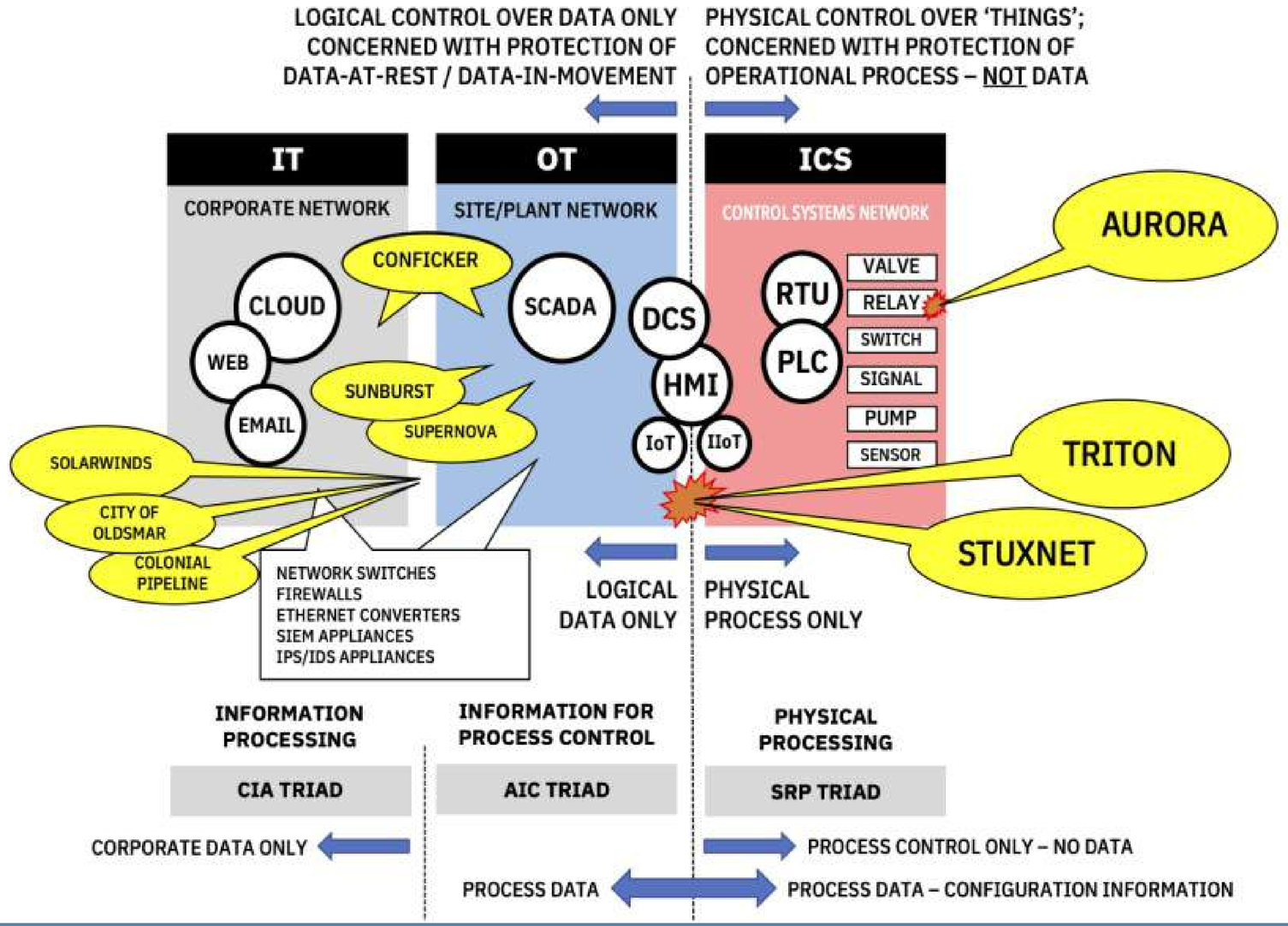
2014 - A Wake-Up call for SATCOM Security

