# Pen-testing Medical Devices and IVDs

for compliance and security

Regulatory Summit 2026, 2026-03-12

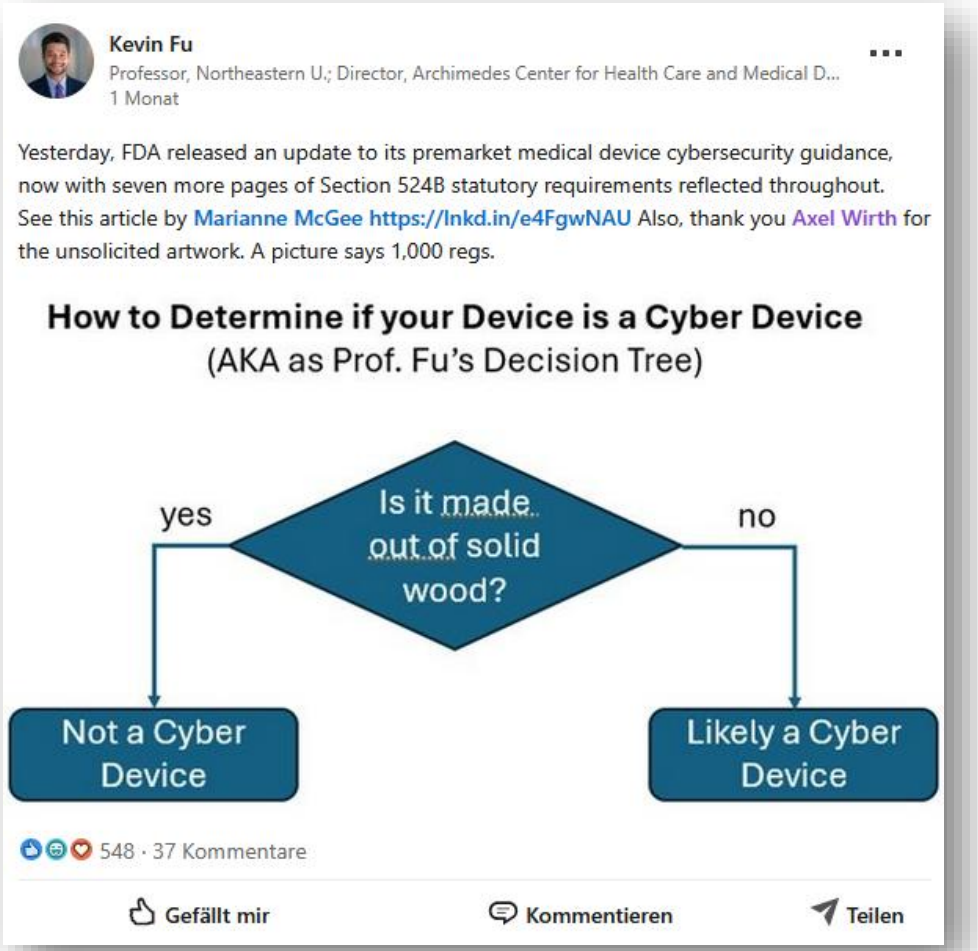
Add value.
Inspire trust.

# Jan Kufner

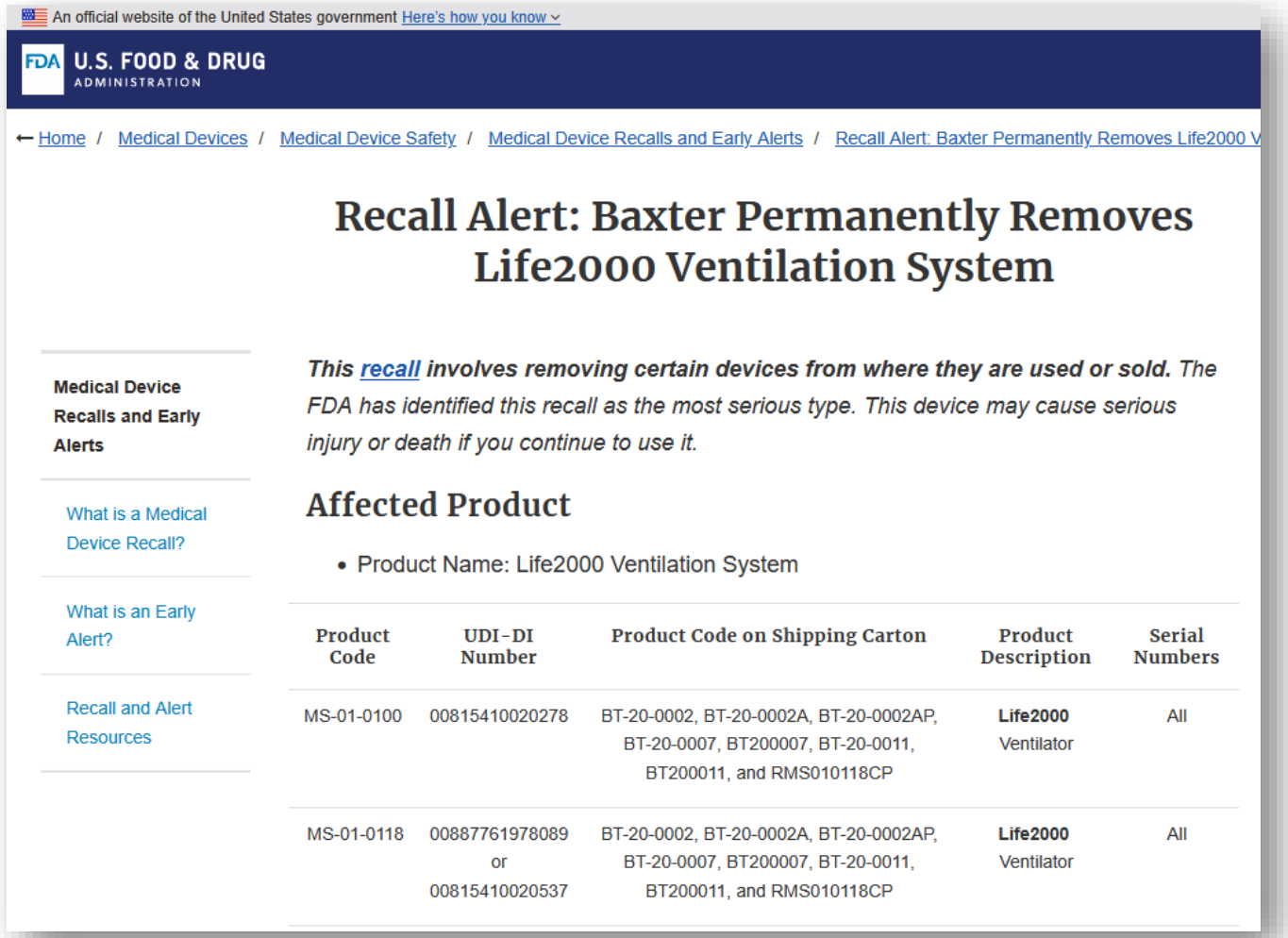
- Team Leader, European Medical Device & IVD Pen-Testing Lab at TÜV SÜD
- Leads a multinational team in Munich, still active in hands-on testing
- Former Cybersecurity Lead at TÜV SÜD's Notified Body with strong regulatory expertise
- Combines technical + regulatory insight in cybersecurity & medical device innovation

