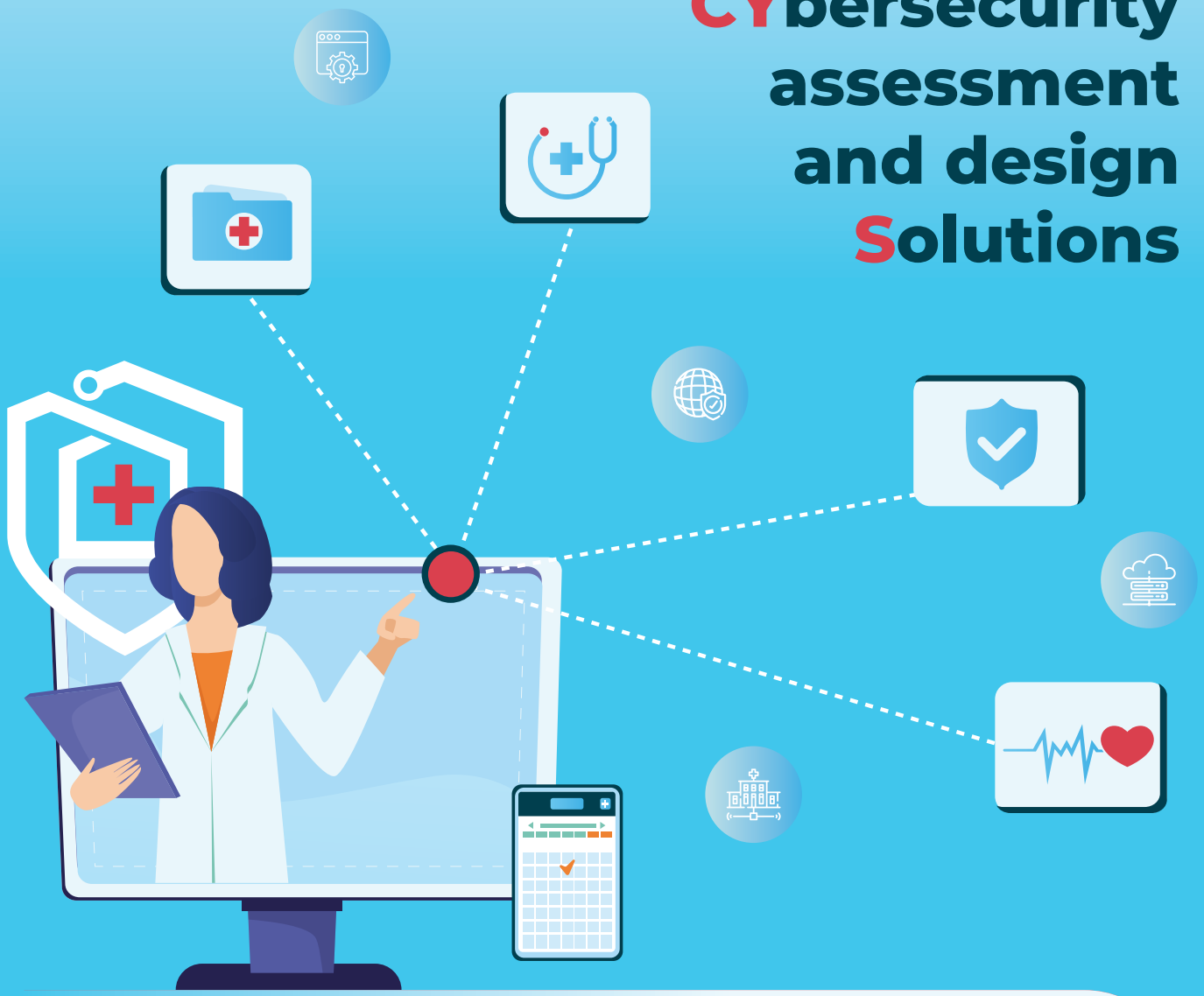
NEMECYS

New Medical Cybersecurity and design Solutions

NEw MEdical CYbersecurity assessment and design Solutions



NEMECYS Toolbox:

Secure IOT Service Mesh & Connector (SISMc)

Developed by Information Catalyst

The ICE Secure IoT Service Mesh (SISMc) is a cutting-edge solution designed to enhance security, observability, and compliance for IoT medical devices and applications. By integrating best practices from Istio and Kubernetes, SISMc provides mutual TLS encryption, access control, audit logging, network policies, and secrets management, ensuring secure service-to-service communication within a Kubernetes cluster.

A key feature of SISMc is its ability to serve as a secure gateway for IoT medical devices in environments where Kubernetes clusters and service meshes cannot be deployed such as patients' homes, remote clinics, or hospital settings. Using a Raspberry Pi - based prototype, SISMc enables end-to-end encryption for data in transit and at rest, protecting sensitive medical data from potential breaches.

Managing and securing a vast number of IoT medical devices presents a significant challenge. SISMc offers centralized device management, allowing for remote updates, patching, and security monitoring, reducing vulnerabilities from outdated software. It enforces network access policies, ensuring that only authorized devices can connect to hospital networks, mitigating security risks from rogue devices.

Unlike expensive proprietary solutions from major providers, SISMc leverages open-source technologies (Kubernetes, Helm, and Istio) to deliver a scalable, cost-effective, and continuously updatable integration framework for medical IoT applications.

SISMc empowers healthcare providers, software developers, and medical device manufacturers to focus on innovation while ensuring robust security, compliance (HIPAA, GDPR), and interoperability in connected healthcare environments.

Technical Inquiries for the Tool

If you are interested in learning more about the tool, its capabilities, or technical details, please contact **info@informationcatalyst.com, arturo.arriaga@informationcatalyst.com**

Scan to access the tool

www.nemecys.eu **@NEMECYS_eu** **nemecys-horizon-eu-project**

SINTEF · mode · IBM · ATC Athens Technology Center · ribera · I.R.C.C.S. Ospedale San Raffaele Gruppo San Donato · Med&Lab · ICE Information Catalyst · University of Southampton · pd neurotechnology medical solutions · DEBIOTECH

Co-funded by the European Union

The NEMECYS project is co-funded by the European Union under grant agreement ID 101094323, by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee grant numbers 10065802, 10050933 and 10061304, and by the Swiss State Secretariat for Education, Research and Innovation (SERI). The information and views set out in this publication are those of the author(s) only and do not necessarily reflect hose of the European Union, HADEA, UKRI or SERI. Neither the European Union nor the granting authorities can be held responsible for them.