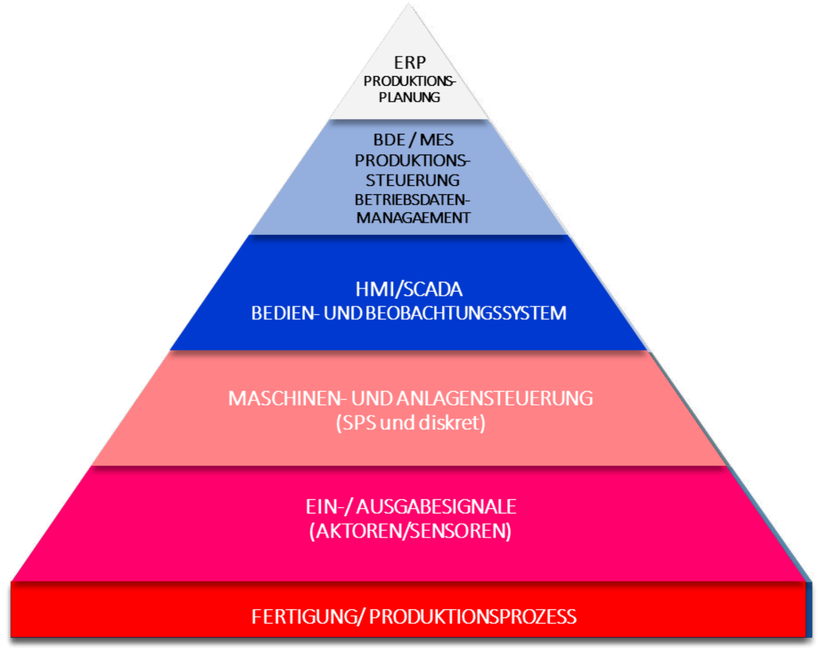
Industry	Threat
Aviation	• Ability to disrupt, intercept or modify non-safety communications such as In-Flight WiFi * • Ability to attack crew and passenger's devices • Ability to manipulate SATCOM antenna positioning and transmissions.
Maritime	• Ability to disrupt, intercept or modify onboard satellite communications • Ability to attack crew's devices • Ability to control SATCOM antenna positioning and transmissions • Ability to perform cyber-physical attacks using HIRF
Military	• Ability to pinpoint the location of military units • Ability to disrupt, intercept or modify satellite communications • Ability to perform cyber-physical attacks using HIRF
Space	• Ability to disrupt satellite transponders

2018 - Last Call for SATCOM Security

https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html

Das Problem: IT und OT „under Fire“!

