FOR IMMEDIATE RELEASE

SEPTON Finalizes Cybersecurity Toolkit for Connected Medical Devices: Real-World Validation Phase to Begin

Athens, July 2025 — The **SEPTON project**, funded by the European Union under the Horizon Europe programme (Grant Agreement No. 101094901), proudly announces the finalization of its full suite of advanced cybersecurity tools. Designed to safeguard **networked medical devices (NMDs)** and the wider **Internet of Medical Things (IoMT)** ecosystem, the SEPTON toolkit is now entering its **real-world validation phase** across healthcare premises in Europe.

Cutting-Edge Tools for Medical Cybersecurity

Coordinated by **SPACE HELLAS SA**, the SEPTON project brings together a multidisciplinary consortium of 10 partners from five countries, uniting expertise in cybersecurity, medical IT systems, AI, edge computing, and healthcare delivery. The project has developed a **comprehensive cybersecurity framework** that includes the following main components:

🛡️ **1. Polymorphic Protection Agents**

- Self-morphing agents that dynamically change their attack surface to evade malware and intrusions.
- Deployed on medical device endpoints to ensure proactive protection.
- Compatible with embedded systems and constrained devices.

🧠 **2. Anomaly Detection Engine (Network and Device Level)**

- Based on **Deep LSTM Autoencoders**, trained on traffic data from **NetFlow** and **Zeek**.
- Detects anomalous behaviors and potential attacks on hospital networks in real-time.
- Incorporates **feature fusion** from structured and historical traffic to enhance accuracy.

⚙️ **3. Hardware Acceleration Tool**

- Deploys anomaly detection on **Jetson AGX Orin** edge devices using **ONNX** and **TensorRT**.
- Supports **quantized inference (FP16)** for optimized performance.
- Achieves **up to 5× inference speedup and 90% energy reduction** vs traditional architectures.
- Fully compliant with standards such as **IEC 62443**, **ISO/IEC 27001**, and **ISO 14971**.

🔗 **4. Secure Data Exchange Mechanism**

- Blockchain-based infrastructure for secure, traceable, and tamper-evident data sharing between NMDs.
- Supports smart contracts for data access governance.
- Integrates **differential privacy** and **encryption schemes** for confidentiality.

🔍 **5. NMD Vulnerability Assessment Tool**

- Provides a risk scoring engine for identifying known vulnerabilities in device firmware and software stacks.
- Uses CVE, SBOM, and firmware scanning mechanisms.
- Integrates into the SEPTON dashboard for real-time status reporting.

📊 **6. Centralized SEPTON Dashboard**

- Unifies visual analytics, alert management, device status, performance telemetry, and risk monitoring.
- Offers role-based access control and secure communication protocols.
- Supports plug-and-play integration with healthcare infrastructure.

Real-World Validation in Healthcare Settings

Following successful integration and internal testing, the complete SEPTON toolkit is now being prepared for **pilot deployment and validation** in operational environments. These include:

- **Erasmus Medical Center (NL)**: Focus on surgical robotics, implantable device traffic, and cross-network interoperability.
- **EBIT's PACS Environment Set Up (IT)**: Simulation of emergency scenarios and data analytics using real traffic.

The validation phase will assess the **technical, functional, regulatory, and usability** readiness of each SEPTON tool under real-life operating conditions, with a focus on interoperability, resilience, and regulatory alignment (e.g. MDR, GDPR, NIS2 Directive).

A Major Step Toward Cyber-Resilient Healthcare

SEPTON's mission is to empower European healthcare systems with **cybersecurity-by-design capabilities**, enabling them to anticipate and neutralize cyber threats while preserving the safety and privacy of patients. The project supports the EU's broader ambition for **digitally sovereign, safe, and interoperable healthcare infrastructures**.

About SEPTON

SEPTON (Security Protection Tools for Networked Medical Devices) is a 36-month Research and Innovation Action (RIA) under the **HORIZON-HLTH-2022-IND-13** call. With a total funding of nearly €5 million, the project develops next-generation solutions for threat detection, prevention, and response tailored to the realities of modern medical environments.

Contact Information:
Project Coordinator – SPACE HELLAS SA
Email: npap@space.gr
Website: www.space.gr