SAN FRANCISCO
EVENTS LIST

FDA's Software Monsters: Cybersecurity, Interoperability, Mobile Apps and H...

Date : Jan 18, 2018 - 09:00 AM - Jan 19, 04:30 PM

Event URL : http://www.sfbayeventslist.com/events/fda-s-software-monsters-cybersecurity-interoperability-mobile-apps-and-h-1510688961

Organizer : Netzealous LLC - NewYorkEventsList

Venue :

Location : DoubleTree by Hilton Hotel San Diego Downtown1646 Front StreetSan Diego, CA 92101United States,
San Diego, CA , US, ZIP: 92101

Description

***** LIMITED TIME OFFER: FREE $100 AMAZON GIFT CARD! *****
REGISTER TODAY!

Software's level of complexity and use is expanding at exponential levels. Likewise, the potential risks to health follow suit. Ransomeware attacks hold your software hostage until you pay hundreds or thousands of dollars. Life supporting and life sustaining healthcare grinds to a halt.

www.sfbayeventslist.com

Extracting personal healthcare information is another plague that has a huge financial incentive for hackers. Your software is running on thin ice.

The FDA looks at software in one of three ways: Standalone, such as for a mobile app; device-based software used to control a device's performance, or simply electronic records. FDA's risk classification will gradually clarify how it intends to manage the health risks with premarket and postmarket controls. What the FDA did not see was the cancer of cybersecurity attacks, the failure of interoperability, and the explosion in the use of wireless communication and mobile apps.

Inadequate cybersecurity programs and the lack of interoperability for healthcare users pose the greatest threat to any healthcare system. Software exploitations are using more sophisticated approaches and the hackers' programs are readily available on the "dark web."

The increasing sophistication required to protect software programs and have them work with other programs requires progressive software design and software validation considerations. In many instances, validation is limited to the immediate use of the software rather than its environment of use, its performance with other software programs and software hacking. FDA can ask you what you have considered before you take a product to market. Whether your software can survive unscathed is another question. When software causes a problem, fixing the malfunction or "bug" may be more difficult as software becomes more sophisticated, customized by users and placed in a network system. In these kinds of circumstances, it is difficult to decide who is responsible for managing and fixing the software problems, preventing them from recurring. This becomes a major regulatory headache for FDA and generates business-to-business conflicts. When firms are designing and marketing software, they should be mindful of the unknowns that lurk in the future of software regulated as a device by the FDA.

Why you should attend:

For decades, firms have experienced serious problems with software and have been at a loss to make a well-informed follow up. Software problems represent one of the most common root causes for recalls that are associated with deaths and serious injuries beyond what should be necessary to quantify. FDA sees firms revise software only to create more problems rather than solve them. The infusion pump industry is a classic example that drove FDA to implement a new rigorous paradigm for premarket review and performance criteria evaluation.

The growth of the medical software industry outpaces how FDA's regulatory process is designed. How can you anticipate and defend against the malicious remote hacking and shut down of an insulin infusion pump? In some instances, clinicians have weighed the risk of software failure against the benefits of using a device at all. You need to understand and apply the current provisions that NIST has put forth in recent reports FDA will integrate them into its regulatory oversight of cybersecurity management.

Device software is often used in conjunction with other software-based devices, but their interoperability was never anticipated. Can one software program defeat the performance

capability or back up safety features of another software program? When interoperability problems surface, which software manufacturer takes the lead to solve the problem and deal with proprietary software issues?

These are the kinds of issues that will be highlighted during the seminar. The issues require careful consideration even though no obvious answer appears at hand.

Topics:

- FDA's risk-based regulatory strategy
- Cybersecurity
- Interoperability
- National Institute of Standards and Technology
- Voluntary standards and programs
- Mobile Apps
- Premarket software validation and design requirements
- Postmarket Software recalls

Who Will Benefit:

- Regulatory Affairs
- Quality Assurance
- Software Design Engineers
- Manufacturing
- Complaint Dept.
- Hospital Risk Dept.
- Own label marketers

Event Categories :