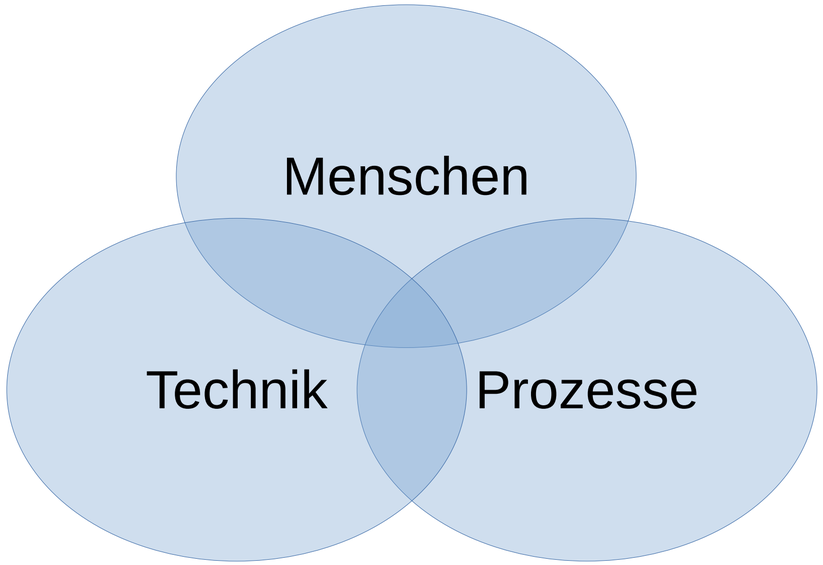


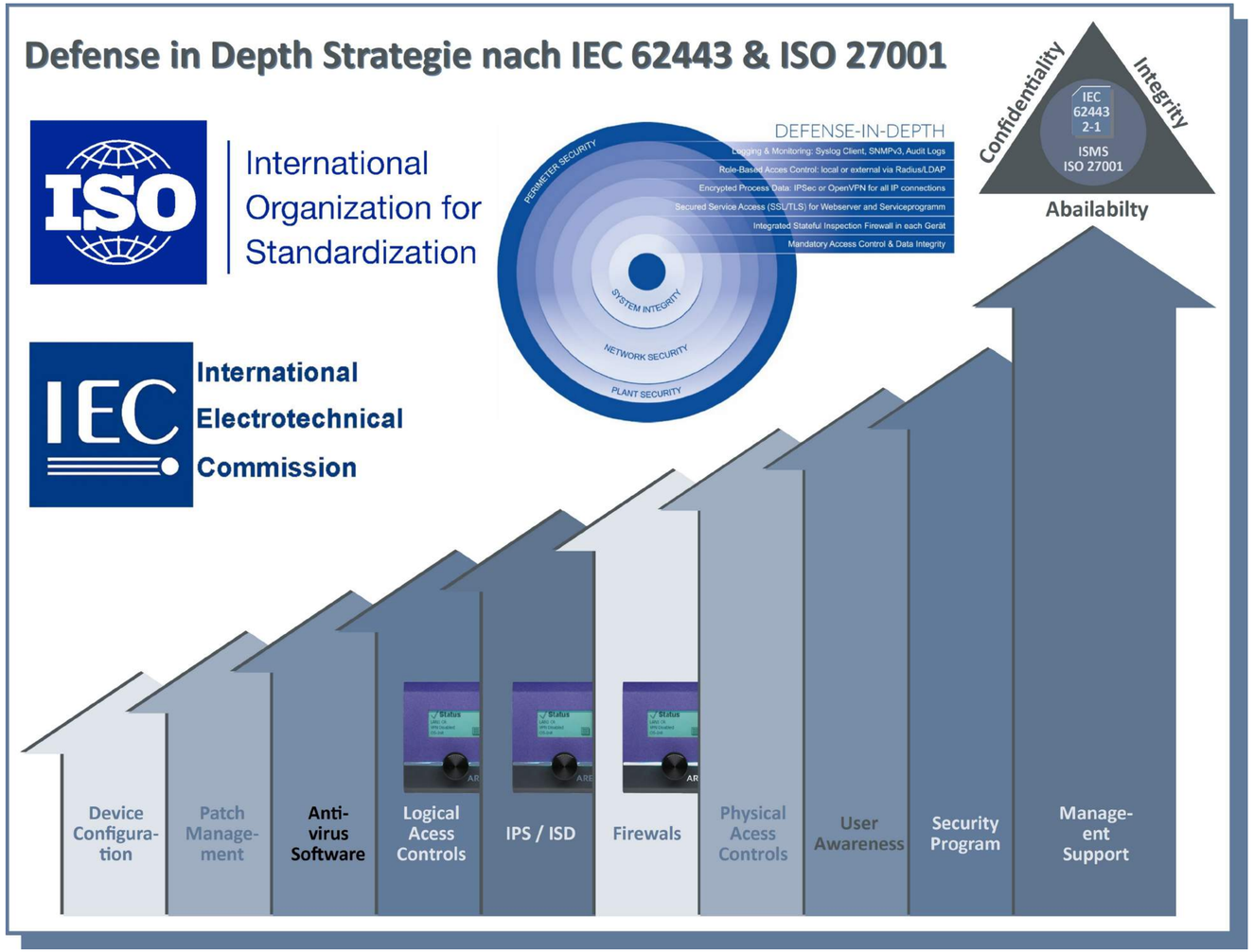


infracritical
Rev. 3 - 16-Jan-2022

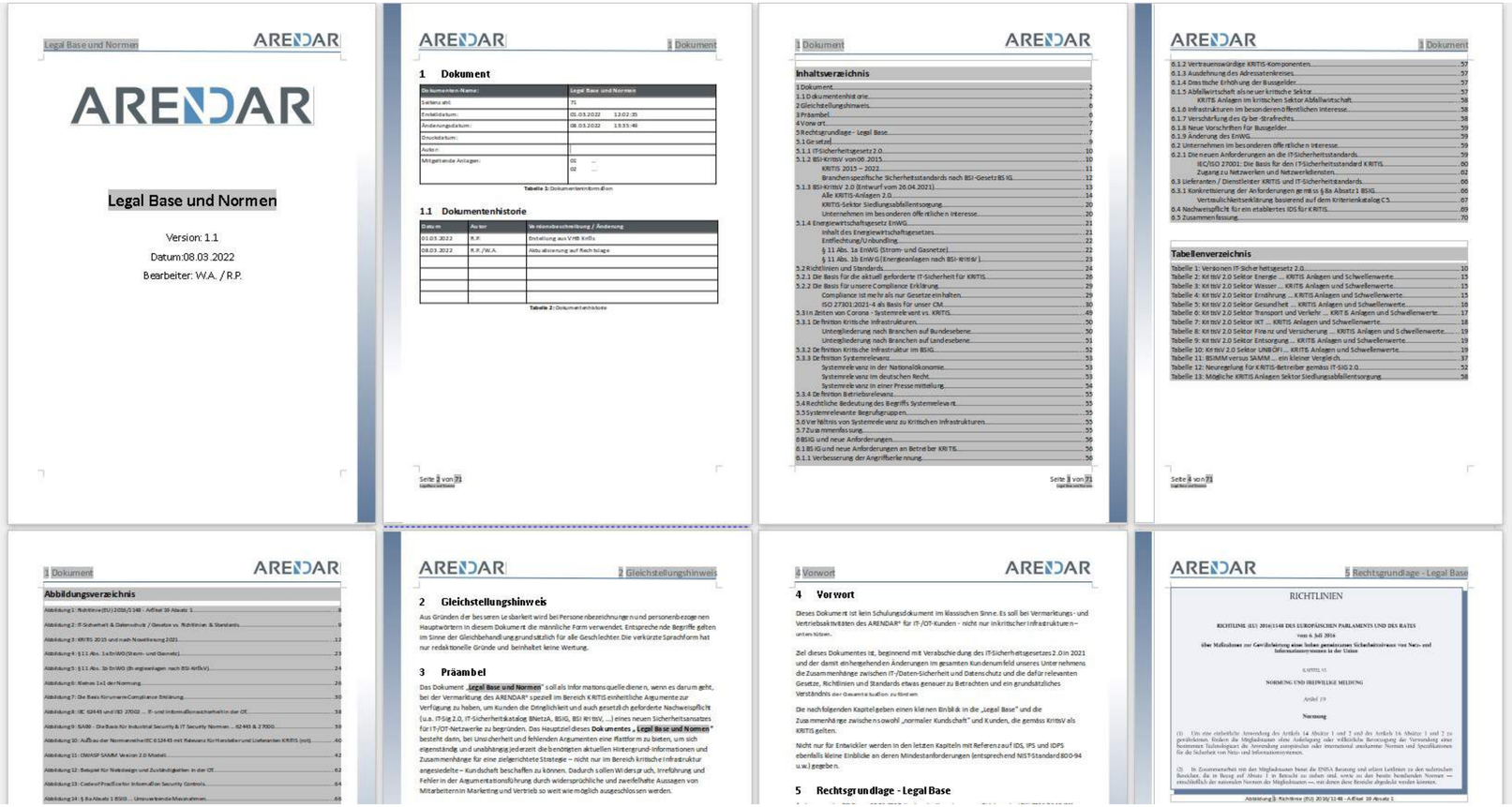
Ziele Faktoren Methoden

- Sicherheit
- Funktionserhalt
- Verfügbarkeit
- Integrität
- Vertraulichkeit





An Normen und Vorgaben besteht kein Mangel!



„Auditoren haben die Normen unterschiedlich interpretiert. Es kommt darauf an die Industrie zu verändern!“

(Frei nach einem weißhaarigen bärtigen Trierer)

Warum SAMM?

Sichere Software bedarf eines definierten Prozesses der Software Entwicklung.

