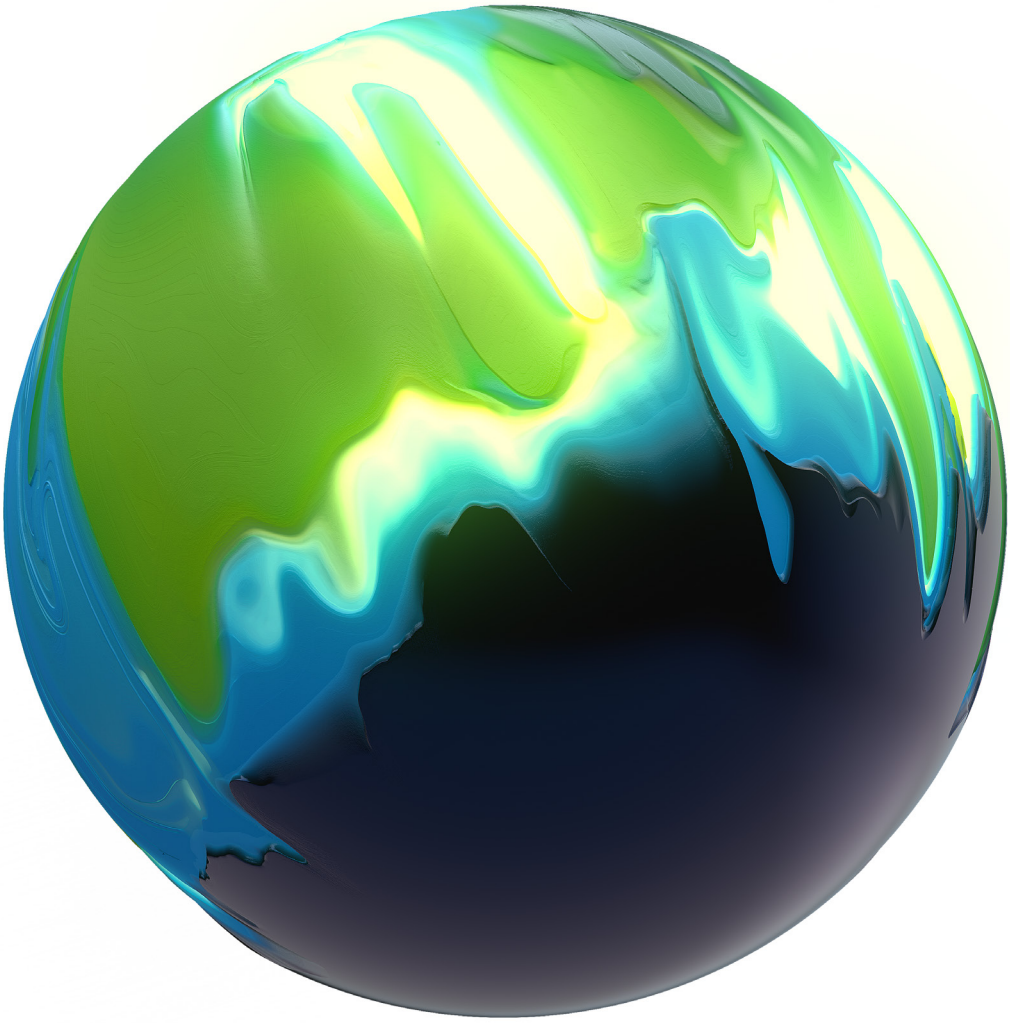
Deloitte.



Medical Device Security Testing

A smart, efficient way to add security testing to your development lifecycle
Security testing should be an essential element of any rigorous security strategy in medical device and healthcare software development. Manufacturers often leave this type of testing to outsourcers as they lack the requisite talent or expertise in-house. Particularly when it comes to embedded devices or interconnected medical networks, this type of testing can be an extremely complex endeavor. Deloitte provides security testing services that go beyond conventional software penetration testing but is designed to assess embedded systems, too. Our services not only ensure regulatory compliant documentation but also provide consulting and training that makes a real impact on your security practices and policies.

MAKING AN IMPACT THAT MATTERS since 1845

Cybersecurity in medical ecosystems

The demand for smart, connected medical devices is growing in modern healthcare, with new product launches often featuring connectivity to the internet, hospital networks and/or other medical devices. These features form an IOT ecosystem that is vulnerable to security threats. As the ecosystem expands, it is vital for manufacturers to introduce strategic and tactical measures that will make ecosystems more resistant to cyberattacks. The regulatory requirements introduced by legislators and the – perhaps even more effective – best practices established by the industry are designed to harden IOT systems against these threats. The most popular are:

