Cybersecurity for Medical Devices – Lessons Learned from Critical Industries

Christof Ebert and Ruschil Ray | MedConf 2025 | www.vector.com/medical-consulting

V1.0 | 2025-05-07

Agenda

1.	Welcome!
2.	Cybersecurity in MedTech
3.	Lessons Learned From Critical Industries
4.	Where Do You Go From Here?

Who We Are

Vector Group

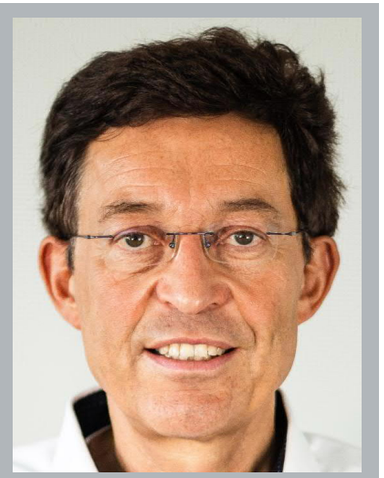
Employees:
> 4,500 Vectorians

Customers:
> 9,000 companies, worldwide

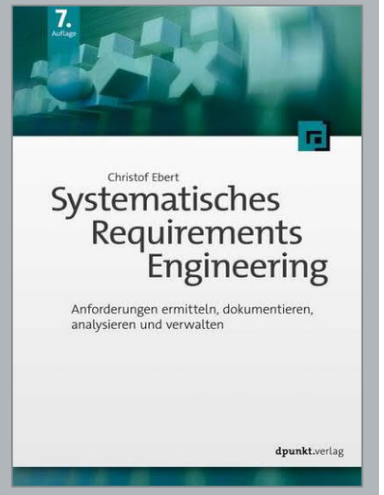
- Automotive
- Medical
- Critical systems

Turnover:
1.01 bn €
in 2024

Christof Ebert

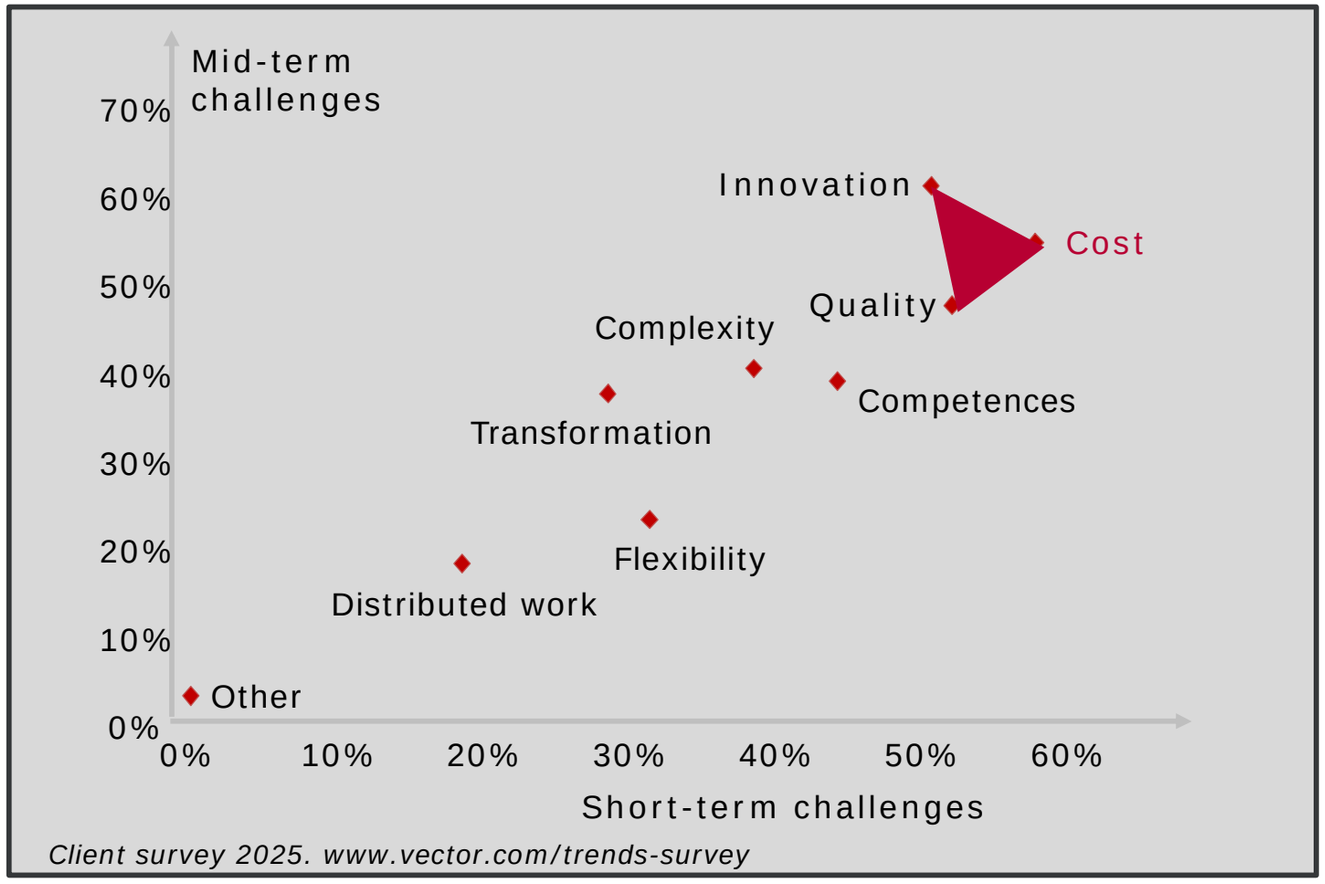


- Managing director of Vector Consulting Services.
- Supporting clients worldwide in technology and agile transformation.
- 12 years in senior R&D positions with a global systems OEM.
- Patents in AI and autonomous systems
- Member of several industry advisory boards.
- Ed. Boards of IEEE Computer, IEEE Software, JSS, SQJO
- Professor at Stuttgart University and the Sorbonne in Paris.



www.vector.com/consulting

Industry Trends 2025 — The Return of the Magic Triangle



Client survey 2025. www.vector.com/trends-survey

> *With their **broad practical background** Vector Consulting Services provided lots of good stimulus and supported implementation. On this basis we achieved **significant improvements**.«*
>
> ***Dr. Ulrich Lefarth,** **Head of Engineering**, **Hitachi***

Innovation and cost pressure immediately impact quality.