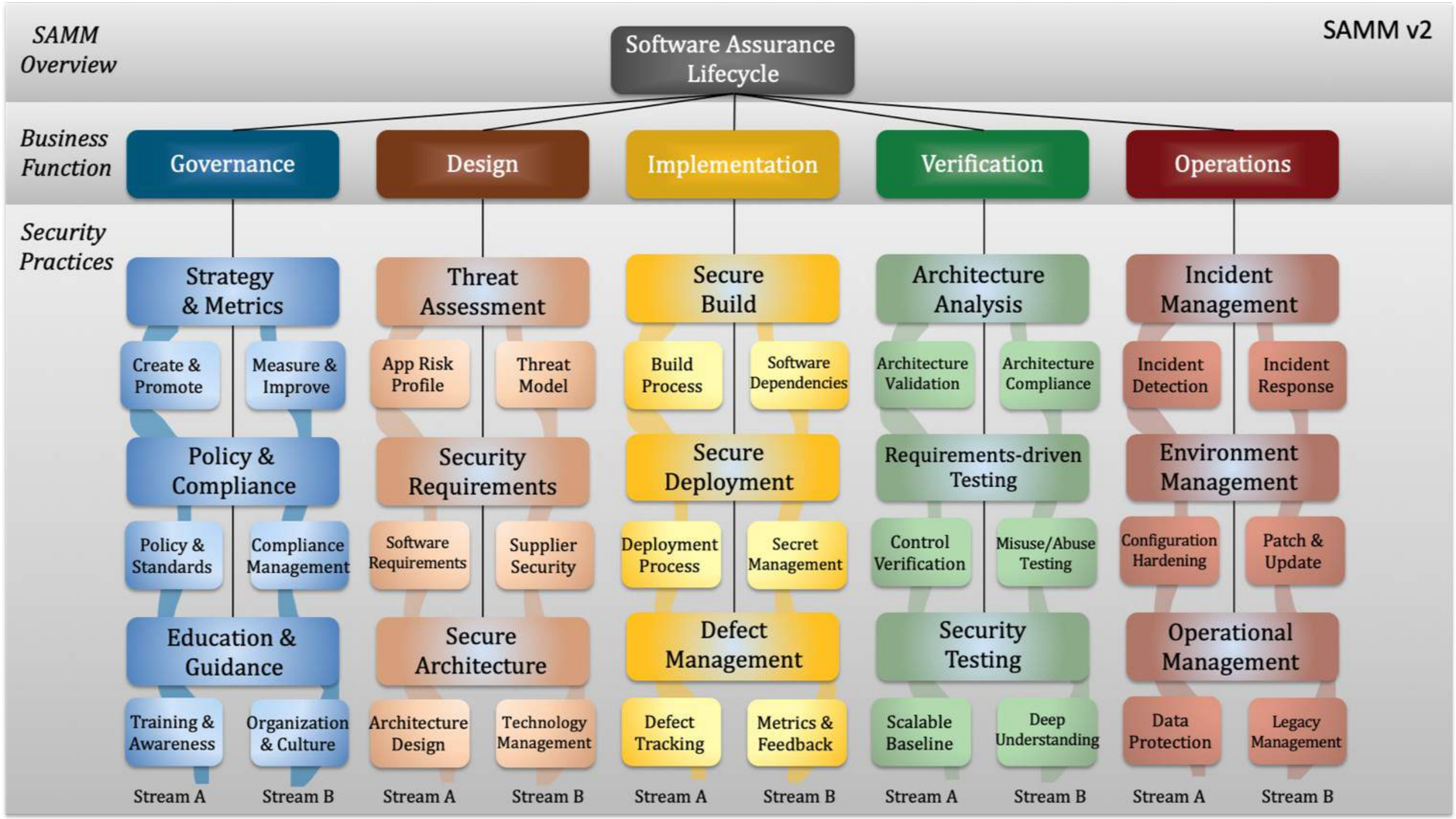
Das Open Web Application Security Project (OWASP) hat hierfür mit dem Software Assurance Maturity Model (OWASP SAMM) ein wertvolles Rahmenwerk geschaffen.

Was ist SAMM?

Die derzeit aktuelle Version OWASP SAMM v2 definiert insgesamt 30 Security-Aktivitäten für die Kernbereiche Governance, Design, Implementierung, Verification und Operations.

Basierend auf einem detaillierten Fragenkatalog können Unternehmen damit ihren individuellen Reifegrad nicht nur pro Einzelaktivität, sondern auch aggregiert auf die jeweiligen Bereiche sowie den gesamten Entwicklungsprozess ermitteln.

Was ist SAMM?


SAMM Overview
SAMM v2
Software Assurance Lifecycle
Business Function
Governance
Design
Implementation
Verification
Operations
Security Practices
Strategy & Metrics
Create & Promote
Measure & Improve
Policy & Compliance
Policy & Standards
Compliance Management
Education & Guidance
Training & Awareness
Organization & Culture
Threat Assessment
App Risk Profile
Threat Model
Security Requirements
Software Requirements
Supplier Security
Secure Architecture
Architecture Design
Technology Management
Secure Build
Build Process
Software Dependencies
Secure Deployment
Deployment Process
Secret Management
Defect Management
Defect Tracking
Metrics & Feedback
Architecture Analysis
Architecture Validation
Architecture Compliance
Requirements-driven Testing
Control Verification
Misuse/Abuse Testing
Security Testing
Scalable Baseline
Deep Understanding
Incident Management
Incident Detection
Incident Response
Environment Management
Configuration Hardening
Patch & Update
Operational Management
Data Protection
Legacy Management
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B
Stream A
Stream B

These zu SAMM

Arendar hat von Anfang an auf einen definierten Prozesses der Software Entwicklung gesetzt.

SAMM ist ein Werkzeug, um zu beweisen, daß Arendar auf dem richtigen Weg ist!