# Regulatory Update

# How to Determine if your Device is a Cyber Device




https://www.linkedin.com/posts/drkevinfu_yesterday-fda-released-an-update-to-its-activity-7344470096779657216-Mnpv



An official website of the United States government Here's how you know

FDA U.S. FOOD & DRUG ADMINISTRATION

← Home / Medical Devices / Medical Device Safety / Medical Device Recalls and Early Alerts / Recall Alert: Baxter Permanently Removes Life2000 V

# Recall Alert: Baxter Permanently Removes Life2000 Ventilation System

**Medical Device Recalls and Early Alerts**

What is a Medical Device Recall?

What is an Early Alert?

Recall and Alert Resources

***This recall involves removing certain devices from where they are used or sold.*** *The FDA has identified this recall as the most serious type. This device may cause serious injury or death if you continue to use it.*

## Affected Product

- Product Name: Life2000 Ventilation System

| Product Code | UDI-DI Number | Product Code on Shipping Carton | Product Description | Serial Numbers |
|---|---|---|---|---|
| MS-01-0100 | 00815410020278 | BT-20-0002, BT-20-0002A, BT-20-0002AP, BT-20-0007, BT200007, BT-20-0011, BT200011, and RMS010118CP | **Life2000** Ventilator | All |
| MS-01-0118 | 00887761978089 or 00815410020537 | BT-20-0002, BT-20-0002A, BT-20-0002AP, BT-20-0007, BT200007, BT-20-0011, BT200011, and RMS010118CP | **Life2000** Ventilator | All |

https://www.fda.gov/medical-devices/medical-device-recalls-and-early-alerts/recall-alert-baxter-permanently-removes-life2000-ventilation-system?utm_medium=email&utm_source=govdelivery

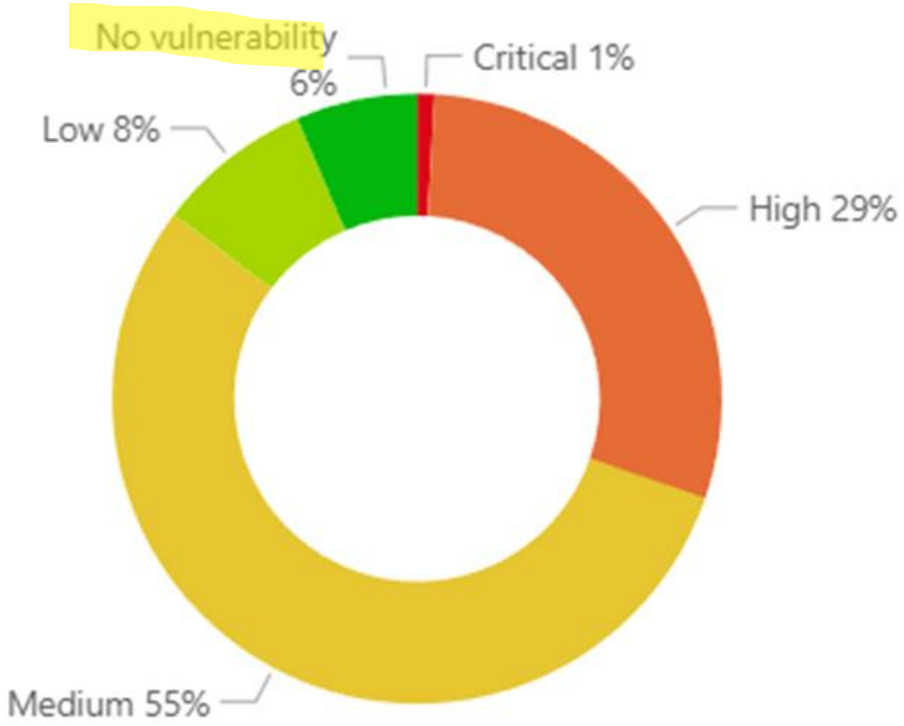
# SOTA

- 81001-5-1 mandatory (although not harmonized | consensus standard)
- 60601-4-5 guidance (if you must use it as a list for security requirements)
  - configurable password strength
  - X.509-based PKI
  - … tate of Cyber Security
- Cyber Resilience Act (CRA) not applicable for medical devices