Agenda

1. Welcome!
2. Cybersecurity in MedTech
3. Lessons Learned From Critical Industries
4. Where Do You Go From Here?

Medtronic Insulin Pumps (2021): Cybersecurity researchers discovered **IoT device vulnerabilities** in Medtronic insulin pumps that allow attackers to **control the devices remotely**, prompting alerts from the FDA.

Pacemaker manufacturer incident (2024): Vulnerability to allow unauthorized access. Identified weaknesses in communication protocols that could be exploited remotely to manipulate device settings.

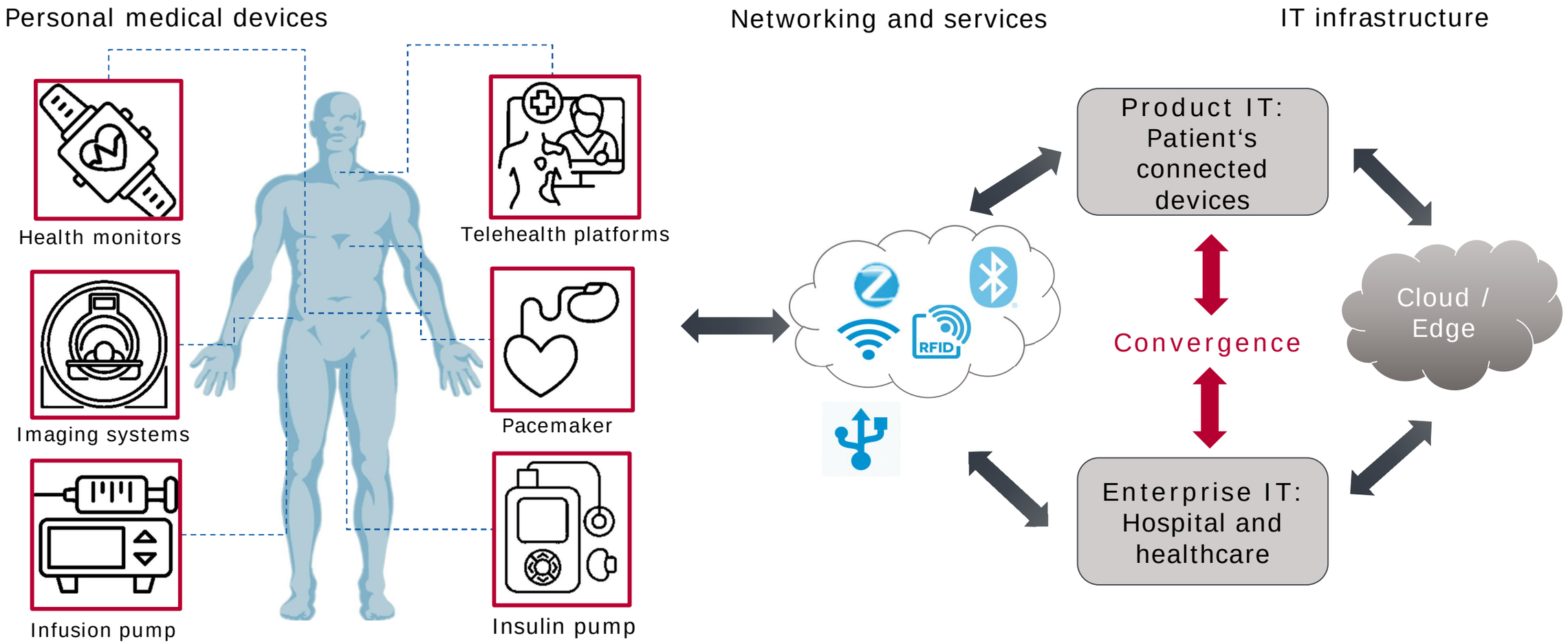
Health Care Services Corporation (HCSC) (2021): Em
by a **phishing attack** that led to unauthorized access to sensitive
information.

Medical Imaging Systems (2024): A significant **ransomware attack** targeted several medical imaging systems, which not only encrypted data but also threatened the integrity of images, impacting diagnostic capabilities.

Kaseya (2021): The attack affected numerous businesses, including healthcare providers that relied on Kaseya's software for IT management. This incident showcased the risks associated with **third-party software vulnerabilities**.

Sources: FDA, CISA, NIST, Industry reports (Ponemon, McKinsey etc.), professional organizations (AHA, HIMSS)

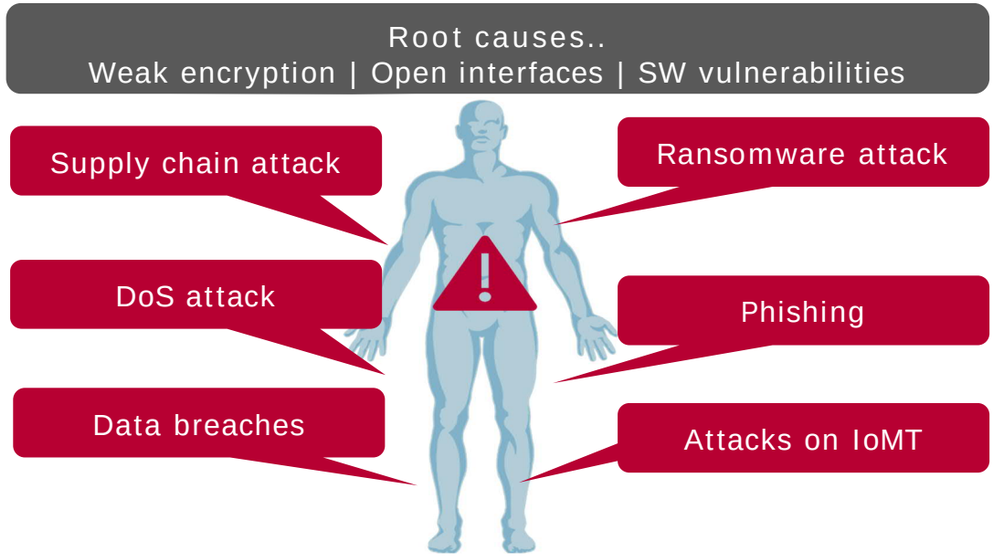
Medical Devices are Connected—and Increasingly Subject to Cyberattacks