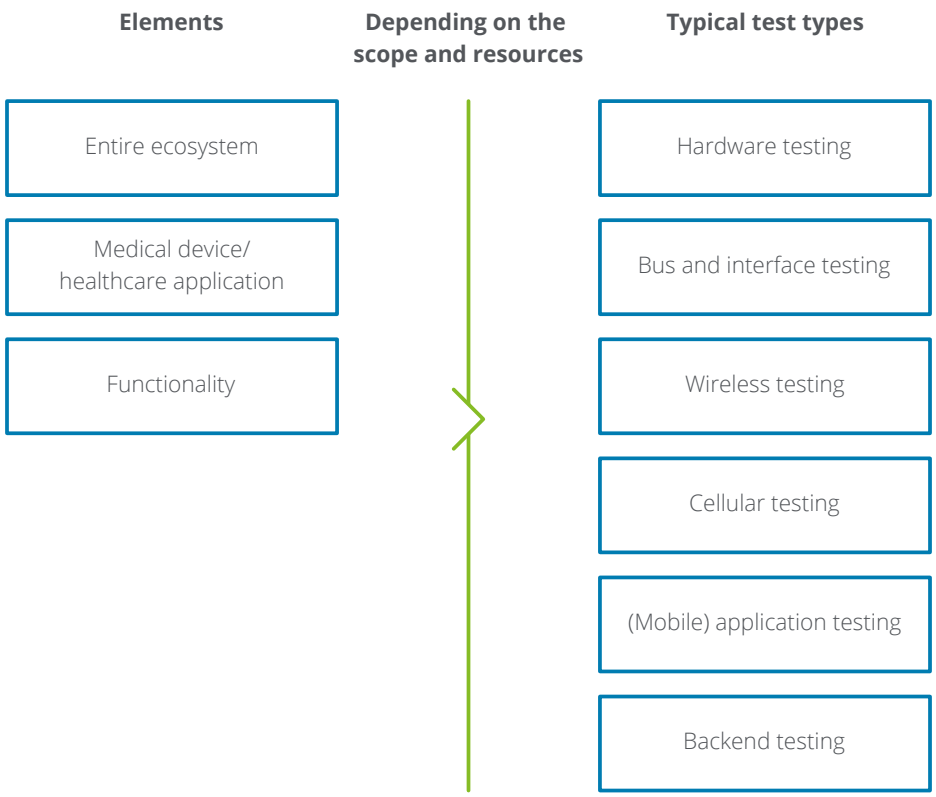
- IEC TR 60601-4-5: Medical Device Cybersecurity
- IEC 81001-5-1: Security – Guidance for the Product Life Cycle
- ISO 62443 Series: Security for Industrial Automation
- MDCG 2019-16: Medical Device Cybersecurity
- FDA Cybersecurity: Quality System Considerations and Content of Premarket Submissions
- FDA Cybersecurity: Postmarket Management of Cybersecurity in Medical Devices
- FDA Cybersecurity: Cybersecurity for networked medical devices [...]

The value of security testing

Today's healthcare sector has become a significant target for hackers and cybercriminals. When private and confidential health data is compromised, the safety and health of patients may potentially be at risk. It is virtually impossible, however, to eliminate threats and vulnerabilities solely through the design process. With such a complex environment, healthcare manufacturers and operators need to work together to manage cybersecurity risks. It is not only vital to implement security-by-design principles early in the lifecycle but also to conduct simulation exercises that replicate real-world (simulated) attacks on the medical ecosystem.

When we break down the network of interconnected medical devices and services used in real-life environments, these are the key elements and the most common security test types[1].

Fig. 1 – Typical test types



[1] illustrative diagram

Why blackbox testing is not enough?

Security testing is about more than just running attacks against an unknown target like a malicious hacker would. Most real-world hackers are intrinsically motivated and have plenty of time and resources. If one fails, another will inevitably take over. The sheer number of potential attackers may itself expose weaknesses given the likelihood of so many attacks. Security testers need to manage their time wisely, as they are working within the limited budget available for a particular project. To compensate for this disadvantage, companies should give testers a certain amount of background information on the full attack surface, the threat model or even the system architecture. We believe this type of focused security testing offers more bang for your buck and not only saves money but also fits better into today's fast go-to-market timelines.

Deloitte's approach

Our approach starts with a deep technical analysis to identify vulnerabilities in the design and software, combining that with testing in simulated real-world scenarios. In addition to the technical results of the analysis, we give clients a risk overview based on a set of application scenarios.

We only use the best proven methodologies the industry has to offer for our security testing services to ensure we identify all potential weaknesses and provide reliable resilience against potential attacks:

Design threat/attack model

Perform security testing

Provide risk evaluation and feedback

Conduct security training and expert labs

With this approach, we have created a testing roadmap for the life sciences industry that complies with regulatory requirements and good practices. For more guidance along the entire product development lifecycle, see our paper on Medical Device Cybersecurity @ Scale

Design threat/attack model

To make sure security testers focus on the right areas in their simulated attacks, they should either take the lead in the analysis phase or, where "Security Advisors" or "Security Quality Assurance" experts are guiding engineering teams, play a supporting role in this phase.