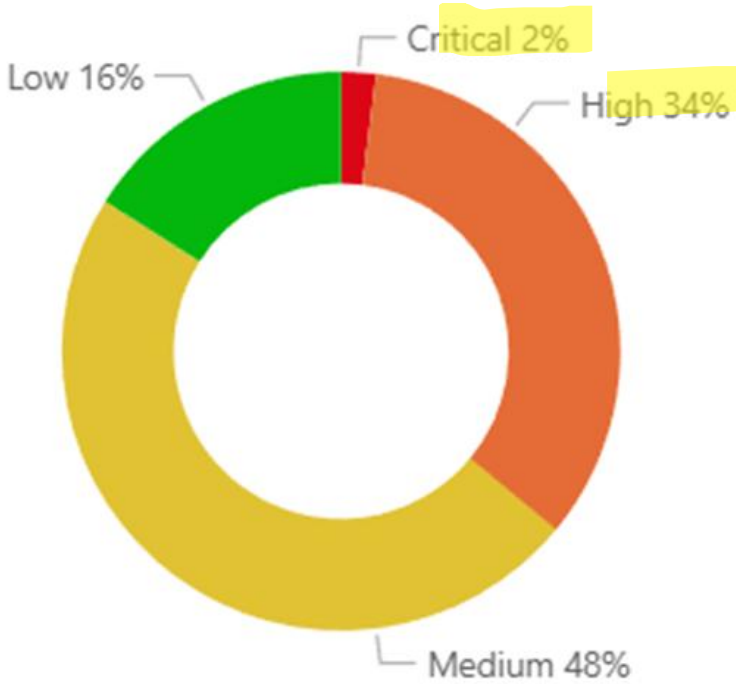
# State of Cyber Security

## Cybersecurity Testing of Software in Unannounced audits (n = 41)

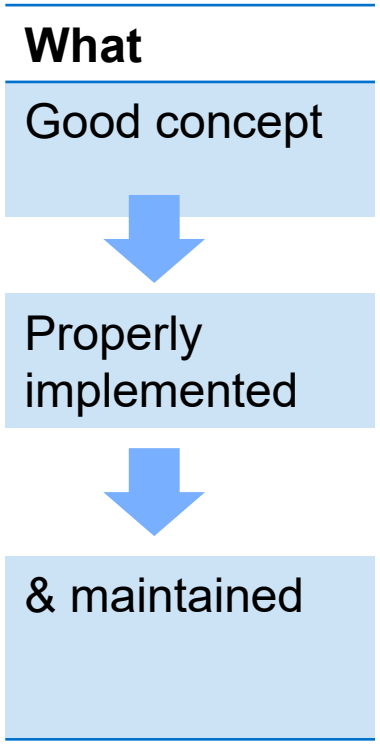
### Identified vulnerabilities




### Patient Saftey Risk of identified vulnerabilites



# NBs & FDA`s view



# NBs & FDA`s view

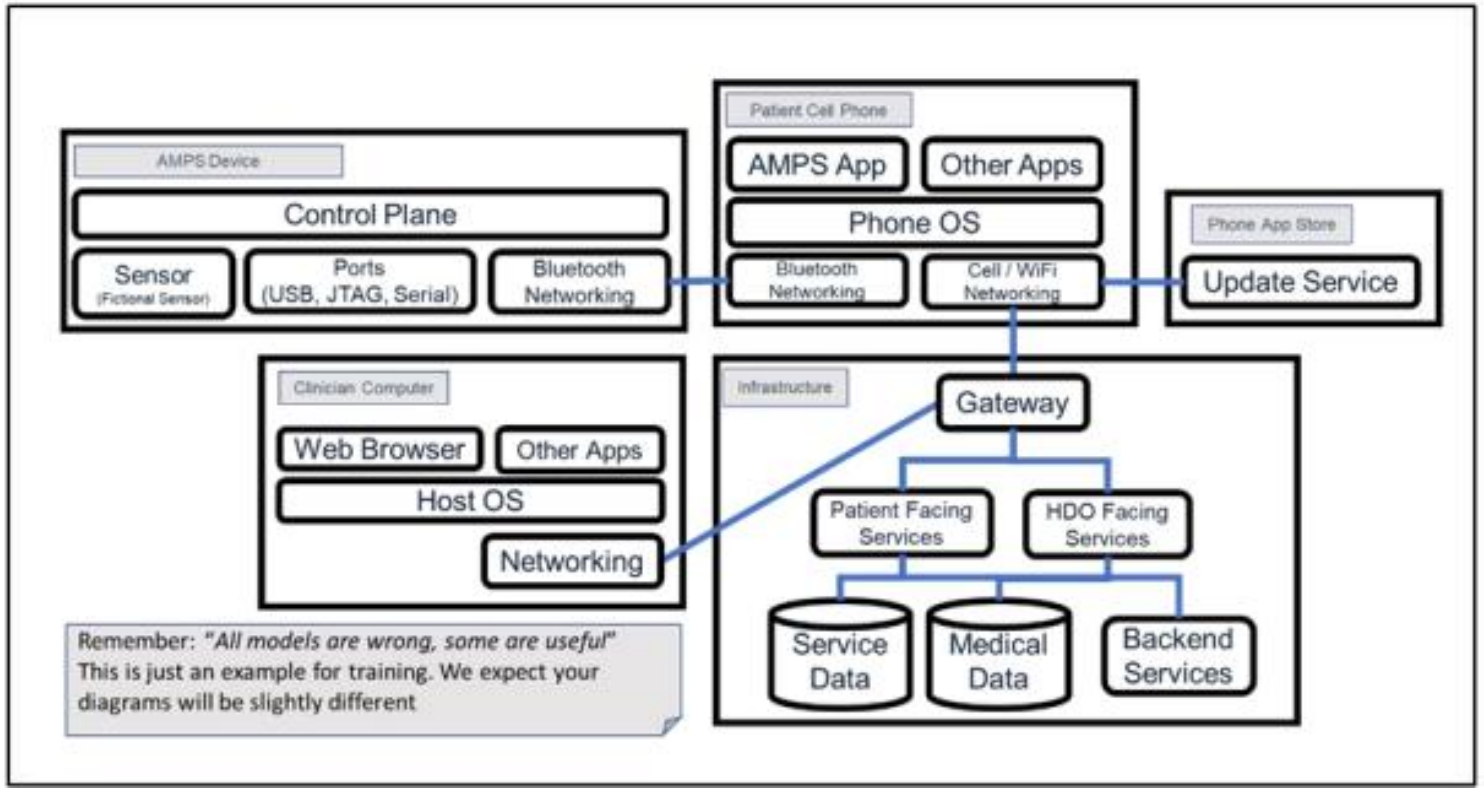
| What | How |
|---|---|
| Good concept | Laid out in the security Risk Management (STRIDE) |
| Properly implemented | Verified via pen-test |
| & maintained | done via patch management |