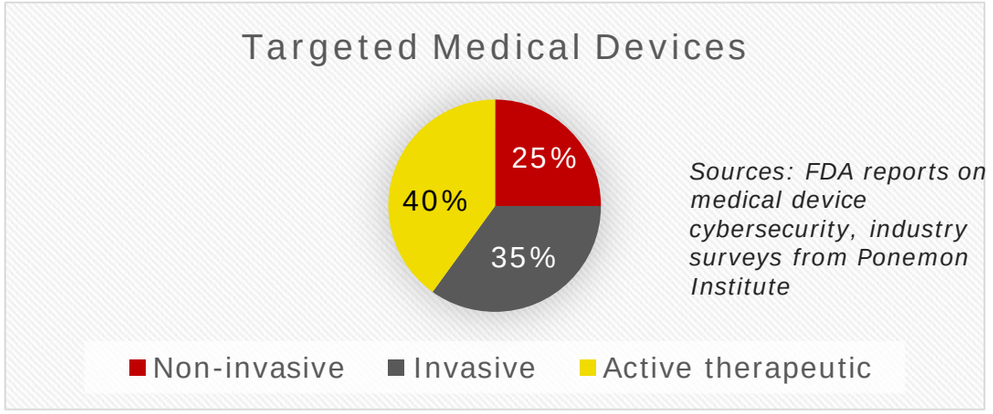


Convergence of medical devices, infrastructure and networked services demands effective and efficient cybersecurity hardening for the entire life-cycle

Cyberattack Trends in MedTech

- IT, OT, IoT convergence: Standard stacks invite for standard attacks with a wealth of global malicious competences
- Legacy systems: Outdated technology due to long life-time
- Weak security protocols: Lack of encryption, insecure default settings
- Inadequate security practices: Limited resources, lack in security test
- Third-party integrations: Supply chain vulnerabilities
- Human factors: Social engineering
- Regulatory complexity: Growing documentation and compliance burdens eat budget that could be used for R&D





Cybersecurity and thus functional safety are today major business risks for medical devices.

Example: Insulin Pump

Risk drivers:

- Sensitive medical data
  Risk: Disclosure of health data
- Safety-critical functionality
  Risk: Over-delivery of insulin
- Cybersecurity vulnerabilities
  Risk: Compromised app allows remote access

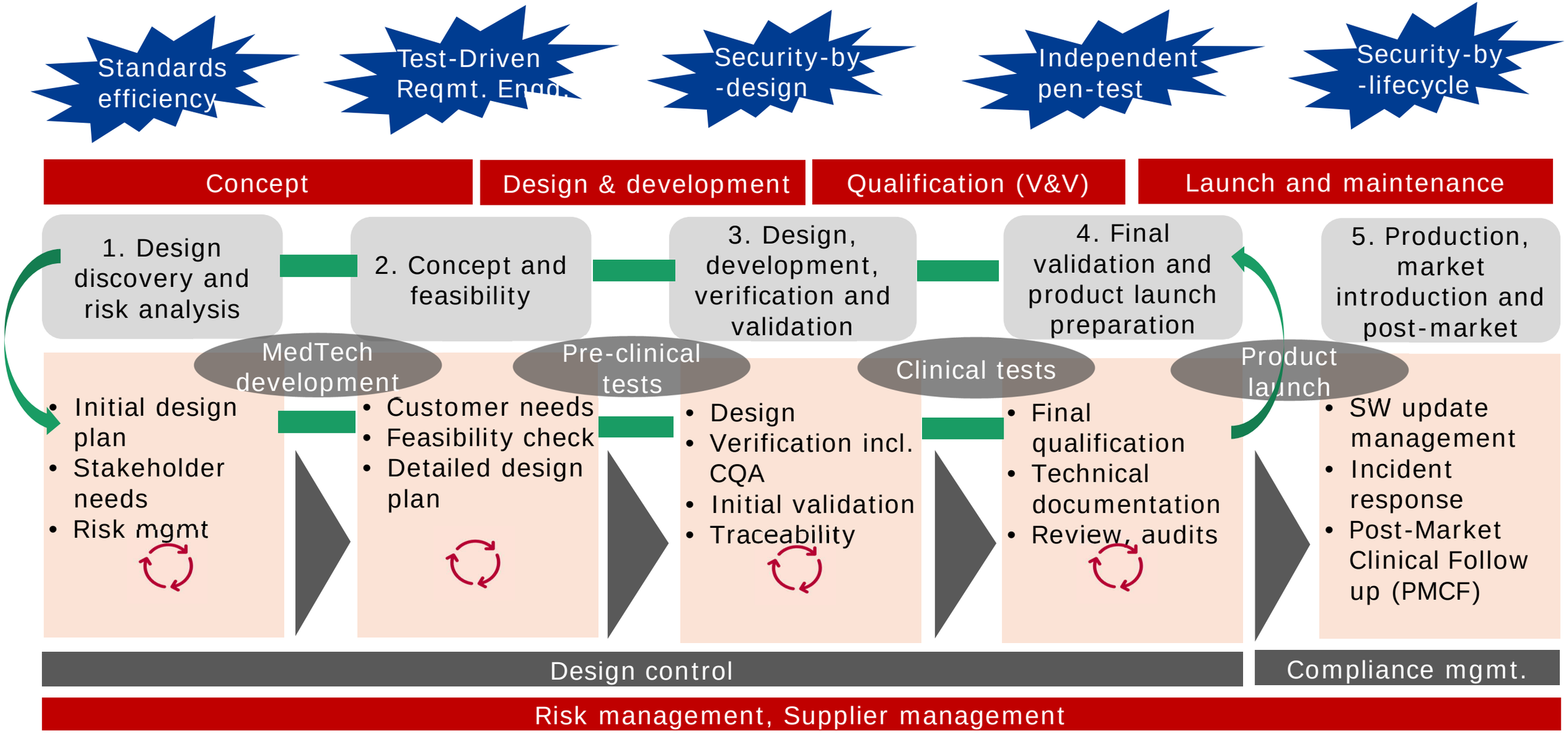
Sources: Insulin pump suppliers, own research.
Picture: Medtronic; but research not limited to Medtronic

