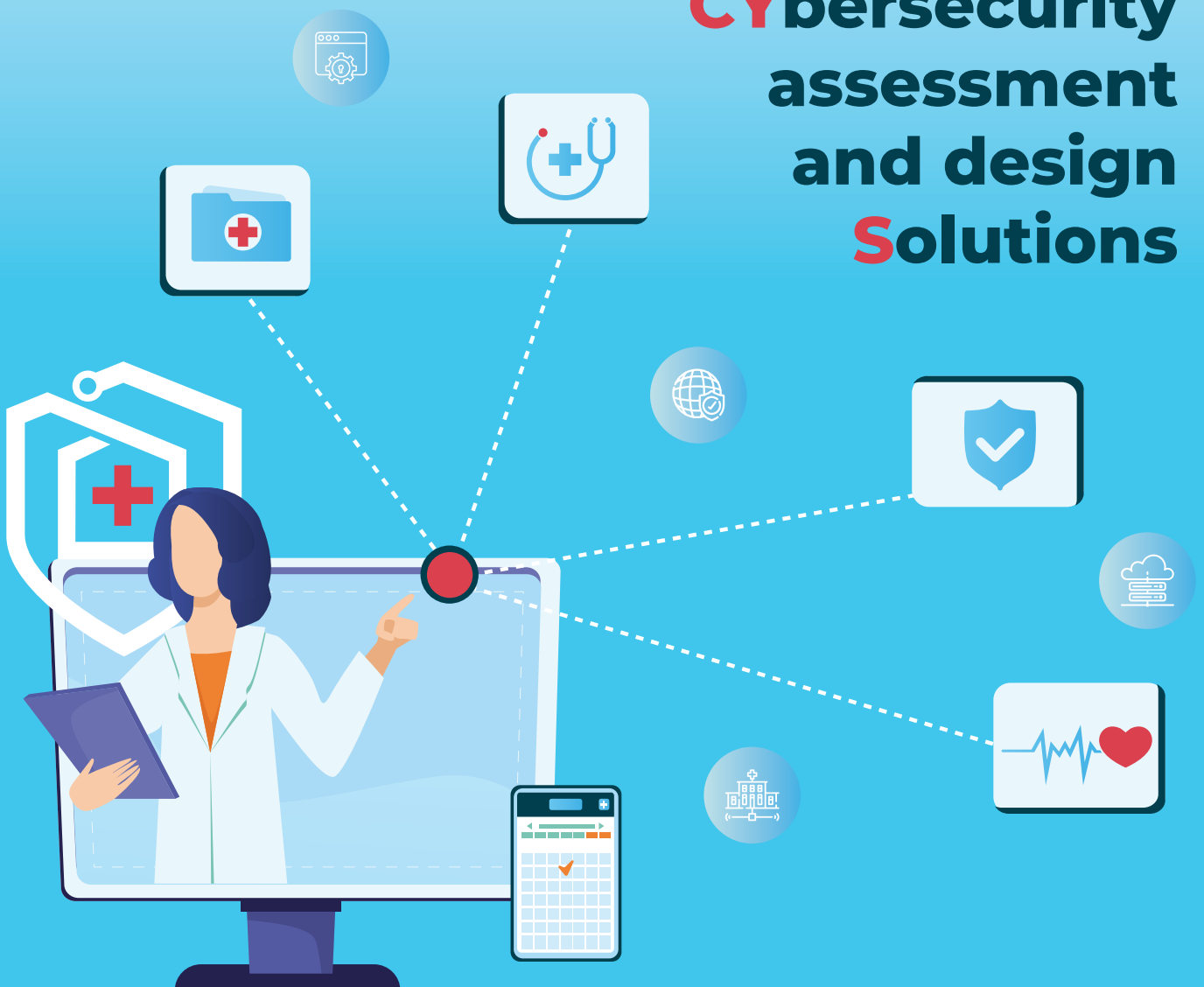




# NEMECYS

NEW MEDICAL CYBERSECURITY AND DESIGN SOLUTIONS

## **NEW** **ME**dic **CY**bersecurity assessment and design **S**olutions



### **NEMECYS Toolbox:** Network Assessment Tool

Developed by ATC

The Network Assessment Tool (NATool) was developed by ATC in the framework of the NEMECYS project to support the security evaluation of medical device networks by providing an all-in-one tool for device discovery, risk assessment, and traffic analysis. Designed for use by network administrators, cybersecurity professionals, and device vendors, NATool offers comprehensive visibility into connected assets and their exposure levels.

By performing active scans to detect devices, fingerprint services, and match known vulnerabilities (via the CVE database), it enables early identification of potential security risks. NATool also passively captures and analyzes network traffic through mirror ports, correlating communication patterns with external threat intelligence such as IP blacklists and metadata enrichment. This allows users to detect malicious activity or policy violations in real time.



Results are presented in structured PDF and JSON reports, supporting both human-readable insights and seamless integration into the broader NEMECYS platform.

NATool contributes to platform-wide cybersecurity assurance by supplying key indicators to other NEMECYS tools, enabling collaborative risk mitigation and regulatory readiness.



### Technical Inquiries for the Tool

If you are interested in learning more about the tool, its capabilities, or technical details, please contact [a.mpantis@atc.gr](mailto:a.mpantis@atc.gr) | [g.zissis@atc.gr](mailto:g.zissis@atc.gr)



Scan to  
access  
the tool

[www.nemecys.eu](http://www.nemecys.eu)

 [@NEMECYS\\_eu](https://twitter.com/NEMECYS_eu)

 [nemecys-horizon-eu-project](https://www.linkedin.com/company/nemecys-horizon-eu-project)



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 those of the European Union, HADEA, UKRI or SERI. Neither the European Union nor the granting authorities can be held responsible for them.