# Security Concept

# Pitfalls for market authorization the security concept

1. Missing (data flow diagram)
2. Bad concept
3. Bad documentation (tip: use STRIDE)

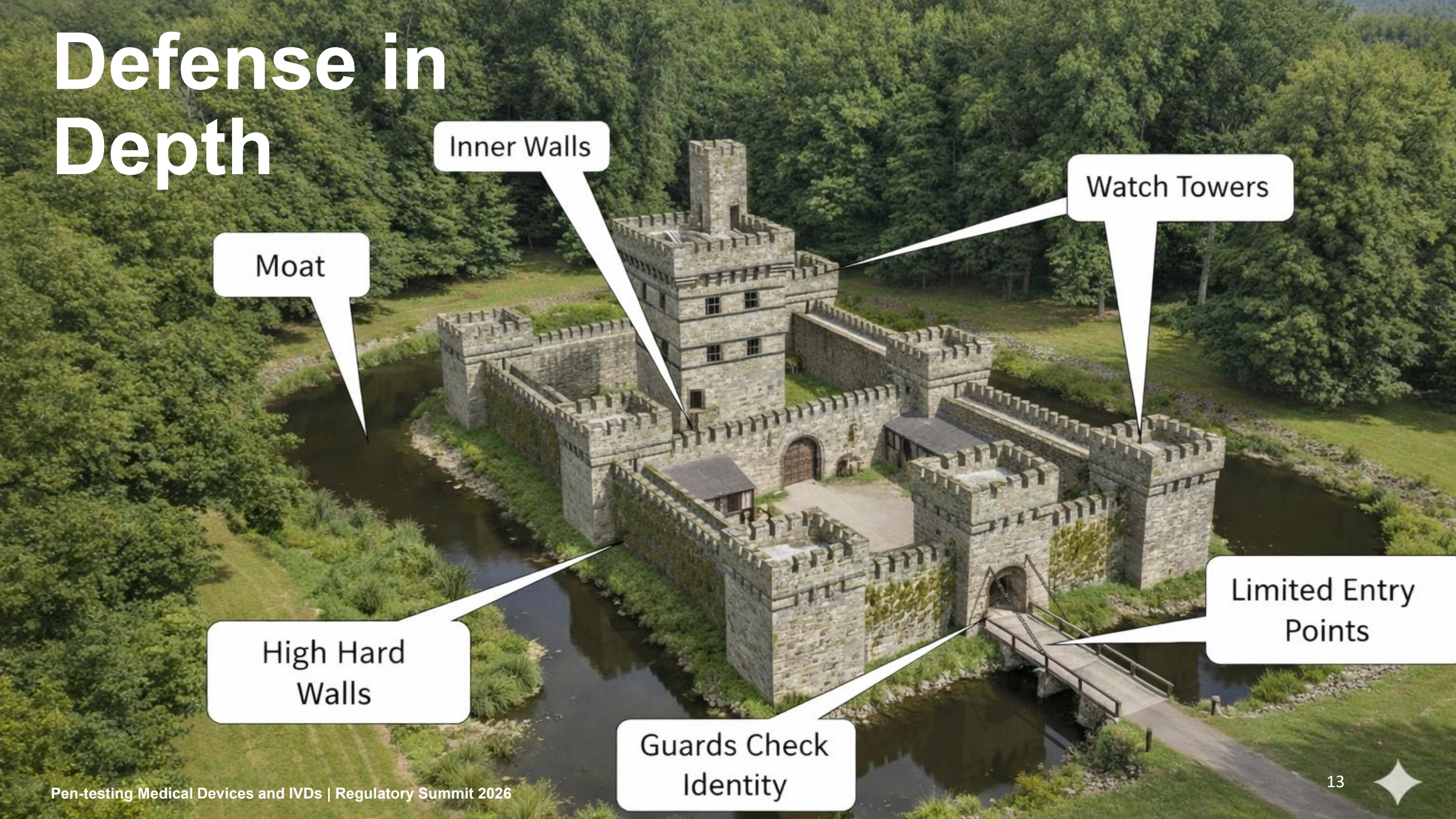
# Data Flow Diagram




| Element | Symbol | Discussion |
|---|---|---|
| External Entity | | **Object:** A sharp-cornered rectangle. **Represents:** Anything outside your control. Examples include people and systems run by other organizations or even divisions. |
| Process | | **Object:** A rounded rectangle. **Represents:** Any running code, including compiled, scripts, shell commands, Structured Query Language (SQL) stored procedures, et cetera. |
| Data Store | | **Object:** A drum. **Represents:** Anywhere data is stored, including files, databases, shared memory, cloud storage services, cookies, et cetera. |
| Data Flows | | **Object:** A double-headed arrow. **Represents:** All the ways that processes can talk to data stores or each other. If a conversation is only initiated by one side, you can represent the initiating side as an empty arrow. |
| Trust Boundary | | **Object:** A closed shape drawn with a dashed or dotted line. **Represents:** A way to display different trust levels between objects. |

https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf

# Defense in Depth



# Defence in depth (example WebApp)

| | |
|---|---|
| **Network / Transport Layer** | • TLS 1.3 with HSTS, no insecure ciphers<br>• DDoS protection, traffic filtering & rate limiting<br>• … |
