Proposed Manufacturer Toolstack:
Secure-by-Design R&D for Connected Medical Devices

Manufacturers need to embed security requirements and best practices throughout the medical device development process.

Our Secure-by-Design Approach

By using tools developed within the NEMECYS project

1 Identify design inputs:

- **Cyber Compass:** Navigate through regulatory obligations.
- **Risk and Threat Modelling (SSM):** Define risks and mitigation controls.
- **Procurement & Compliance:** Align with regulatory and CMD operator requirements.

2 Kickstart the RnD process:

- **Secure Software Development Pipelines:** Embed security in every build.
- **Firmware Fuzzing:** Detect vulnerabilities early in firmware.
- **AI Privacy Risk Assessment:** Assess data privacy in ML models.
- **Secure IoT Service Mesh:** Protect communication between devices and systems.

3 Prototype your medical device:

- **Network Assessment Tool:** Identify misconfigurations and weak points.
- **Secure IoT Service Mesh:** Reinforce secure communication channels.

The Impact

- Medical devices developed based on security-by-design principles.
- Vulnerabilities identified and fixed early in the R&D process.
- Improved compliance and trustworthiness of connected medical devices.

NEMECYS

Contact us

nemecys.eu
info@nemecys.eu
NEMECYS_eu
NEMECYS Horizon Europe Project
NEMECYS Horizon Europe Project