Fig. 2 – Analysis and planning steps

01 Attacker evaluation

- Attacker profiles (types of attackers, motivation, skills and resources)
- Attacker classification (examples): competitor, tuner, PR hacker, data thief, blackmailer, saboteur, terrorist, government agency, others
- Attack vectors in terms of functional safety (safety), data protection, financial loss and quality in terms of technical documentation
- Test plan based on the result of the threat analysis

02 Entry points

03 Threat analysis

04 Testing plan

05 Technological analysis

06 Penetration testing

07 Risk mapping

08 Recommendations and residual risk

Medical Communication Busses
CAN, Ethernet, and other vendor specific communication bus systems

(Mobile) Applications
Device interaction, 3rd party device integration, comfort items

Integrated Security for Medical Systems
Alarm systems, field service access points, remote maintenance

Connected Medical Services
Global data transfer capabilities and central data stores. Telehealth capabilities

Visualization & Reporting
Reporting systems and interfaces to display and trend medical data

Wireless Communication
WiFi, Bluetooth, GSM, CDMA, RFID, and other wireless technologies

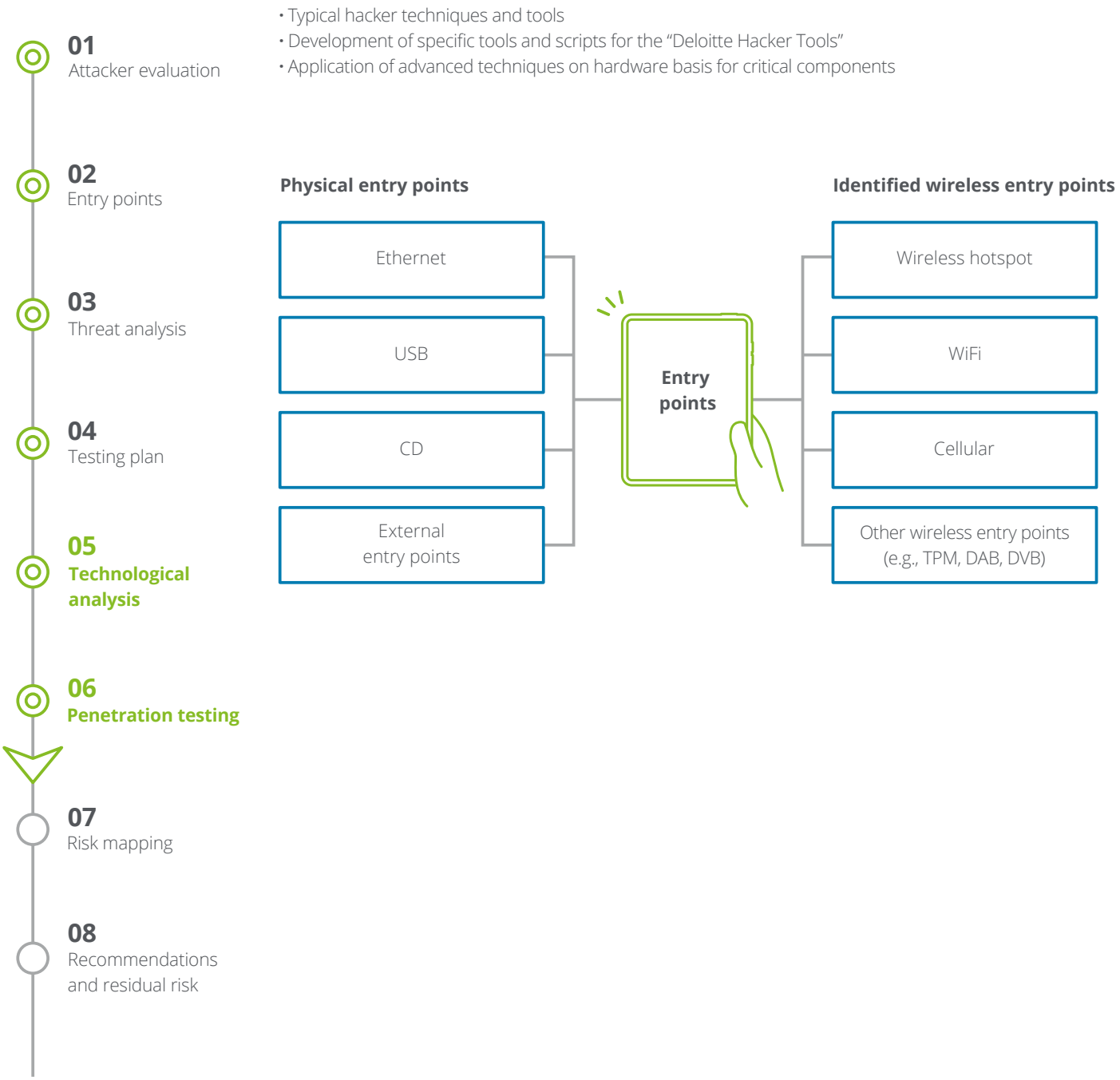
Advanced Medical Systems
Sensors and other advanced device safety systems

Interfaces
Interfaces for integration into hospital information management systems

Perform security testing

Testers can either carry out security testing on-site or in our specialized labs within the European Union. This allows testers to travel on-site at short notice and easily transport equipment as well as test targets. We rely on highly-skilled talent and leverage cross-industry expertise in sectors from automotive to production automation.