Erser Schritt: SAMM Assessment

Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

Organization:	
Team/Application:	
Interview Date:	
Team Lead:	
Contributors:	

Governance					
Stream	Level	Strategy & Metrics	Answer	Interview Notes	Rating
Create and Promote	1	Do you understand the enterprise-wide risk appetite for your applications ?	opportunities		1,13
		You capture the risk appetite of your organization's executive leadership The organization's leadership vet and approve the set of risks You identify the main business and technical threats to your assets and data You document risks and store them in an accessible location			
	2	Do you have a strategic plan for application security and use it to make decisions?	Yes, we consult the plan before making significant decisions		
		The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget The plan is consistent with the organization's business drivers and risks The plan lays out a roadmap for strategic and tactical initiatives You have buy-in from stakeholders, including development teams			
	3	Do you regularly review and update the Strategic Plan for Application Security?	Yes, but review is ad-hoc		
		You review and update the plan in response to significant changes in the business environment, the organization, or its risk appetite Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies You adjust the plan and roadmap based on lessons learned from completed roadmap activities You publish progress information on roadmap activities, making sure they are available to all stakeholders			
Measure and Improve	1	Do you use a set of metrics to measure the effectiveness and efficiency of the application security program across applications?	Yes, for two metrics categories		
		You document each metric, including a description of the sources, measurement coverage, and guidance on how to use it to explain application security trends Metrics include measures of efforts, results, and the environment measurement categories Most of the metrics are frequently measured, easy or inexpensive to gather, and expressed as a cardinal number or a percentage Application security and development teams publish metrics			
	2	Did you define Key Perfomance Indicators (KPI) from available application security metrics?	Yes, for some of the metrics		
		You defined KPIs after gathering enough information to establish realistic objectives You developed KPIs with the buy-in from the leadership and teams responsible for application security KPIs are available to the application teams and include acceptability thresholds and guidance in case teams need to take action Success of the application security program is clearly visible based on defined KPIs			
	3	Do you update the Application Security strategy and roadmap based on application security metrics and KPIs?	Yes, but review is ad-hoc		
		You review KPIs at least yearly for their efficiency and effectiveness KPIs and application security metrics trigger most of the changes to the application security strategy			
		Policy & Compliance	Answer	Interview Notes	Rating
Policy & Standards	1	Do you have and apply a common set of policies and standards throughout your organization?	Yes, for most or all of the applications		1,88
		You have adapted existing standards appropriate for the organization's industry to account for domain-specific considerations Your standards are aligned with your policies and incorporate technology-specific implementation guidance			
	2	Do you publish the organization's policies as test scripts or run-books for easy interpretation by development	Yes, most or all of the content		
		You create verification checklists and test scripts where applicable, aligned with the policy's requirements and the implementation guidance in the associated standards You create versions adapted to each development methodology and technology the organization uses			
	3	Do you regularly report on policy and standard compliance, and use that information to guide compliance improvement efforts?	Yes, but reporting is ad-hoc		