Risk oriented cybersecurity is essential to ensure patient safety

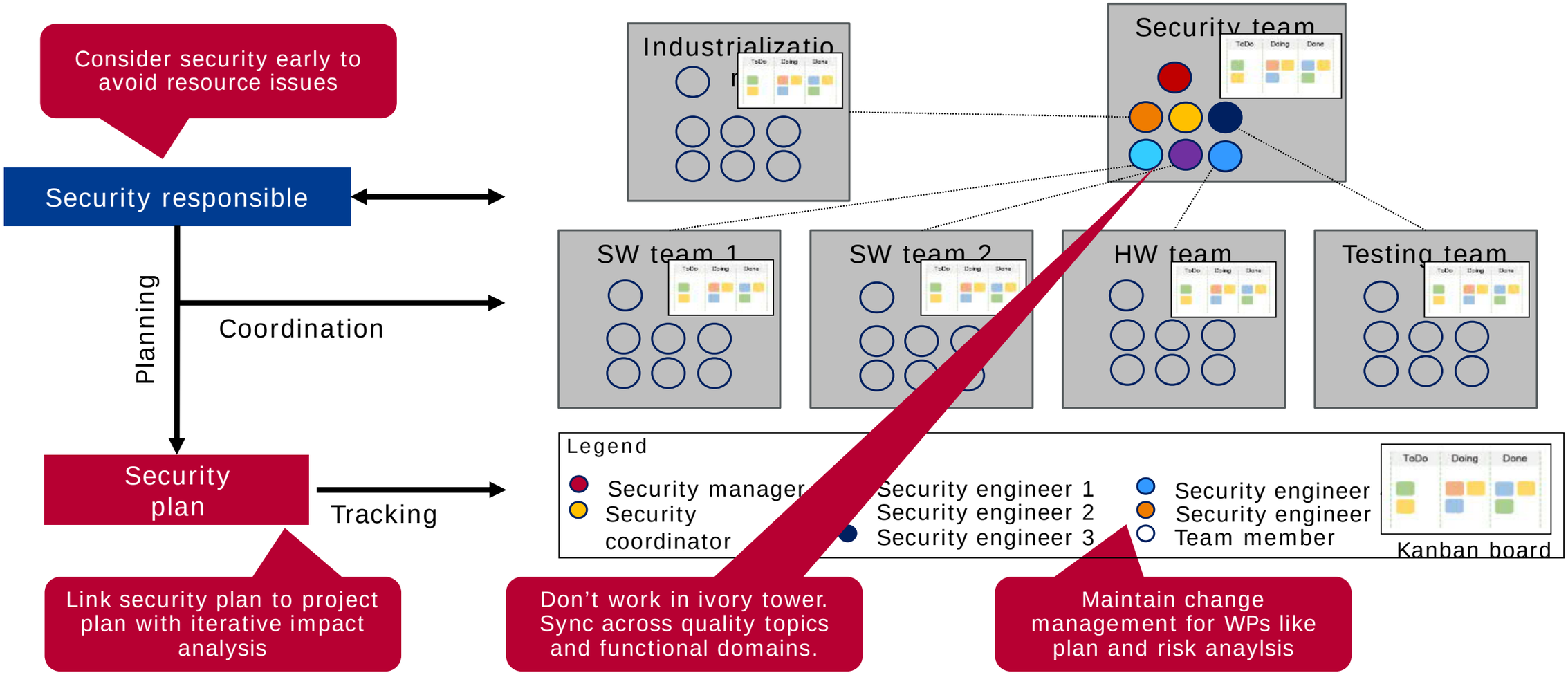
Agenda

1. Welcome!
2. Cybersecurity in MedTech
3. **Lessons Learned From Critical Industries**
4. Where Do You Go From Here?

Best Industry Practices Mapped to Medical Device Product Development Lifecycle



Standards Efficiency: Lessons Learned



Establish agile push-pull for efficient and effective standard propagation and best practice sharing.

Standards Efficiency: MedTech Guidance

Product liability:
A product, that is put in service,
must provide the level of safety which can be expected by general public.

Functional safety

- IEC 60601 (Safety & performance medical electrical equipment)
- IEC 62304 (Medical device SW lifecycle)
- ISO 14971 (Medical device risk management)
- IEC 62366 (Usability engineering, UX in medical devices)

Cybersecurity

- IEC 62443 (Cybersecurity in industrial automation)
- NIST SP 800-53 (IS risk management)
- FDA Guidance on cybersecurity
- ISO/IEC 27001 (Information security)
- NIS2: EU directive on IT security that also affects MedTech

Certification & homologation

- FDA (US)
- EMA (EU)
- Health Canada

Emerging guidelines

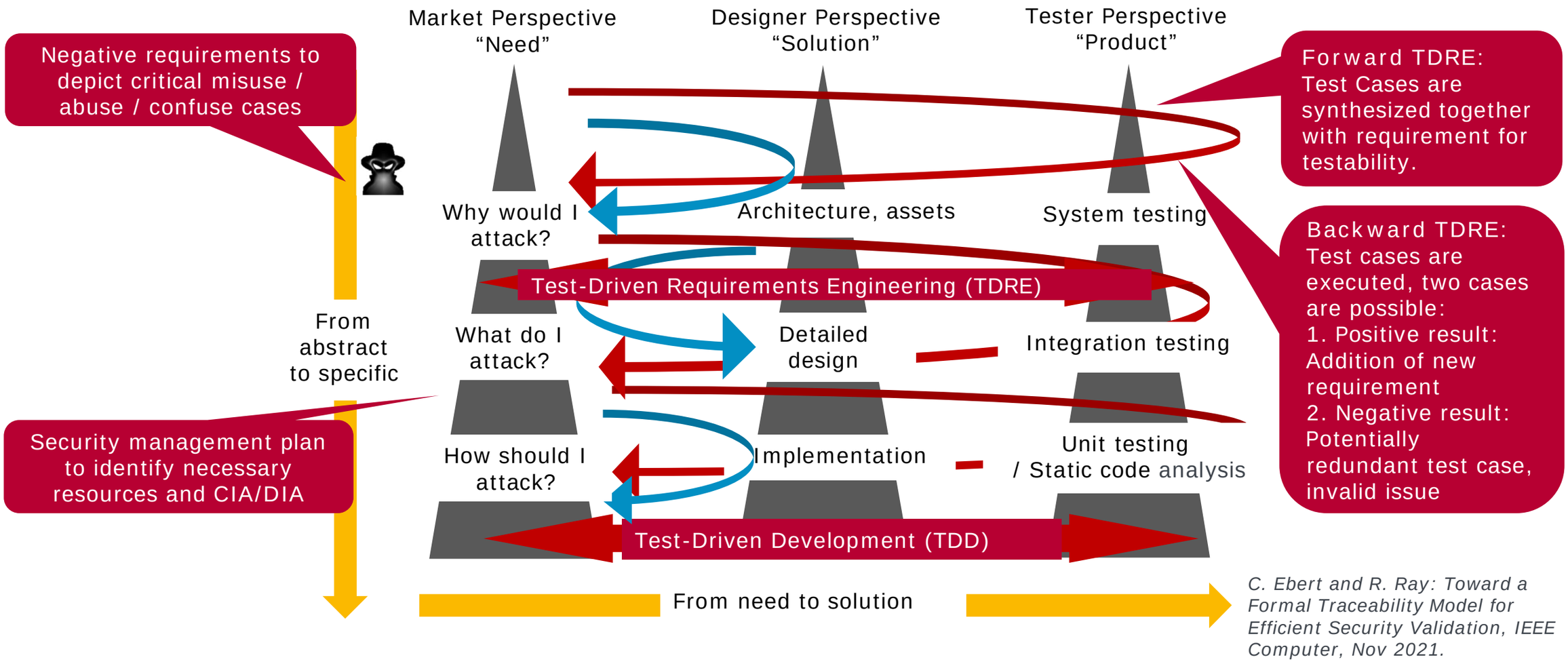
AAMI TIR57

Process maturity: ISO 330xx and risk management: ISO 31000
Methodological frameworks such as ASPICE, are demanded by “higher-level” quality standards

Product development process: ISO 9001, ISO 16949 (automotive), etc.