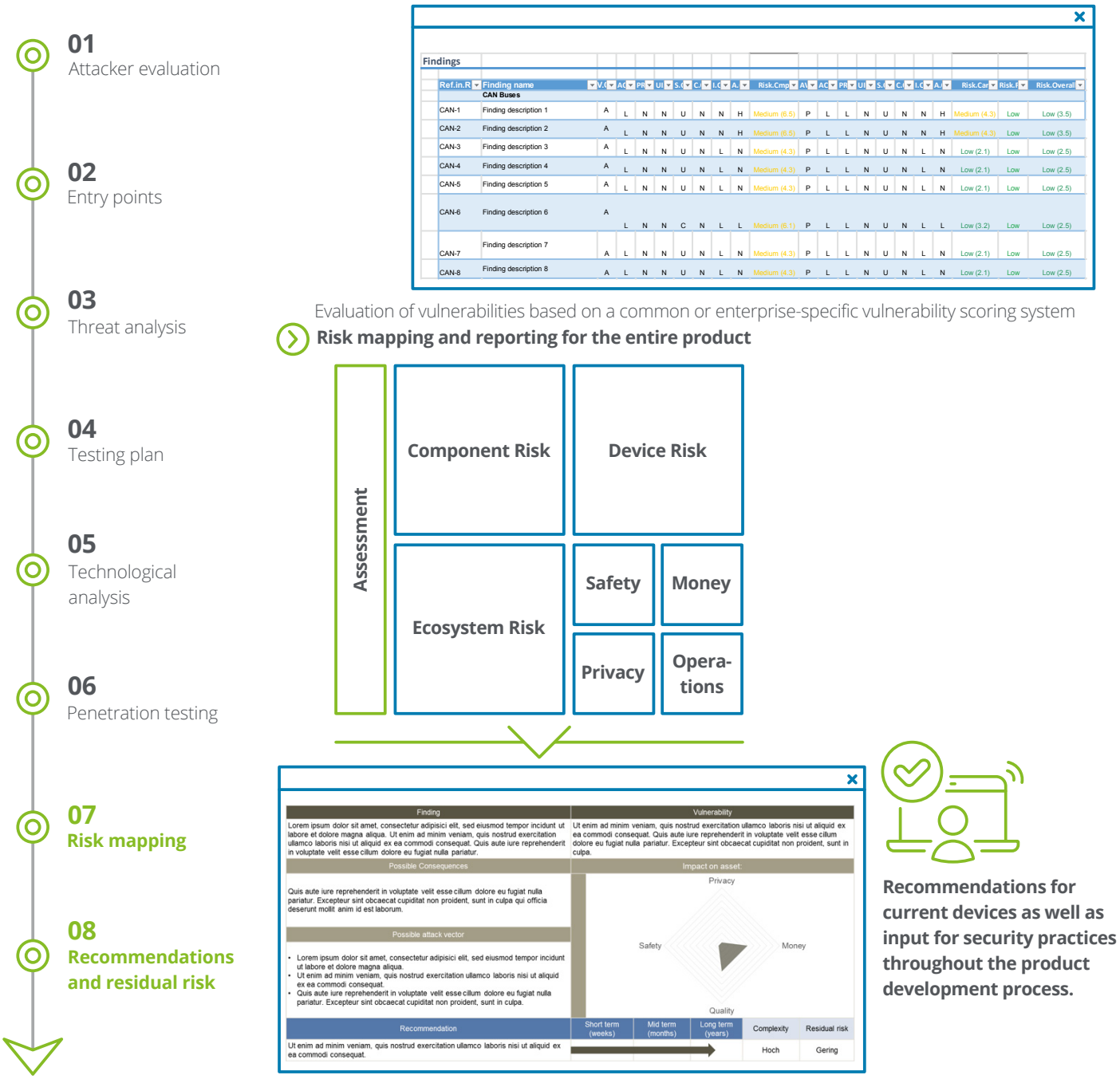
Fig. 3 – Execution steps



Provide risk evaluation and feedback

Our job is not finished after we issue a standard report. We provide continued support to help you understand the severity of the identified risks and how best to respond, knowing full well that cybersecurity risks have to be seen within the context of the particular use case and medical circumstances. We also know how important it is to have a closed loop from security testing back to the design process. You can rely on our support to help your engineering team understand and respond to the findings of our evaluation.

Fig. 4 – Risk reporting steps



Recommendations for current devices as well as input for security practices throughout the product development process.

Conduct security training and expert labs

To ensure continuous improvement and knowledge transfer back to the engineering team, we are happy to share what we have learned. Our training sessions and workshops are tailored to the key challenges of the life sciences industry and your specific engineering processes. We can show you how to use tools effectively or add security practices to your agile workflows.

Fig. 5 – Making a long term impact

Once we have completed our evaluation of your medical ecosystem, we feed this back into your organization.