SAMM Assessment

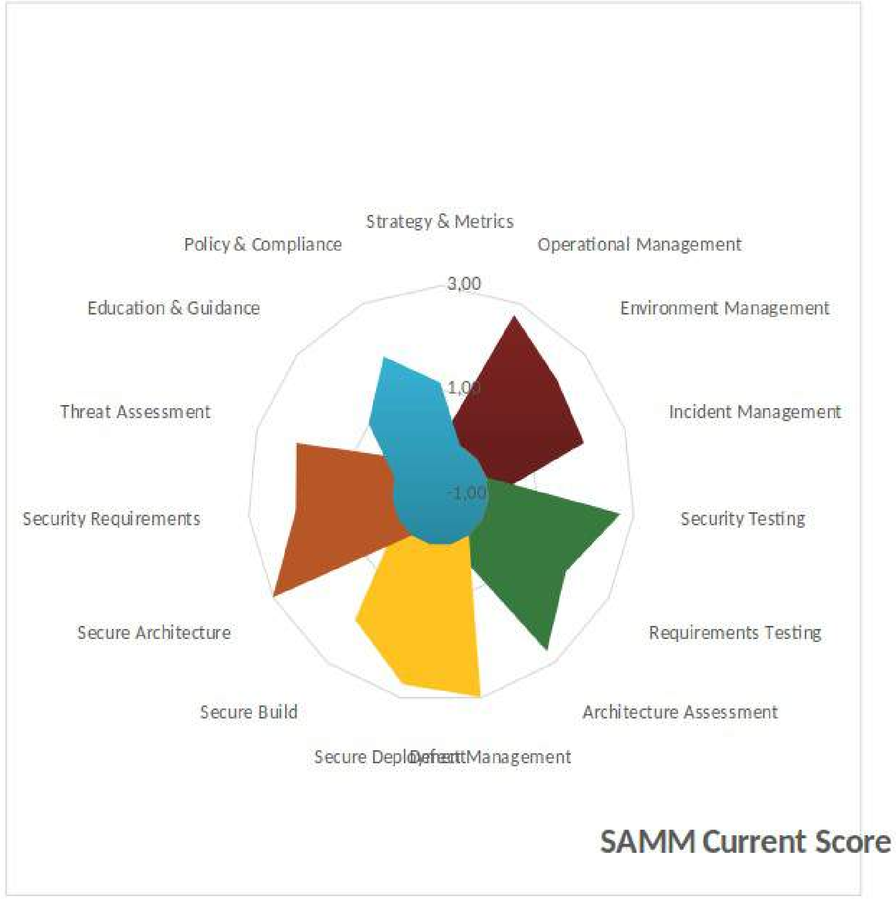
ARENDAR

Current Maturity Score

Business Functions	Security Practices	Current	Maturity 1	2	3
Governance	Strategy & Metrics	1,13	0,75	0,13	0,25
Governance	Policy & Compliance	1,88	1,00	0,63	0,25
Governance	Education & Guidance	1,00	0,38	0,13	0,50
Design	Threat Assessment	2,13	1,00	0,75	0,38
Design	Security Requirements	2,00	0,63	0,75	0,63
Design	Secure Architecture	3,00	1,00	1,00	1,00
Implementation	Secure Build	2,00	0,63	0,63	0,75
Implementation	Secure Deployment	2,75	1,00	1,00	0,75
Implementation	Defect Management	3,00	1,00	1,00	1,00
Verification	Architecture Assessment	2,75	1,00	0,75	1,00
Verification	Requirements Testing	2,00	0,50	0,75	0,75
Verification	Security Testing	2,75	0,75	1,00	1,00
Operations	Incident Management	2,13	1,00	0,13	1,00
Operations	Environment Management	2,25	0,50	1,00	0,75
Operations	Operational Management	2,75	1,00	0,75	1,00

Business Functions	Current
Governance	1,33
Design	2,38
Implementation	2,58
Verification	2,50
Operations	2,38