Reference to multiple standards instead of just copy paste. Adress standards simultaneously.

Test-Driven Requirements Engineering (TDRE): Lessons learned



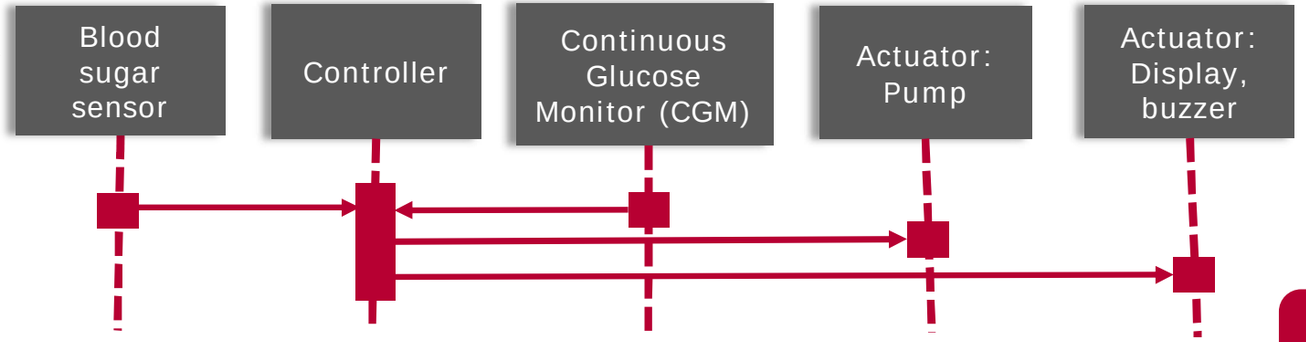
C. Ebert and R. Ray: Toward a Formal Traceability Model for Efficient Security Validation, IEEE Computer, Nov 2021.

Triple peak model to efficiently and reliably connect requirements with test and qualification.

Test-Driven Requirements Engineering (TDRE): MedTech Guidance

Testable and traceable security requirements. to design elements

Scenario: Computation and delivery of insulin dosage



TDRE implemented as follows:

- Regulatory requirements for medical technology
- Customer needs.
- Security standards and constraints

Req. ID	Requirement Description
/FR 1/	When blood glucose sensor OR CGM computes the blood sugar level, then this reading is sent to controller via RF or BLE.
/FR 2/	When blood sugar level exceeds the safe maximum threshold, then insulin dosage pump signal set to one shot delivery, „Blood sugar too low“ is displayed, buzzer alert set to TRUE.
/FR 3/	When there is a new software update is TRUE, ‘Accept software update’ signal is set to TRUE, and controller accepts update from remote programmer.

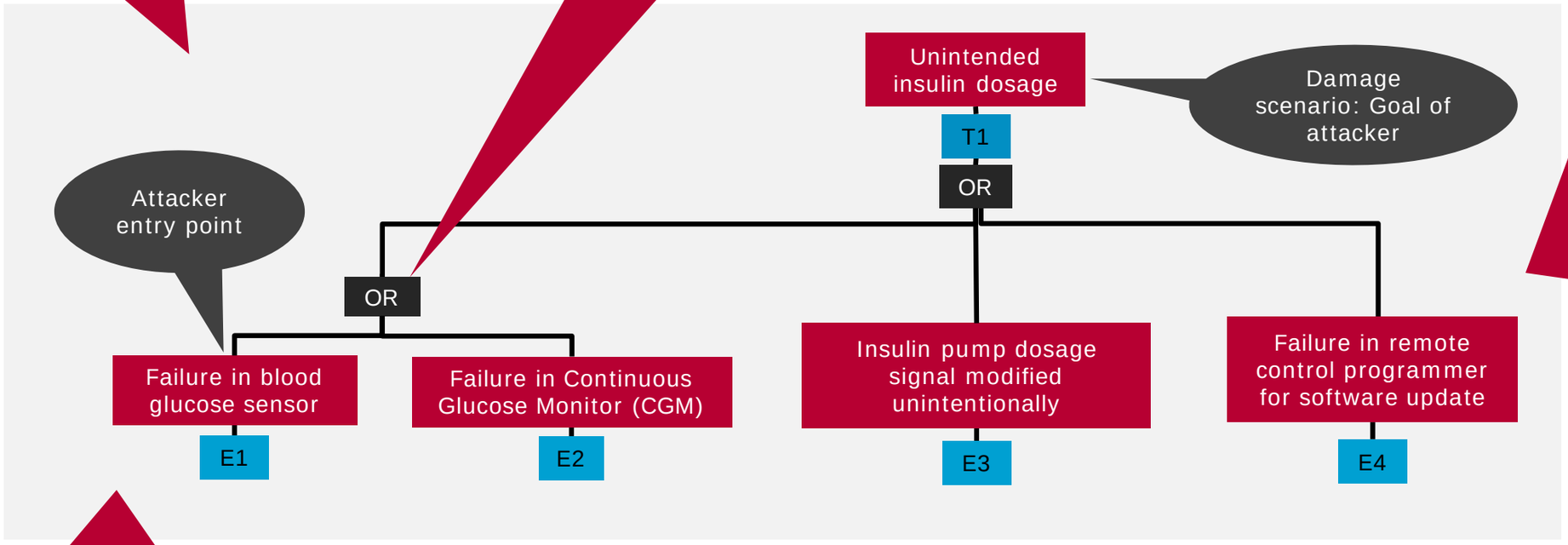
Security requirements. reviewed by experts for completeness and correctness

Security requirements should be testable and well traced to architectural components

Security-by-Design: Lessons Learned

Threat modelling for security architecture design and reviews

Application of secure coding guidelines and design principles



Fault Tree Analysis (FTA) using as threat modelling method

T1: Top event;
E1,E2,E3,E4: Error conditions

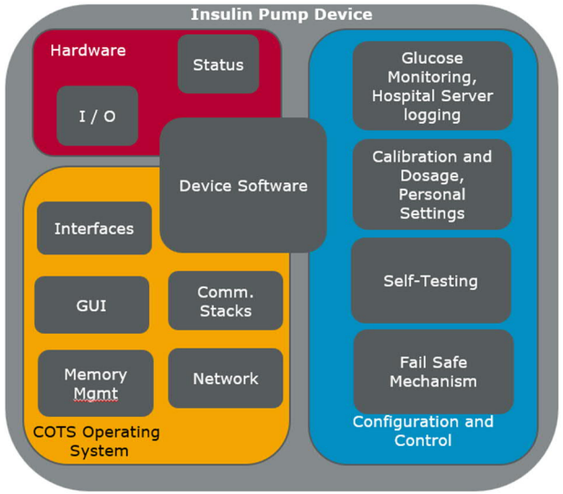
Threat modelling to identify test scenarios

- Ensures system works for unexpected user action.
- Diagnostic capability of FTA deduces the error conditions: vulnerabilities that can be exploited by hacker.