- Helping you understand how to develop more secure medical devices and infrastructure
- Teaching you how to perform security analysis on your own

Security testing on buses and on connected ecosystem

- Hardware/SW attacks
- Complex embedded components
- Bus Systems
- Mobile applications
- Ethernet
- Other RF
- Backend comms
- WiFi & BT(LE)

Security testing of components

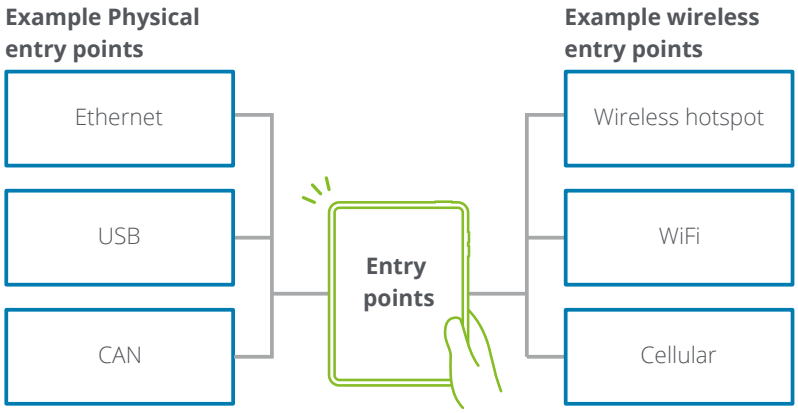
- Hardware/SW attacks
- Communication interfaces and busses
- Reconnaissance
- Debug interfaces
- PCB reverse engineering
- External memory chips
- Signal measurement and analysis
- Side channel attacks

Digging deeper into embedded cybersecurity

When it comes to embedded medical devices in a complex IOT ecosystem, you need more than just software-related testing. Deloitte offers a full range of services that go beyond those outlined below. We will work together to find out the minimum level of service you need and whether it makes sense to include more advanced security testing in an effort to strengthen security, reduce risk and expand your business opportunities.

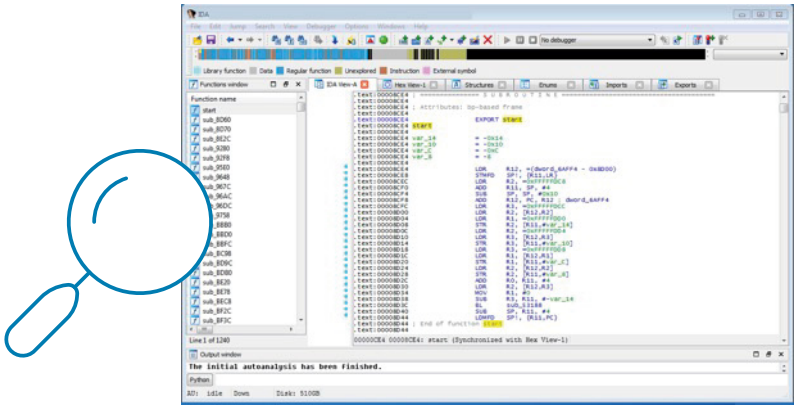
Fig. 6 – Details: software- and firmware security

01
Booting
- Authentication/encryption
- Programming errors in boot flow



02
Software update
- Delivery and protection of update image
- Checking authenticity/encryption
- Programing errors in checking/flashing flow

03
Main software/firmware
- Communication handling
- Authentication/encryption
- Use of known vulnerable software components
- Data storing/handling/user files and input



04
Preparing and executing proof-of-concept attacks against the revealed weaknesses

Fig. 7 – Details: ethernet security

01
Identifying possible entry points for the Ethernet network

02
Connecting to possible entry points – even if it requires moderate dismantling – in various configurations (MitM, SPAN, simple connection)

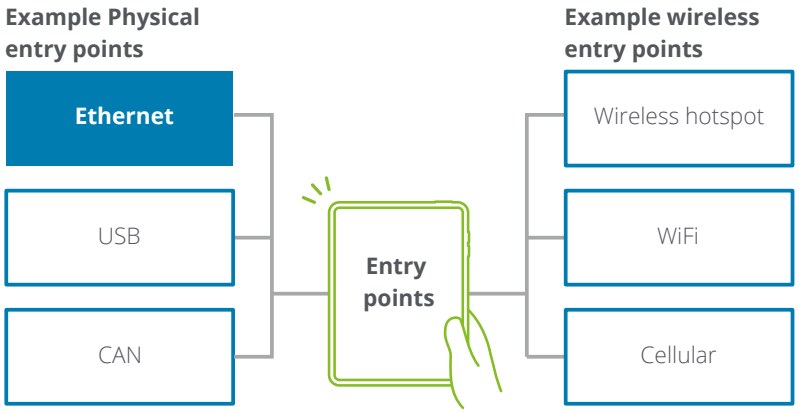
03
Identifying connected components and available services (e.g., sniffing, scanning)

04
Identifying the used protocols (sniffing)

05
Analyzing the identified services and protocols, connecting them to features and identifying possible weaknesses (e.g., unencrypted protocol, weak authentication schema)