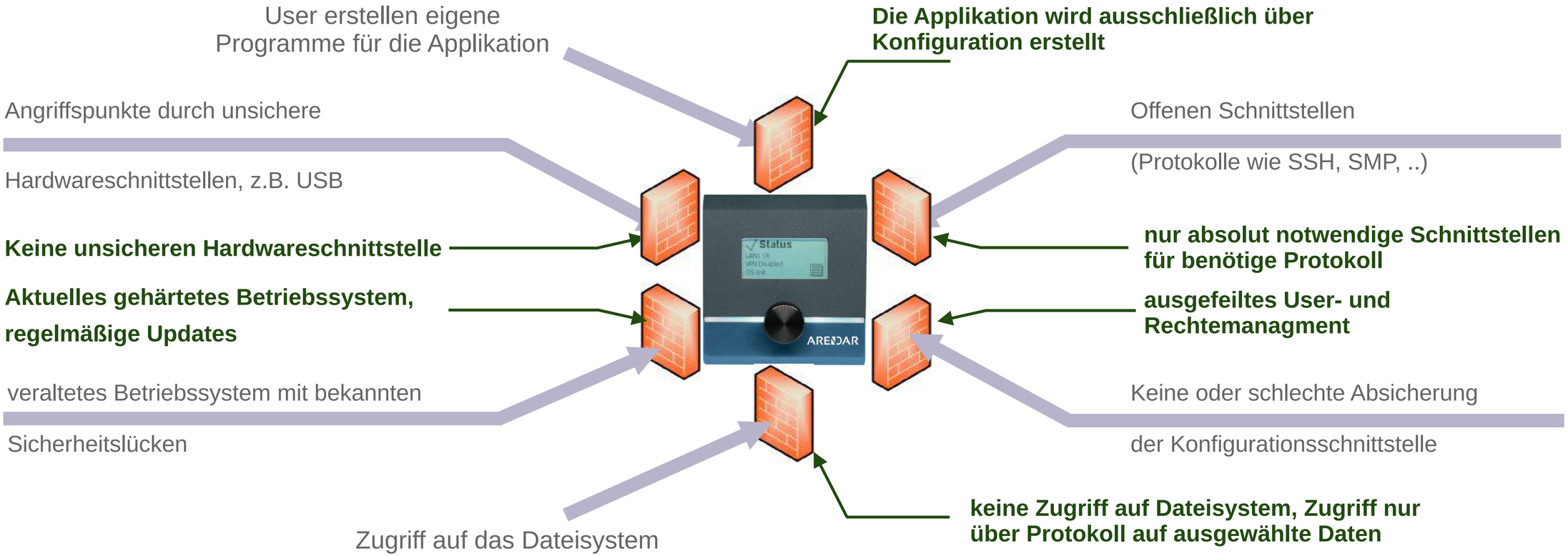
Current Maturity Score



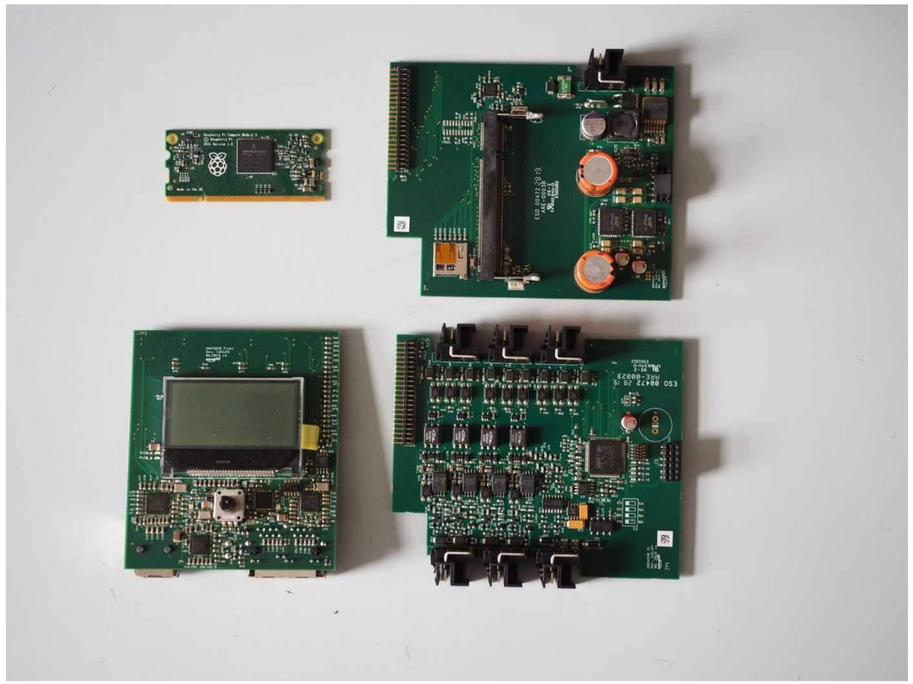
eco VERBAND DER INTERNETWIRTSCHAFT

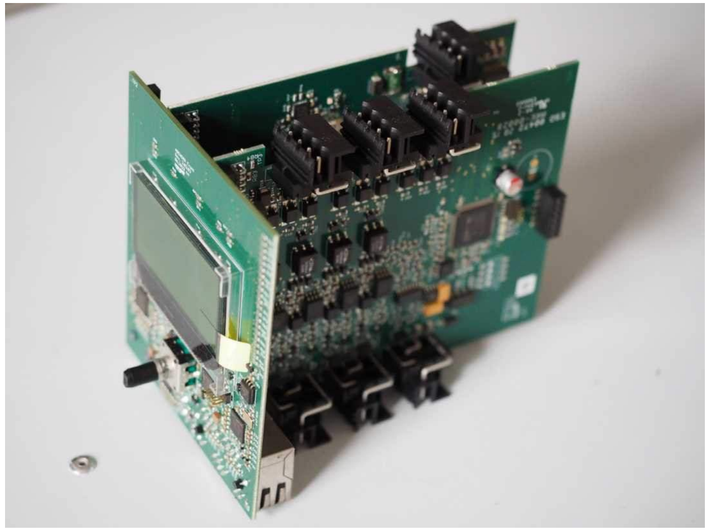
Was macht der ARENDAR anders

Angriff Abwehr durch „**Security by Design**“ in Hard- und Software



Design-Entscheidung für eigene Hardware:





Made in Germany
Made in Rheinland-Pfalz

Kontakt

Rudolf Preuß
Geschäftsführender
Gesellschafter

Arendar IT-Security GmbH
Am Kleinen Rotenberg 21
54516 Wittlich

Email:
rudolf.preuss@arendar.io
Tel.: 06571 / 95579-299
Fax: 06571 / 95579-28

Homepage: www.arendar.eu