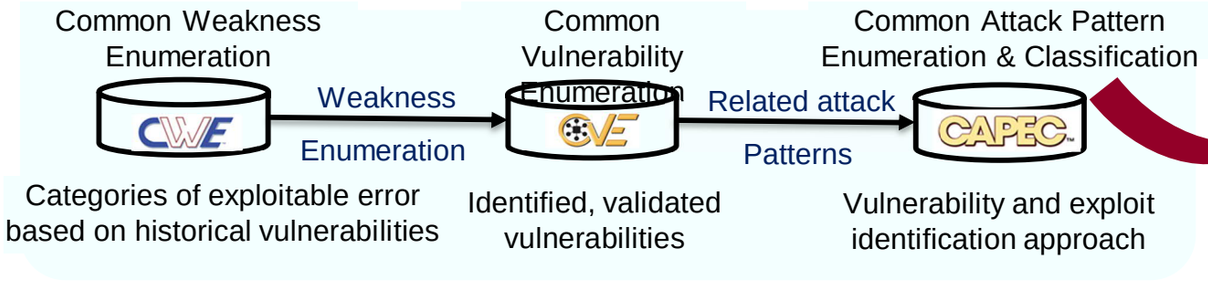
Threat modelling helps to deduce misuse, confuse and abuse scenarios

Security-by-Design: MedTech Guidance

Architecture schematics: Better identify threats & vulnerabilities



Assets	Damage scenario	Threat scenario	Attack vector / test cases	Risk level
Blood sugar level RF / BLE	Unintended insulin dosage.	Spoof sensor and tamper readings causing excess or low insulin.	Compromise RF / BLE / of Sensor Compromise RF / BLE / Wi-Fi port of CGM	5
Insulin dosage pump signal	Unintended or suspension of insulin dosage.	Spoof controller and causing suspension of insulin by the pump.	Compromise RF / BLE / Wi-Fi port of controller then pump Compromise RF / BLE port of sensor, then controller, followed by pump	5
Software update signal	Software corruption in controller memory.	Spoof remote programmer and tamper controller software causing excess, low or suspension of insulin.	Compromise RF / BLE /Wi-Fi port of remote programmer	5
Buzzer alert signal	Customer distraction, battery drain due to repeated buzzer alerts.	Spoof controller and cause excessive buzzer alerts leading to battery drain, customer distraction.	Compromise RF / BLE / Wi-Fi port of controller, then the buzzer	3



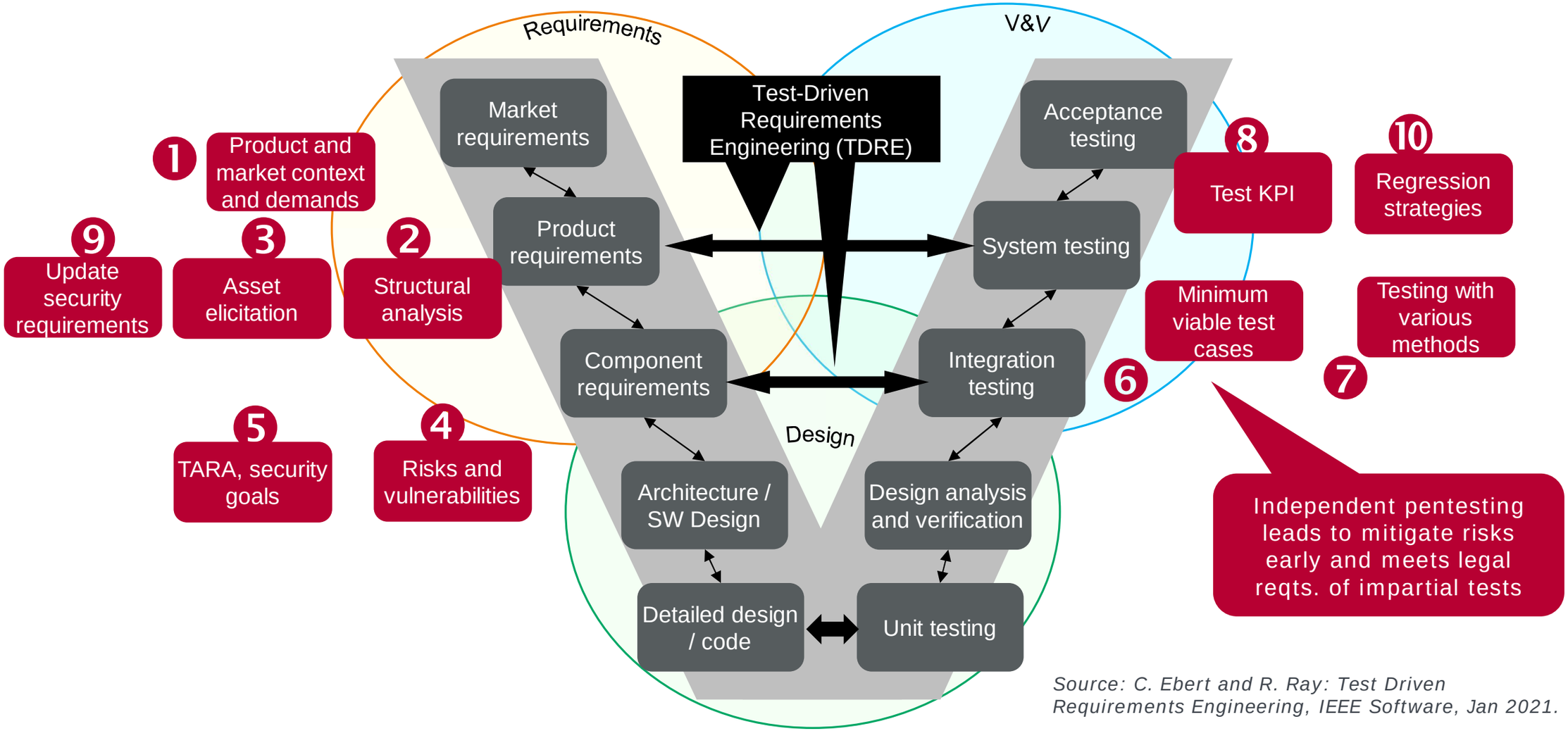
Security heuristics: Threat catalog and vulnerabilities

Trace security controls to risks and goals in risk analysis

Creation of preliminary risk analysis with risk acceptability criteria

Preliminary risk analysis using architecture schematics and vulnerability databases

Independent Pen-Test: Lessons Learned



Source: C. Ebert and R. Ray: Test Driven Requirements Engineering, IEEE Software, Jan 2021.