06
Creating attack scenarios based on previous steps (e.g., collecting sensitive information, replaying attacks, bypassing authentication, fuzzing, tracking identified service/protocol-related attacks)

07
Conducting testing with identified attack scenarios



Source: http://www.technica-engineering.de/en/products/media-converter/

Fig. 8 – Details: wireless security

01
Wireless connectivity could be used for different scenarios
- Web portal or mobile application to medical device
- Medical device to internet, for tracking and updating functionalities or to server data access to patients and medical personal
- Mobile application to medical device

02
Identifying wireless communication channels and interfaces (mobile data, WiFi, Bluetooth, NFC, etc.)

03
Targeting typical communication channel specific weaknesses, e.g.,
- GSM downgrade for MitM
- WiFi de-authentication and PSK cracking for WiFi Access

04
Investigating captured communication, manipulating intercepted traffic and targeting available services,
- SSL communication between the service and the application
- Authentication / authorization Input validation, etc.

05
Investigating segregation between wireless and treatment services. Trying to influence device functions through different wireless entry points.

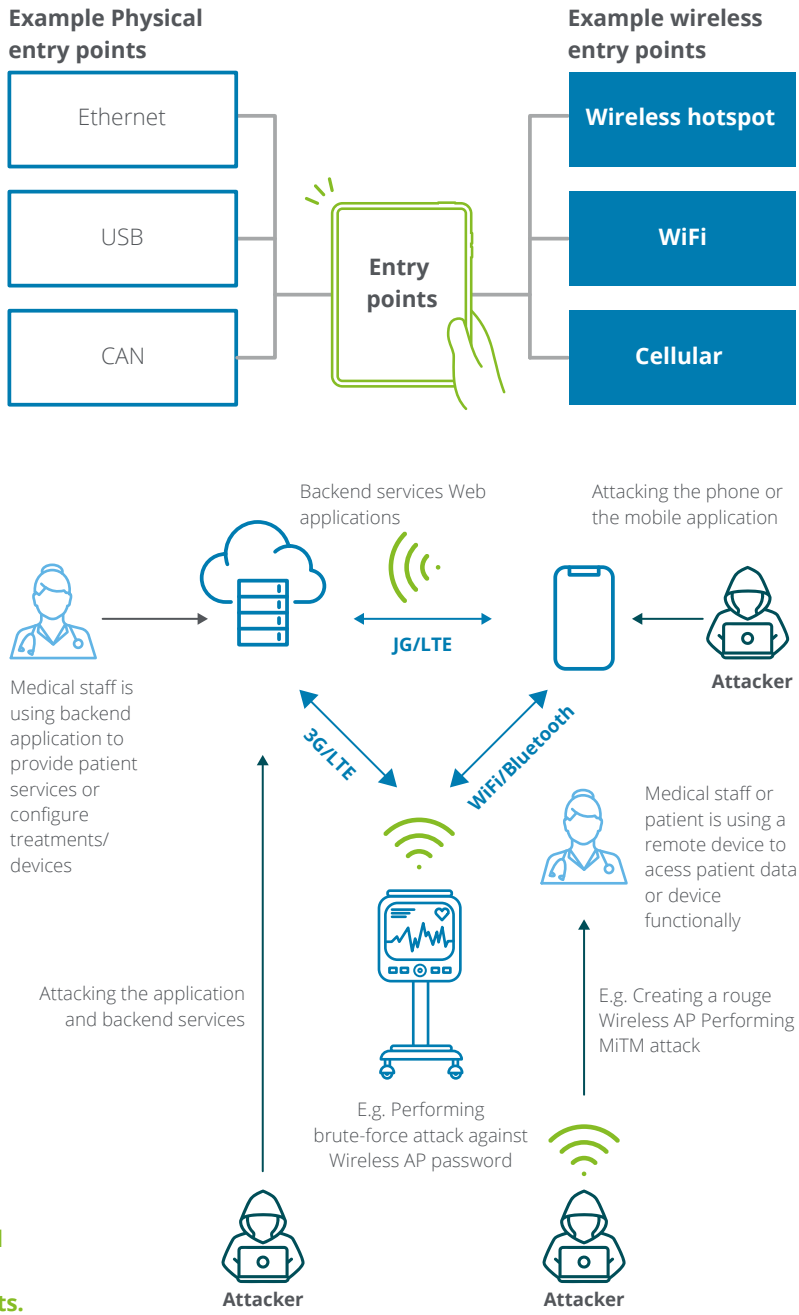


Fig. 9 – Details: cellular security

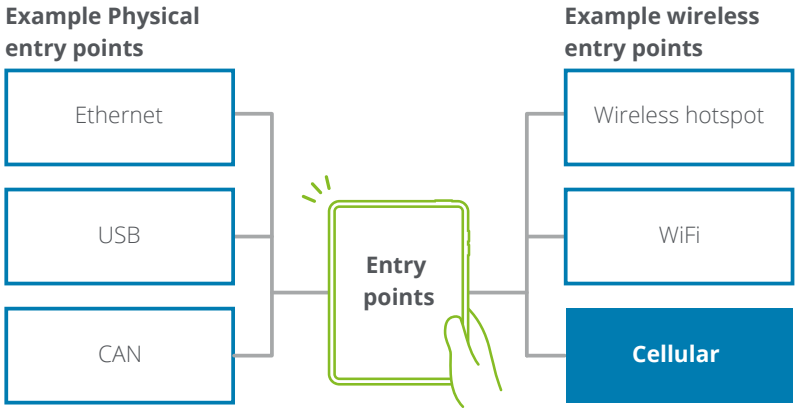
01
Analyzing the possibility of conducting an MitM attack and building the necessary hardware and software configuration (e.g., test environment availability)

02
