

LIST OF FLEXIBLE ACTIVITIES

CORP CYS TEST LAB

WORKPLACE:

Siemens Healthcare, s.r.o.

Lamacska cesta 3/B, 841 04, Bratislava, ID No.:48146676

Offensive Security Testing

Cyber Security Testing Laboratory (CORP CYS TEST LAB)

Lamacska Cesta 3/B, 841 04, Bratislava

Item	Subject of testing		Established method		Technology and testing tools
	Subject category:	Properties	Principle	Method and Standard Designation	
1.	Hardware, Software electronic devices, equipment, imaging technology, medical devices and assistive technology, RED ¹⁾	Identification and vulnerability scanning.	External and Internal Penetration Test (qualitative)	EN 18031 -1 EN 18031 -2 EN 18031 -3 NIST SP 800-115 NIST SP 800-53 OWASP NIS2 SANS 25 PTES	hardware and software, Network scanners, attack simulators
2.	Information and communication technology and network component products, including infrastructure ²⁾	Cryptographic elements of cybersecurity			

Classification:
Unrestricted

This document is managed in electronic form. The printed version is a copy and is an unmanaged document.

Effectivity:
08.09.2025

Categorization of flexible activities

Detailed specification of test subjects

Item No. 1 of the Scope of Accreditation Hardware, software of electronic devices, devices, imaging and medical devices and technology, RED equipment¹	
Category	Medical devices and technology
Subcategory	Medical devices, imaging technology and medical electronic devices
	Angiograph, Computed Tomography, Fluoroscope, Magnetic Resonance Imaging, Mammography, Mobile C Arm, Ultrasound, Robotic X-ray, Uroscopy, Electrocardiographs (ECG), Infusion Pumps, Vital Signs Monitors, Vascular and Cardiac Surgical Devices, Dialysis Equipment, Inhalation Devices, Robotic Surgical Systems, Advanced Diagnostic Systems with Artificial Intelligence, Electronic Implants.
Subcategory	Medical Sensors & Diagnostic Systems
	Optical sensors, ultrasonic sensors, temperature and humidity sensors, automatic analyzers, laser systems, navigation systems, signal analyzers
Category	Other electronic devices
Subcategory	Personal computers (PCs) and servers
	Basic Computing Units, Database Servers MS SQL, MYSQL, PostgreSQL, SQLite, MongoDB, Proxy Server
Subcategory	Computer Accessories
	Keyboards, mice, monitors, printers, scanners, external hard drives, USB devices.
Subcategory	Mobile devices
	Mobile phones, tablets, laptops, smartwatches.
Subcategory	Imaging devices
	Monitors, projectors, screens for interactive whiteboards, virtual and augmented reality (VR/AR) devices
Subcategory	RED (Radio Equipment)
	Mobile Phones, Wi-Fi, Bluetooth, Drones (RPAS – Remotely Piloted Aircraft Systems), Internet of Things (IoT) Devices, GPS, Radio Transmitters and Receivers, Wi-Fi Cameras, Audio Devices, Car Radio Communication Devices, Healthcare Radio Equipment, Smart TVs and Portable Multimedia Devices, Smart Home Devices, Radar Systems
Subcategory	Other devices
	Electronic Voting Systems, Internet of Things (IoT), Biometric Devices, Credit Cards and Payment Terminals,

Classification:
Unrestricted

This document is managed in electronic form. The printed version is a copy and is an unmanaged document.

Effectivity:
08.09.2025

Item No. 2 of the Scope of Accreditation Information and communication technology and network component products, including infrastructure ²	
Category	Information and communication technologies AI
Subcategory	Medical & Laboratory Systems
	Laboratory Information System (LIMS), Healthcare Information Systems (HIS), Pharmacy Information Systems (ePharmacy), Electronic Health Records (EHR), Patient Monitoring Systems, Telemedicine Systems
Subcategory	Personal Data Management Systems (DMPs)
	Customer Data Management Systems (CRM), Employee Data Processing Systems, Payment and Transaction Processing Systems, Banking Systems, Insurance and Pension Systems, Email Management Systems, Secure Communication Applications, Tax and Legal Data Management Systems, Legal Information Systems, Educational Data Management Systems (LMS), Autonomous Vehicle Systems, Government Systems
Subcategory	Monitoring systems and Big Data
	CCTV & Video Surveillance Systems, Facial Recognition Systems, Access Control Systems, Big Data Processing Systems, Social Media Data Processing Systems, Biometric Authentication Systems, Security Monitoring Systems (SIEM Security Information and Event Management, IDS/IPS Intrusion Detection/Prevention System), VPN (Virtual Private Network), Virtual Private Networks (VPN, VLAN)
Subcategory	Network Components and Infrastructure
	Network Devices (Routers, Switches, Gateways, Access Points (Wi-Fi Access Points) of the network Firewall a security Equipment (Firewall, NAT equipment (Network Address Translation) IDS/IPS (Intrusion Detection and Prevention Systems) Network cables and optical devices (Ethernet cables (e.g. CAT5e, CAT6, CAT7), Optical fibers, SFP modules and interconnects Physical & Virtual Devices (Test Server, Virtual Machines, Various Network Devices (Routers, Firewalls, Switches, Servers) & Connected Devices (IoT), Cloud Systems,
Subcategory	Communication and Service Technologies
	Hyperconverged Infrastructures (HCI), Network Virtualization (SDN – Software Defined Networking), Wireless and Mobile Communication Technologies (5G and LTE technologies, Wi-Fi 6, Bluetooth and Zigbee), Public Communications Networks and Services
Subcategory	Network Management and Monitoring Systems
	Tools for network management and configuration (Network Management Systems (NMS), Network Configuration Management, Tools for monitoring network performance (Bandwidth Monitoring, Latency and Jitter Monitoring)
Subcategory	Security solutions for network and data protection
	VPN (Virtual Private Network), Encryption Devices, DLP (Data Loss Prevention) and SIEM (Security Information and Event Management), Cloud Infrastructure and Services (IaaS Infrastructure as a Service, PaaS Platform as a Service, SaaS Software as a Service, CDN (Content Delivery Networks) and Edge Computing, Data Storage (SAN Storage Area Network, NAS Network Attached Storage), Data Center Management.