10 steps for Vector grey-box cybersecurity testing using triple peak model

Independent Pen-Test: MedTech Guidance

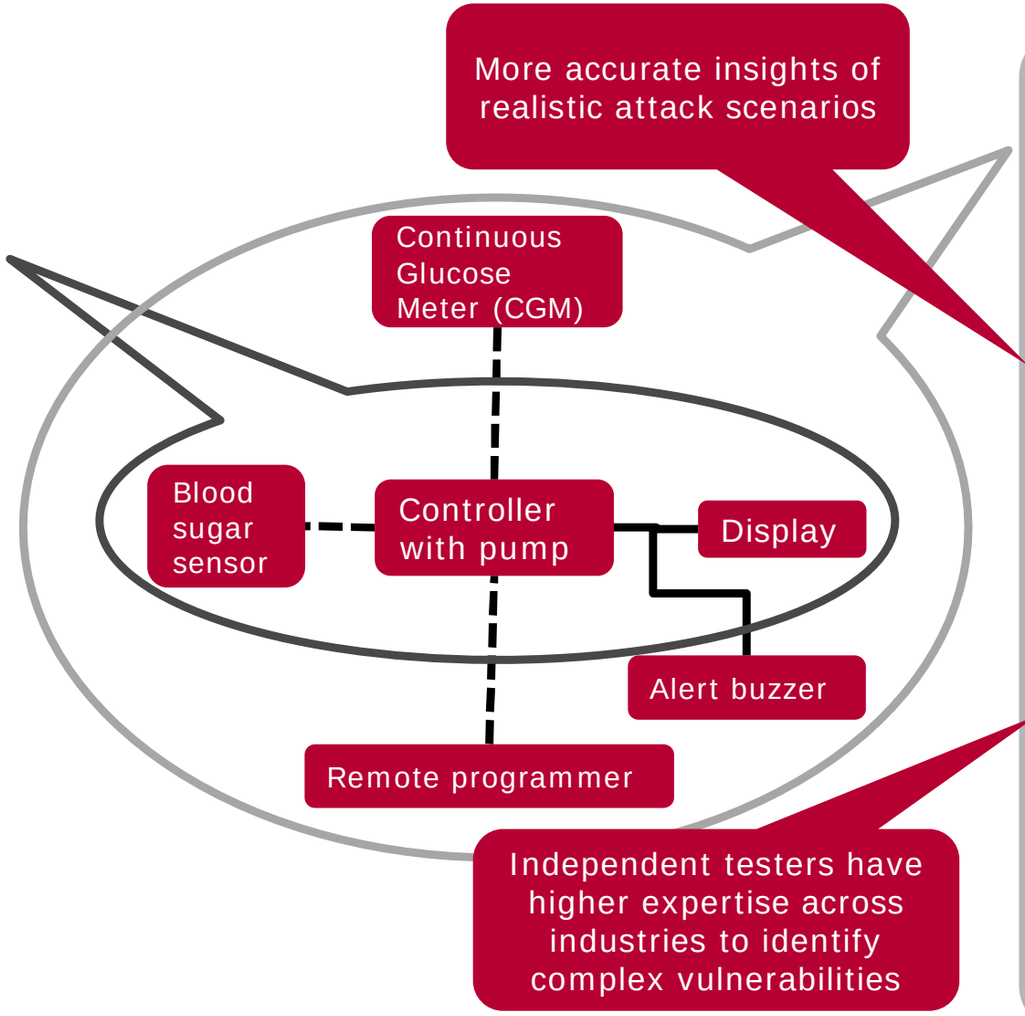
Traditional pen-test

- Unaware of architecture misses crucial vulnerability categories: Alert buzzer, CGM, remote programmer.
- Brute force to determine safe minimum, maximum threshold, lead to false positives. More test effort.
- No risk analysis: Inefficient resource prioritization.

- Test cases: ~ 40 TCs
- False positives: 20
- Missed vulnerability: 5
- Vulnerabilities found: 8

- Effectiveness
  Category coverage: 62%

- Efficiency
  Vulnerability discovery average
  On average 5 TCs needed for finding 1 vulnerability



Independent grey-box pen-test

- Knowledge of high-level architecture taken in account. Good attack pathway coverage.
- Accurate attack tree, less false positives, more valid vulnerabilities found.
- Risk-oriented test approach: efficient resource usage.

- Test cases: ~ 15 TCs
- False positives: 2
- Missed vulnerability: 0
- Vulnerabilities found: 13

- Effectiveness
  Category coverage: 100%

- Efficiency
  Vulnerability discovery average
  On average 1 TC needed for finding 1 vulnerability

Independent grey-box pen-test for enhanced vulnerability detection efficiency and effectiveness

Security-by-Lifecycle: Lessons Learned

Requirements

Design

V&V

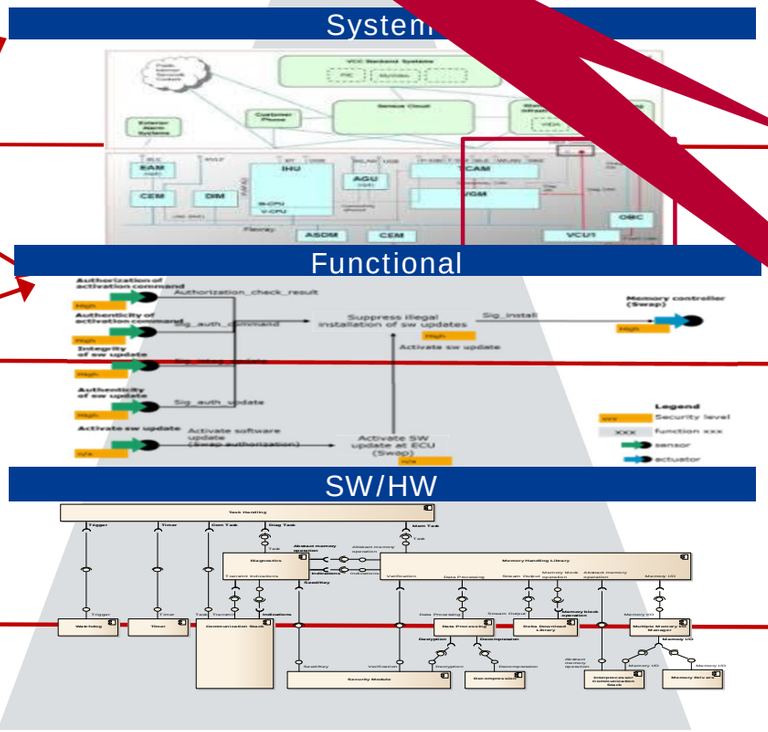
Systematically decompose SYS to SW & HW security reqmts.