Identifying the used protocols and services (sniffing)

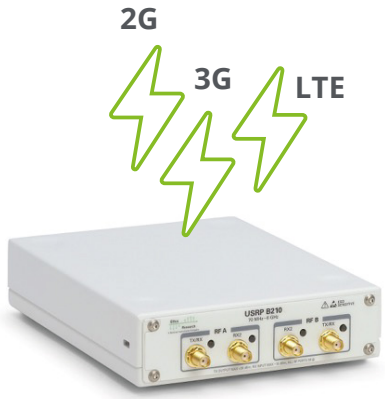
03
Analyzing the identified services and protocols, connecting them to features and identifying possible weaknesses (e.g., unencrypted protocol, weak authentication schema)

04
Creating attack scenarios based on the previous steps (e.g., collecting sensitive information, replaying attacks, bypassing authentication, fuzzing, tracking identified service/protocol related attacks)

05
Conducting testing with identified attack scenarios (e.g., testing the SSL MitM possibilities)



An Ettus B210 SDR with GPS-disciplined oscillator and WBX transceiver card.



Source: https://www.ettus.com/all-products/usrp-b200-enclosure/

Fig. 10 – Details: backend application security

01

Mobile application-level penetration testing, focusing on the typical mobile-related application problems, both general and specific to the given mobile platform, e.g.,

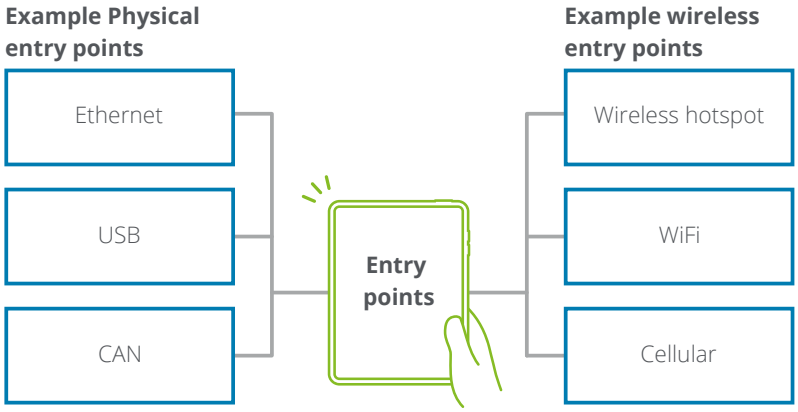
- Storing sensitive data
- Fostering security-conscious usage of mobile APIs (e.g., intents, cryptography)
- Communication security
- Application self-protections

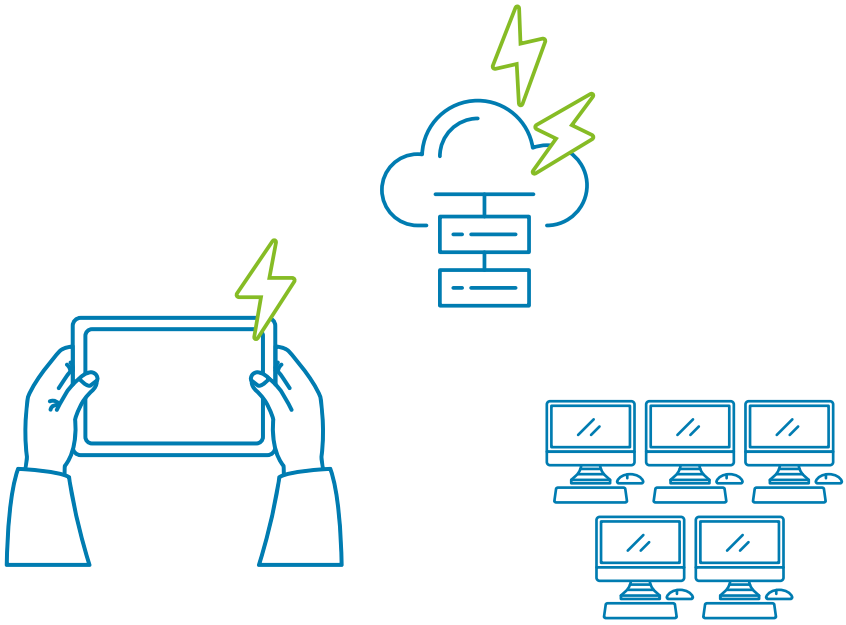
02

Application and infrastructure-level penetration testing of the backend services used by:

- Mobile applications
- Devices
- Web applications used by the customer
- Other connected device services provided to third parties

Focusing on typical infrastructure and application-level security problems, like authentication, authorization bypasses, injection attacks (e.g., XSS, XXE, SQLi) and communication security.