| **Authentication & Access Control** | • Strong authentication (password policy, OAuth2, OIDC)<br>• Multi-factor authentication (2FA/MFA)<br>• … |
| **Application Layer Security** | • Input validation & output encoding (prevent XSS, injection)<br>• CSRF protection (tokens, sameSite)<br>• … |
| **Data Protection** | • Encryption of sensitive data at rest (DB/disk encryption)<br>• Hashing passwords with modern algorithms (bcrypt, Argon2)<br>• … |
| **Monitoring & Detection** | • Intrusion detection (IDS/IPS, SIEM integration)<br>• … |
| **Operational Security** | • Continuous updates & patching (app, OS, middleware)<br>• Regular pen-testing<br>• … |

# Penetration Testing

# CVSS vs ISO severity

- **Guest account can change all medication at hospital CVSS v3.1 Vector** AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N **4,3**

## Base Score Metrics

### Exploitability Metrics

**Attack Vector (AV)***

| Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P) |
|---|---|---|---|

**Attack Complexity (AC)***

| Low (AC:L) | High (AC:H) |
|---|---|

**Privileges Required (PR)***

| None (PR:N) | Low (PR:L) | High (PR:H) |
|---|---|---|

**User Interaction (UI)***

| None (UI:N) | Required (UI:R) |
|---|---|

**Scope (S)***

| Unchanged (S:U) | Changed (S:C) |
|---|---|

### Impact Metrics

**Confidentiality Impact (C)***

| None (C:N) | Low (C:L) | High (C:H) |
|---|---|---|

**Integrity Impact (I)***

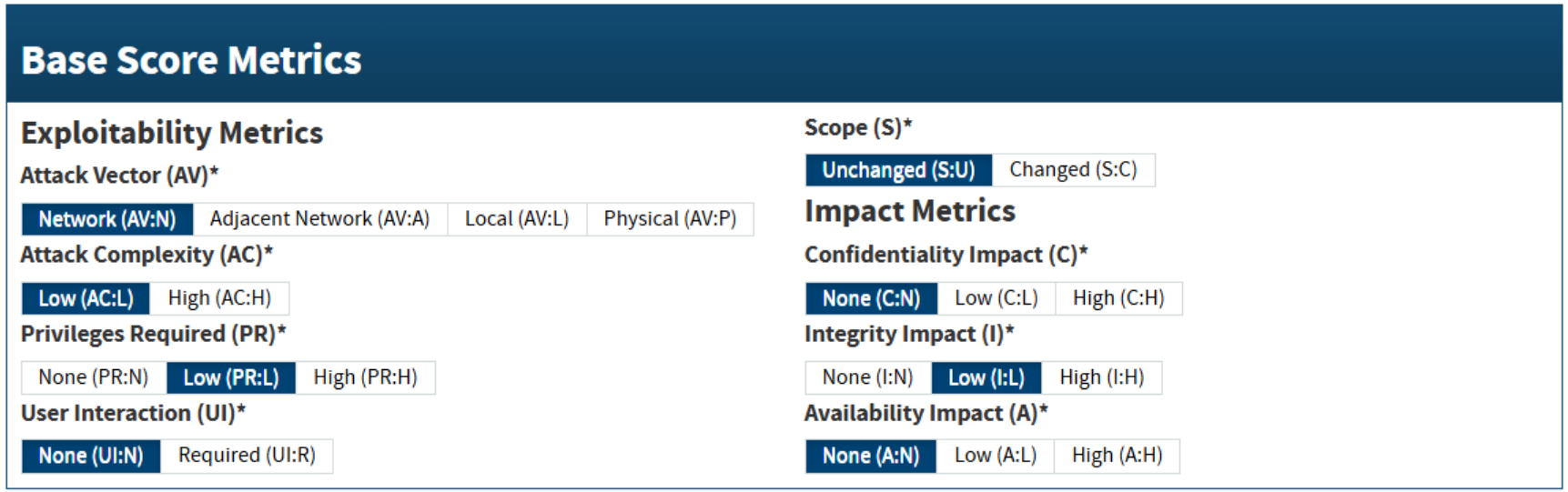
| None (I:N) | Low (I:L) | High (I:H) |
|---|---|---|

