CYBER THREATS IN HEALTHCARE AND WAYS TO RESPOND

SGS DIGITAL TRUST SERVICES FOR MEDTECH PRODUCTS

Medical systems and devices have become more and more connected and interoperable. Simplified patient and patient-data-management, real time availability of diagnostic data across hospital networks, and new remote monitoring features are significantly increasing effectiveness and efficiency in healthcare. The advantages provided are many. However, connected MedTech products and systems are prone to cyber security threats.

In fact, medical systems and hospital networks have become one of the most attractive targets for hackers. Why? One reason is that the data in the systems is very valuable. Medical records can be stolen and sold; social security numbers and respective identities can be misused to generate financial gain. Hospital networks are part of critical infrastructure. Availability and performance of such systems is key, making equipment attractive to digitally hold for ransom.

Unnoticed digital manipulation of products and systems can lead to fatal situations. Security researchers have shown several times how to hack pacemakers or insulin pumps. The WannaCry worm incident in 2017 was an eye opener. In the United Kingdom, NHS stroke centers had to close, surgeries had to be postponed. Thousands of patients were heavily affected. The threats are real, and actions have to be taken.

RESPONSES TO CYBERSECURITY THREATS

Worldwide, regulators are adopting MedTech standards and conformance requirements by adding cybersecurity requirements to national and regional product approval criteria. The FDA has published guidance documents on Premarket and Postmarket Management of Cybersecurity in medical devices and is encouraging manufacturers to provide according evidence. In Europe, the new EU Medical Device Regulation 2017/745, coming into effect in 2020, is mandating cybersecurity requirements to be considered. Furthermore, the European Cybersecurity Act and General Data Protection Regulation are increasing the pressure on introducing security certification for medical products.

Manufacturers, have so far focused on functionality, performance and functional safety of products. Now they also need to consider cybersecurity throughout a product's life cycle. This is not an easy thing to do. "Security by design" requires dedicated knowledge and is impacting the complete development process from product definition to release, along with product maintenance in the field through product disposal. The interaction with component suppliers is heavily affected as well.

SGS SOLUTIONS

SGS has united all its existing cybersecurity capabilities under a single umbrella – Digital Trust Services (DTS). DTS covers a full range of product and system related cybersecurity services for the medical device industry:

CYBERSECURITY BY DESIGN – METHODOLOGIES

- Tailored trainings introducing methodologies that support a secure development lifecycle
- Trainings introducing best practices for cybersecure IoT development

CUSTOMER SPECIFIC SECURITY ASSESSMENTS AND SECURITY REVIEWS

- Gap Assessments
- Tailored security assessments and reviews
- Cybersecurity testing and pre-testing services

PRODUCT EVALUATION AND CERTIFICATION SERVICES

- Cybersecurity assessment to ISO 14971 offering risk management reviews/audits where cybersecurity threats are generating safety risks requiring mitigation
- Security audits related to information security requirements listed in the new EU Medical Device Regulation 2017/745
- Product security assessment and certification based on vertical agnostic lightweight security certification schemes as there are:
  - LINCE introduced by the Centro Criptológico Nacional (CCN), Spain
  - BSZ introduced by the Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany
  - FDA recognized cybersecurity testing per UL 2900 standards
- Security Evaluation according to ISO/IEC 15408 Common Criteria, supported by global (CCRA) and European (SOG-IS) recognition agreements

WHY SGS?

SGS established a highly experienced team of security experts with a strong background in security certification of products and systems ranging from semiconductor level, across integration steps up to system and network level.

SGS DTS provides a one-stop-shop approach for all cybersecurity matters. Together with the SGS Electro-Medical team, SGS offers medical device manufacturers a globally integrated solution to get their new devices to market faster.

SGS plays an active role in multiple standard committees, certification scheme development and is a member of various industry groups. The global network, extensive resources, and expert knowledge across all technical domains and industry segments give SGS the expertise to provide large and small manufacturers with reliable services.

SGS is the world's leading inspection, verification, testing, and certification company. Recognized as the global benchmark for quality and integrity, SGS employs 97,000 people, and operate a network of more than 2,600 offices and laboratories worldwide.

FOR MORE INFORMATION, PLEASE CONTACT:

Email: digitaltrustservices@sgs.com

SGS IS THE WORLD'S LEADING INSPECTION, VERIFICATION, TESTING AND CERTIFICATION COMPANY

WHEN YOU NEED TO BE SURE

SGS