Security artifacts traced across vertical and horizontal abstractions

Market needs, software assets, safety/security goals

Product requirements, functional safety/security requirements

Component requirements, technical safety/security requirements



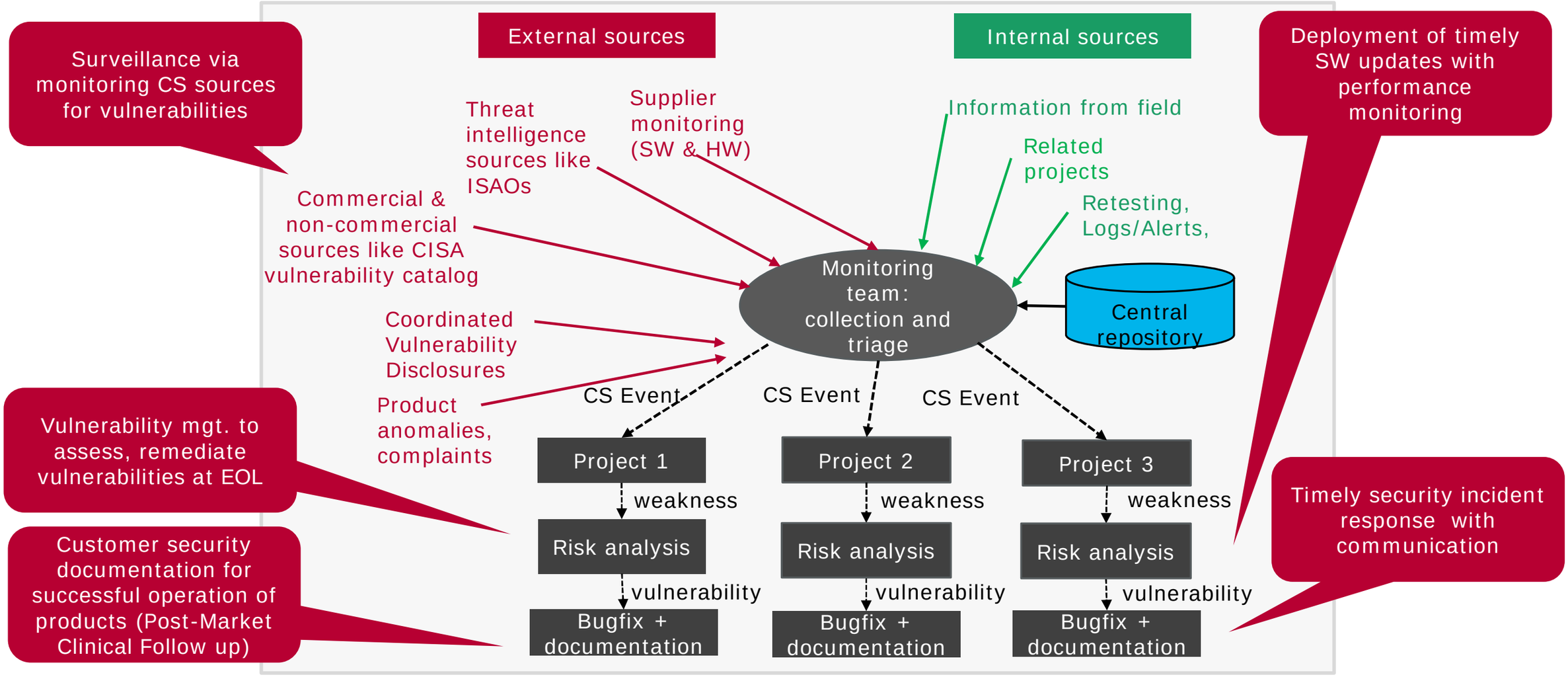
Component and system test, grey-box Pentest, robustness tests, fuzzing, cognitive testing, etc.

Functional test, interface tests, integration test

Unit test, Static code analysis

Ensure consistency with vertical and horizontal traceability across different abstractions

Security-by-Lifecycle: MedTech Guidance



Continuous CS monitoring with incident response ensures security across the lifecycle

Agenda

1. Welcome!
2. Cybersecurity in MedTech
3. Lessons Learned From Critical Industries
4. Where Do You Go From Here?

Learn and Adopt from Other industries

- Standards efficiency: Consider security early on to avoid resource constraints and ensure good collaboration with development/project team.
- Test-driven requirements engineering: Maintain traceable and testable security requirements to test cases to ensure early testing and improved feedback to requirement updates.
- Security-by-design: Perform systematic risk assessment to which lead to security goals followed by security requirements.
- Independent pen-test: Use independent pen-test for unbiased testing and higher vulnerability detection effectiveness.
- Security-by-lifecycle: Monitor CS sources continuously for vulnerabilities before and after production, also create incident response plan to dynamically counter field issues.

Contact us and see us at Vector booth.

https://www.vector.com/medical-consulting/

Join Us at Vector Forum 2025

Vector Forum 2025: Cut Cost, Not Innovation

- Agile for dependability, safety, reliability.
- AI solutions for efficient testing and cybersecurity.
- Future-proof digital transformation.
- Hands-on. Online. Global. Interactive. Free.
- May/June 2025. One hour, each Thursday: 7h EDT, 13h CEST, 16h30 IST, 19h CST.
- With Bosch, DaimlerTruck, Loewenstein Medical, Porsche, Siemens Healthineers and more.

Details and registration...

www.vector.com/forum25

Contact us and achieve value.

Passion. Partner. Value.

Vector Consulting Services

www.vector.com/consulting

consulting-info@vector.com

+49-711-80670-1520

linkedin.com/company/vectorvcs

youtube.com/@VectorConsultingServices