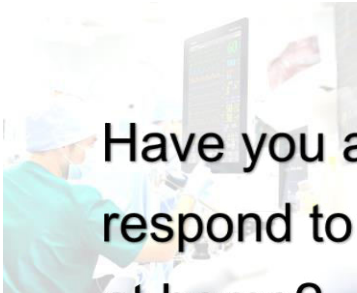
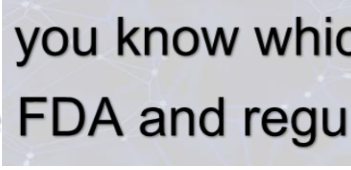



DE0641 Cybersecurity for Medical Device Development



Have you asked yourself how your device would respond to a cyberattack once it's in a hospital or at home?



Do you know which cybersecurity requirements the FDA and regulators in the EU expect you to meet before going to market?



Have you considered how software updates, wireless communication, and data storage in your device could introduce vulnerabilities?



Join our Training and learn the
**Cybersecurity Essentials for
Medical Device Development**

Agenda and Content

- ◆ Welcome, Introduction, Training Goals
- ◆ Cybersecurity Threat Landscape: Why It Matters for Medical Devices
- ◆ Regulatory Frameworks & Standards, e.g.:
 - Medical Device Regulation (MDR)
 - Cyber Resilience Act (CRA)
 - Network and Information Security Directive 2 (NIS2)
 - FDA Guidance
 - ISO 14971
 - IEC 81001-5-1
 - IEC TR 60601-4-5
 - IEC 62443
- ◆ Secure Development Lifecycle - Risk Management & Security Governance
- ◆ Threat Modelling and Security Levels
- ◆ Security Requirements
- ◆ Secure Software Development Fundamentals
 - SW Exploitation
 - Technical Controls and Secure Architecture
 - Coding Guidelines
 - SW Toolchain
- ◆ Validating Device Security: Tools and Techniques for Testing
- ◆ Hardware & Embedded Security
- ◆ Post-Market Security - Vulnerability Handling & Incident Response
- ◆ Pitfalls & Lessons Learned from Real Incidents
- ◆ Q&A and Wrap-Up

As medical devices become more connected, cybersecurity is critical for ensuring patient safety and regulatory compliance.

This expert-led training provides an overview of medical device cybersecurity and equips R&D, QA, and regulatory teams with the tools to integrate cybersecurity into the full medical device development lifecycle.

Who should attend?

Engineers, who want to learn more about cybersecurity related to medical device development, such as:

- ◆ Medical Device Software Developers & Engineers
- ◆ Systems Architects
- ◆ Cybersecurity Specialists / Product Security Engineers
- ◆ Quality Assurance (QA) & Test Engineers
- ◆ Regulatory Affairs Professionals
- ◆ Risk Management & Safety Engineers

Basic experience in cybersecurity and functional safety is beneficial but not required.

Duration: 1 day

Language: English or German in agreement with the participants.

The training material will be in English.

Location: Online

Customer specific on-site or online trainings are also possible – just get in touch!

Certificate: Each participant gets a confirmation of attendance listing the topics covered

For more information, please contact:

Kerstin Tietel

☎ +49 89 44118232

✉ kerstin.tietel@exida.com