**Availability Impact (A)***

| None (A:N) | Low (A:L) | High (A:H) |
|---|---|---|

# CVSS vs ISO severity

- **Guest account can change all medication at hospital CVSS v3.1 Vector** AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N **4,3**



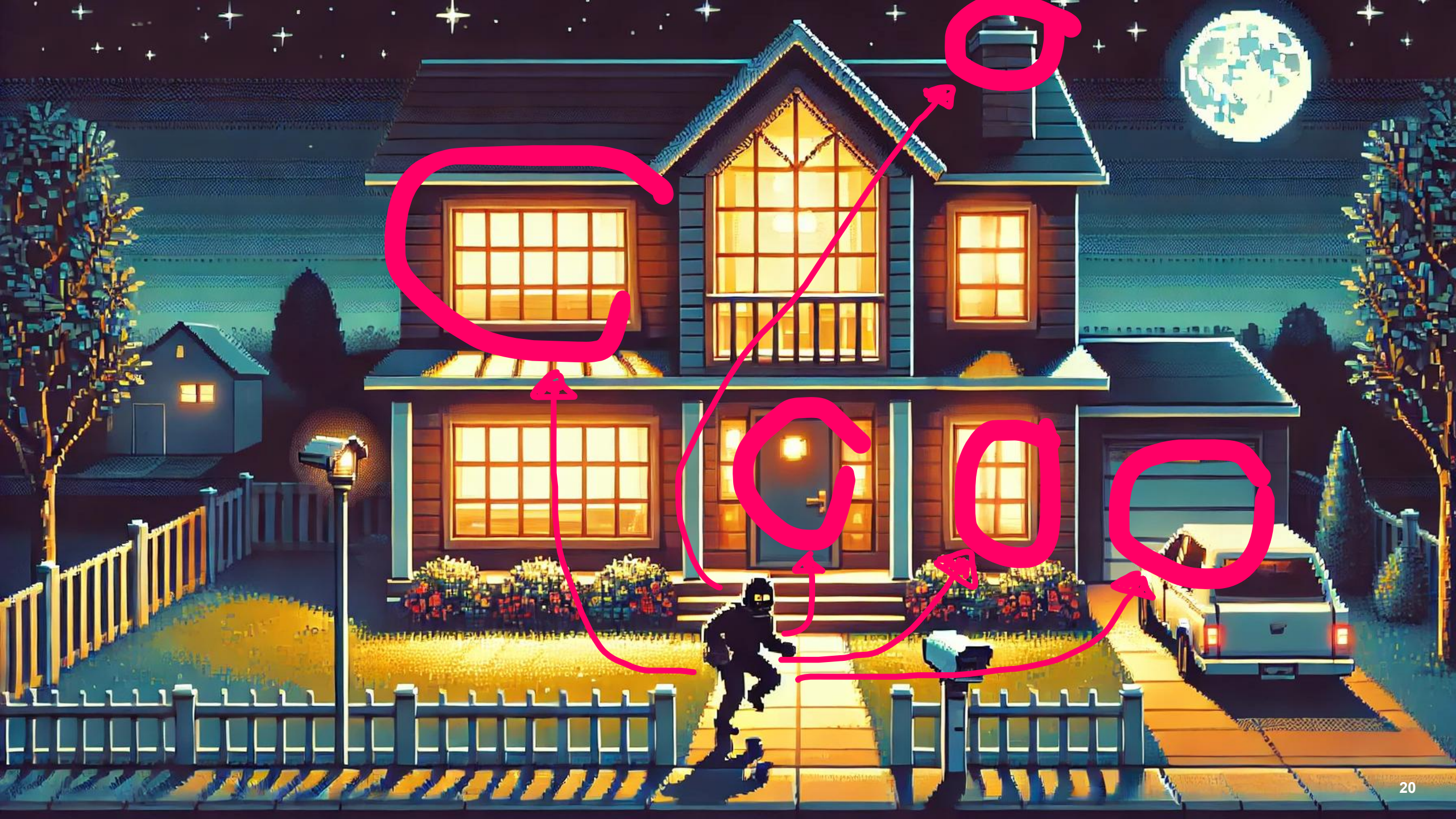

**Lethal doses for patients**

→**Severity:** Catastrophic

→**Probability:** Medium (all patients in the hospital could be affected, however hospital staff is still there)

- **Attack vector:**
  An attack vector is the method or pathway an attacker uses to gain unauthorized access to a system

- **Attack surface:**
  sum of all vectors



# Attack surface analysis

FDA U.S. FOOD & DRUG ADMINISTRATION

- Vulnerability Testing (described in ANSI/ISA 62443-4-1); and
  - Manufacturers should provide details and evidence[47] of the following testing and analyses:
    - Abuse or misuse cases, malformed and unexpected inputs;
      - Robustness.
      - Fuzz testing.
    - Attack surface analysis;
    - Vulnerability chaining;
    - Closed box testing of known vulnerability scanning;
    - Software composition analysis of binary executable files; and
    - Static and dynamic code analysis, including testing for credentials that are "hardcoded," default, easily guessed, and easily compromised.