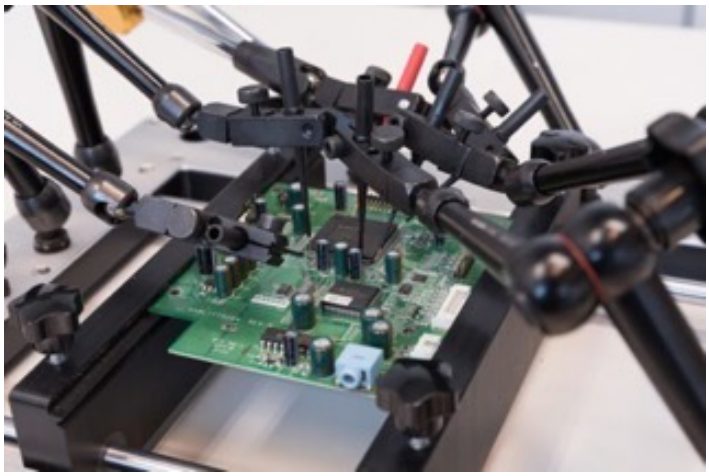


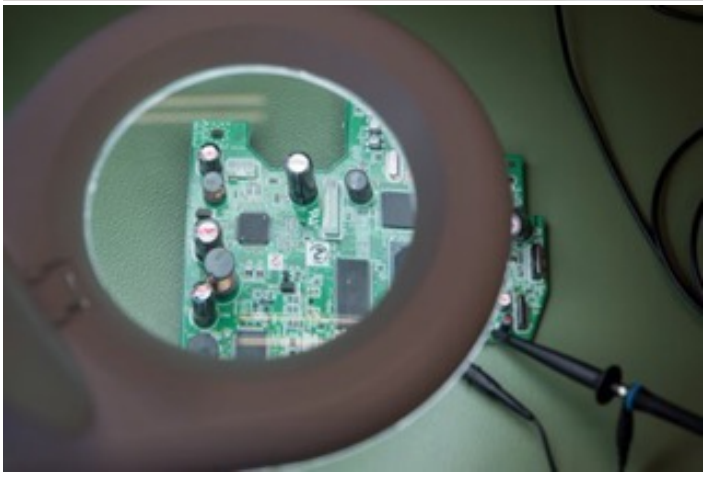
Deloitte specialized cybersecurity testing lab

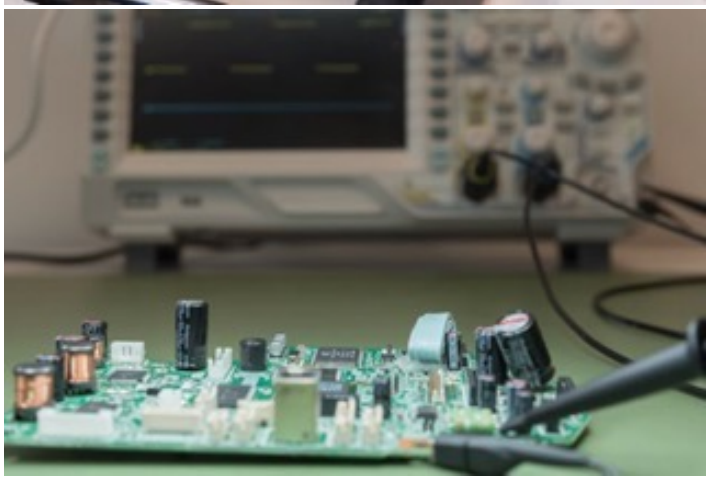
For embedded medical devices within a complex IoT ecosystem, it takes specialized knowledge and toolsets to provide end-to-end penetration testing services for connected ecosystems. That's why Deloitte created a specialized Connected Devices Security Testing Lab where you can avail of the necessary tools and knowledge to perform complex testing activities from the hardware level to cloud-based solutions.

Deloitte cybersecurity services

Deloitte provides end-to-end support for your cybersecurity strategy, whether you are looking for awareness trainings or full-service cybersecurity support where we take on responsibility for your procedures, activities and tools. If you need support, let`s talk.







Contacts

Ingo Dassow
Partner
Global Automotive Cyber Lead
Tel: +49 30 2546 8451
idassow@deloitte.de

Carsten Heil
Director
Risk Advisory
Tel: +49 69 75695 7339
cheil@deloitte.de

More information about Engineering Excellence can be found here:
https://www2.deloitte.com/de/de/pages/risk/articles/engineering-excellence-medtech.html

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Issue 12/2022