Medical Device Cyber Security and Compliance

Overview

Since 1997, SPK & Associates, LLC has been providing engineering-based information system services to the medical device manufacturing industry -- from Fortune 100 to small and medium enterprise.
Unlike standard or corporate IT providers, our solutions unleash a new paradigm that help companies develop innovative products faster, with lower cost, higher quality, and improved customer experience.

Overview

The FDA has recently updated its original 2014 guidance regarding Premarket Submissions for Management of Cyber Security for medical devices. SPK can help your company better align to this guidance – ensuring comprehensive security for your device and avoiding delays in your product release.

SPK works closely with your product development teams to help you achieve a level of security and compliance that's right for you. Our engineers have deep expertise in cyber security, along with decades of network and systems experience. This knowledge, along with over 20 years of Medical Device industry experience with Fortune 500 and SMB companies, will get your device on the fast track to market.

SPK has accredited CREST Security Analysts on staff. CREST examinations are recognized by the professional services industry and buyers as being the best indication of cyber security knowledge, skill and competence.

Cyber Security Risk Assessment

The FDA's recent guidance update strongly recommends that each 510(k) include a Cyber Security Risk Assessment. Working with either your existing product, or one that is currently in R&D, we can create this assessment for you, which includes:

- Penetration Testing
- Vulnerability Inventory
- Threat Event Assessment
- Threat Source Assessment
- CVSS Assessment
- Cyber Security Risk Assessment, 510(k)-ready

We'll analyze for applicable threats, combine them with your Risk Controls, and provide an in-depth view of the risk profile of your product.

Vulnerability Testing During Your Product Development Cycle

One mistake made by med device manufacturers, is to wait too long before incorporating required cyber security testing in

the product development process. We recommend weaving vulnerability testing into your R&D processes early. SPK has experience with the following vulnerability scanners:

- Qualys
- Metasploit
- Nexpose
- Nessus/OpenVAS

However, running a scanner isn't where our value shines. SPK can help you architect a secure device, provide assistance with vulnerability remediation, or audit existing med device systems and software to ensure that you're protected.

Operating System Security

Vulnerability testing also includes testing and remediation of operating system components. We have engineers that are well versed in this area for both Microsoft Windows and Linux operating systems.

- PatchTesting
- DIACAP/NISTFrameworkTesting
    - NIST STIG Checklist
- Hardened / Best Practice Configurations for:
    - Windows Embedded
    - Linux
- Anti-Virus & Malware Protection

HIPAA Compliance

Whether in the cloud, or on-prem, SPK can assist you in implementing a HIPAA compliant solution. SPK has years of experience in dealing with 45 CFR Part 164 requirements regarding encryption, monitoring, AAA, and DR/backup. We understand the HIPAA system requirements and are able to ensure that your device and system are technically compliant.

Our Success Stories

Fortune 500 Medical Device Manufacturer

SPK's customer had developed an inter-operating room product that utilized multicast video streaming. This product was initially developed in a controlled lab network that SPK had managed. After it was released and deployed, SPK continued to assess the system for cyber security vulnerabilities and provide Cyber Security Risk Assessments for each updated release.

SPK has also independently created and executed risk assessments for other medical device products, some while in R&D, others post market.

For more information
Please contact sales@spkaa.com or
visit https://www.spkaa.com/contact
1-888-310-4540