**Get a free attack surface analysis from TÜV SÜD**

→ jan.kuefner@tuvsud.com

https://www.fda.gov/media/119933/download

# Pitfalls for MD pen-testing

1. Skills (iOT) / missing certs (OSCP)
2. In-House pen-testing?
3. Attack surface incorrect
4. Testing depth (Fuzzing / Zero Day angle)
5. Too much automation / only scans

# Pitfalls for MD pen-testing

1. Skills (iOT) / missing cer
2. In-House pen-testing?
3. Attack surface incorrect
4. Testing depth (Fuzzing /
5. Too much automation / c

IG·NB
Interessengemeinschaft der Benannten Stellen für Medizinprodukte in Deutschland

4 (relevant output documents of the) Lifecycle

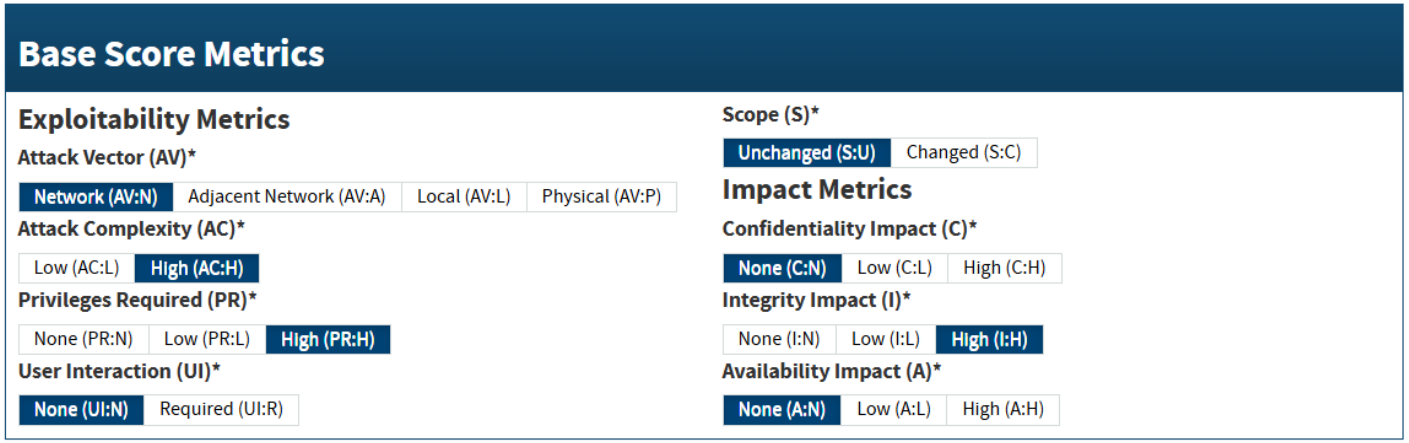
| | Source | Requirements | Questions / Comments |
|---|---|---|---|
| 1. | IEC 62304 cl. 8.1.2 | – document for each SOUP configuration item being used (including standard libraries): title, manufacturer, unique SOUP designator | Has the manufacturer documented all components that are considered software of unknown provenance (SOUP)? |
| 2. | MDCG 2019-16 chapter 3.7 | 'The primary means of security verification and validation is testing. Methods can include security feature testing, fuzz testing, vulnerability scanning and penetration testing.' | • Is the penetration test report available and appropriate?<br>○ Is the penetration test covering all applicable attack vectors?<br>○ Is the tester appropriately skilled?<br>○ Is the tester independent?<br>○ Are appropriate tools used?<br>○ Is / are enough time / resources utilized?<br>• Is appropriate Fuzz Testing conducted where applicable?<br><br>Note 1: Common penetration testing methodologies such as open-source security testing methodologies (OSSTMM), phased structured approaches such as penetration testing execution standard methodologies should be adapted as appropriate for the medical device until appropriate standards are available.<br><br>Note 2: The penetration test should consider any special constraints relating to the medical device(s) such as the safety of the patient and others as well as clinical performance. |
| | IEC 81001-5-1 cl. 5.7.5 | – documented means of ensuring objectivity of the test effort for security requirements testing, known vulnerability scanning and penetration testing | |

11

https://www.ig-nb.de/index.php?eID=dumpFile&t=f&f=4344&token=c9b7fff6f527a154b284a0549166c3d9fd1a155e

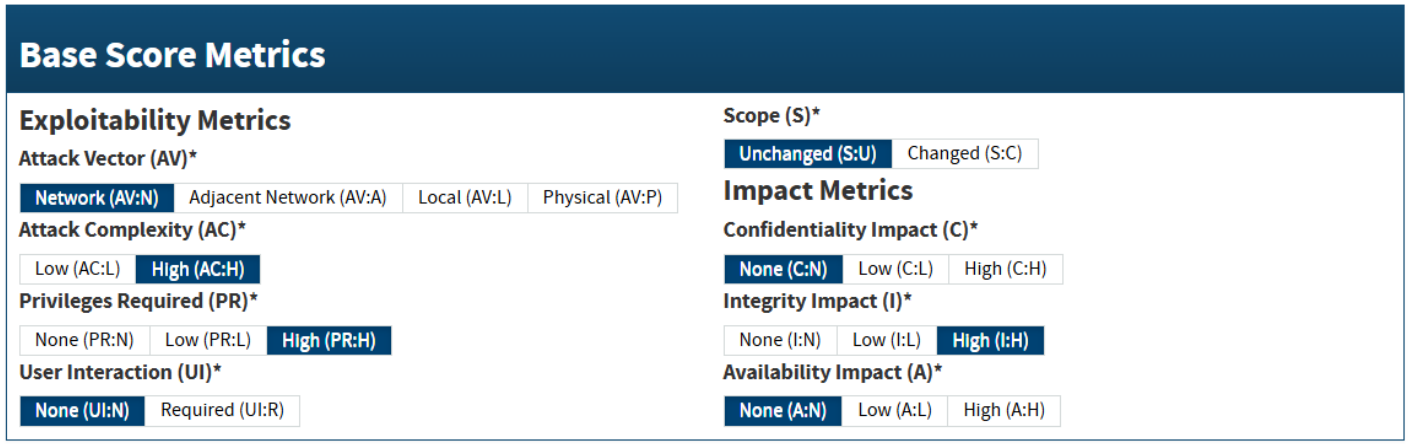
# Vulnerability chaining (→ FDA)