Classification:
Unrestricted

This document is managed in electronic form. The printed version is a copy and is an unmanaged document.

Effectivity:
08.09.2025

Subcategory

Desktop, mobile, Web applications

Business Web Applications, Customer Web Applications, IoT Web Applications, Interactive Collaboration Applications, Data Analytics & Processing Applications, Content Management Applications (CMS), Public Web Applications, Private Web Applications, Web Services (API), Progressive Web Apps (PWA), Single Page Applications (SPA), Static & Dynamic Web Applications, Windows Applications, Linux Applications, Android Applications, iOS/Apple Applications.

Detailed specification of properties

Category:

Vulnerability identification and scanning

Network Scanning, Port & Service Scanning, Fingerprinting & OS Detection, Vulnerability Scanning, Web Vulnerabilities, Configuration & Compliance Scanning, Code Scanning (Static Analysis), OSINT & Passive Information Acquisition, Manual Vulnerability Testing, Cloud & Container Scanning

Category

Cryptographic elements of cybersecurity

Symmetric Cryptography, Asymmetric Cryptography, Hash Algorithms, Digital Signatures, Certificates and PKI (Public Key Infrastructure), Cryptographic Protocols, Key Generation and Management, Authentication Mechanisms, Homomorphic Encryption and Post-Quantum Cryptography

Specification of Test Methods

Method used: Edition r. /version v.

EN 18031 -1: 2024

EN 18031 -2: 2024

EN 18031 -3: 2024

NIST SP 800-115, last update 04.05.2021

NIST SP 800-53, Revision 5 (December 2020)

OWASP: 2025

SANS 25: 2021

PTES: 2020

NIS2: 2023

Last change date: 02.09.2025

Change made by with Effectivity: 08.09.2025

The content was created, reviewed and checked by:

Created by



Electronically signed by: Stanislav Mikusinec
Reason: I am the author of this document
Date: Sep 2, 2025 14:37:22 GMT+2

Reviewed by



Electronically signed by: Viktor Krostofak
Reason: I have reviewed this document
Date: Sep 2, 2025 14:39:01 GMT+2

Checked by



Electronically signed by: Jan Majors
Reason: I am approving this document
Date: Sep 3, 2025 06:43:37 GMT+2

Classification:
Unrestricted

This document is managed in electronic form. The printed version is a copy and is an unmanaged document.

Effectivity:
08.09.2025

Contacts: First contact with the customer (Pentest Request Form)
Ing. Alzbeta Vojtusova – Test coordinator alzbeta.vojtusova@siemens-healthineers.com
Ing. Tomas Vojtkovsky – Test coordinator tomas.vojtkovsky@siemens-healthineers.com
Flexible scope Management Ing. Stanislav Mikusinec – Quality Manager, Flexible Scope Manager stanislav.mikusinec@siemens-healthineers.com

Warning

In order to maintain the integrity and nature of the testing, it is not possible to disclose the specific type of hardware and software equipment used by the laboratory. This data is considered strictly confidential.

Legend:

Category
Subcategory
Items
Added new activity
Delete an activity

Explanatory notes:

Hardware includes physical components that perform calculations, processing, and displaying information. In this category are devices and technology that are physically present and interact directly with the software.

Software includes applications and programs that control the operation of hardware, enable data processing, communication between devices, and provide a user interface.

External penetration test – is a simulated cyber-attack carried out from an external environment (i.e. the Internet), which aims **to test the security of the client's publicly available systems**.

Internal penetration test - is a simulated cyber-attack **from inside the organization**, carried out from the position of an employee, supplier or attacker who already has access to the internal network.

Classification:
Unrestricted

This document is managed in electronic form. The printed version is a copy and is an unmanaged document.

Effectivity:
08.09.2025