- **Change Files on the device (Disable alarms, Ignore SW watchdogs, …) via Internet, however Admin credentials necessary**
  **CVSS v3.1 Vector** AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N **4,4**
- **Get fleetwide SuperUser password via UART**
  **CVSS v3.1 Vector** AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N **4,2**



# Vulnerability chaining (→ FDA)

- **Change Files on the device (Disable alarms, Ignore SW watchdogs, …) via Internet, however Admin credentials necessary**
  **CVSS v3.1 Vector** AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N **4,4**
- **Get fleetwide SuperUser password via UART**
  **CVSS v3.1 Vector** AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N **4,2**




**Shut of life sustaining treatment globally for all patients without alarms**

**→Severity: Catastrophic**

**→Probability: High (all patients globally can be affected)**

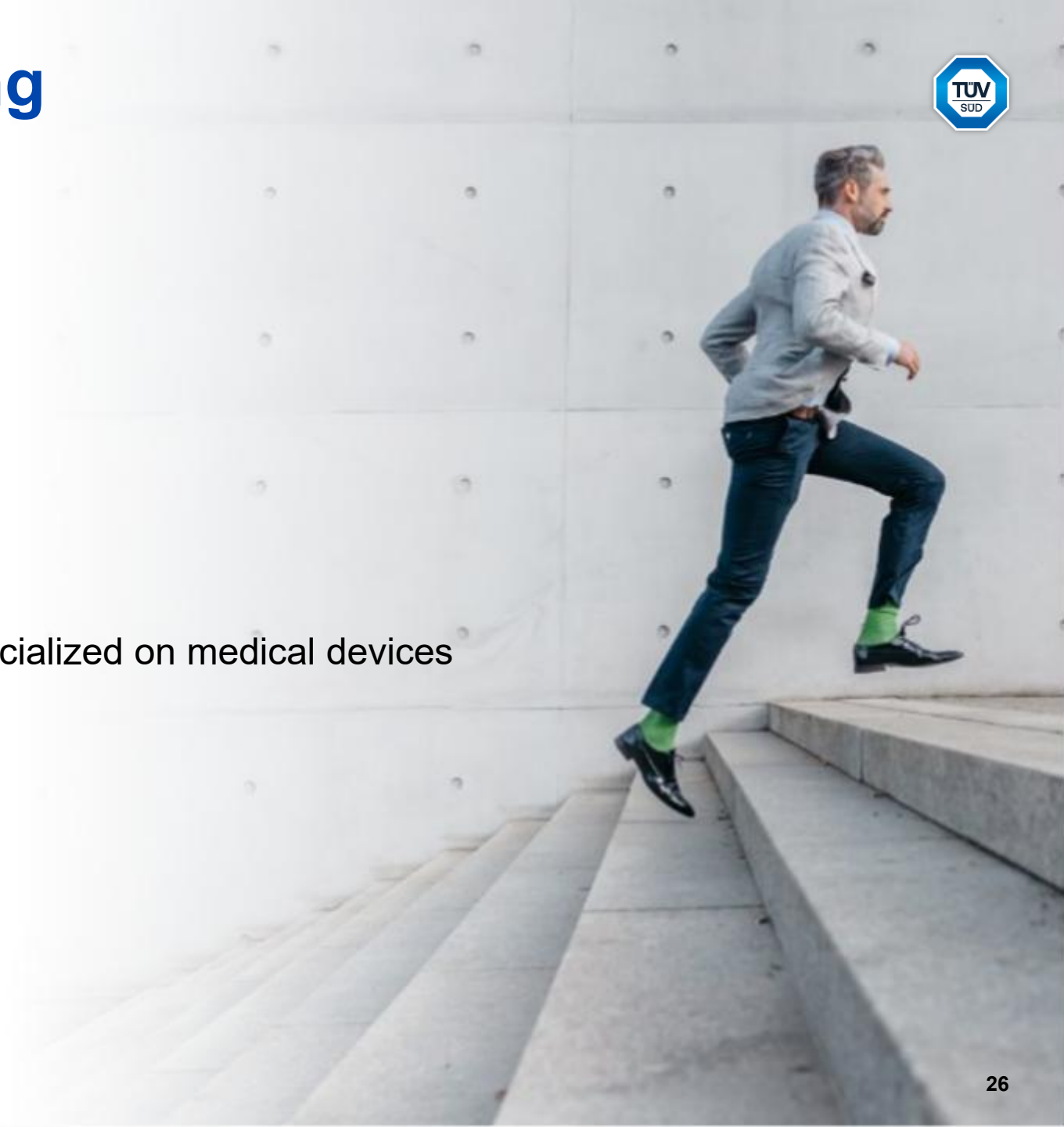
# TÜV SÜD Penetration Testing

**Medical / IVD Experts:**
DICOM, SDC, FHIR, POCT-1a

**Hardware Experts:**
Bluetooth, Wi-Fi, GUI, USB, CanBus

**Time to Market:**
We guarantee timelines, since we are specialized on medical devices
No hickups in certification

**17025 accredited:**
First and only to be 60601-4-5 accredited.



# Customer Inquiries

**Pasha.Razifar@tuvsud.com**

**Follow us on:**

tuvsud.com/en
medicaldevices@tuvsud.com