timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

ICS

WEBINAR WORKBOOK

The Real-World Challenges of Medical Device Cybersecurity:
***MITIGATING* VULNERABILITIES**

WORKBOOK CONTENTS

Welcome to today's webinar on the critical subject of medical device cybersecurity. As we delve into the challenges and regulatory requirements, use this workbook to guide your learning and note-taking.

WEBINAR SPEAKERS

Director of Medical Programs and Cybersecurity for ICS

Milton Yarberry

Milton is a certified PMP and Scrum Master with a background in software architecture, medical device product development and program management. He has 20 years in product development with 10 years in software consulting and 15 years working with Class II and Class III medical device manufacturers.

ICS

ICS specializes in software architecture, medical device product development, and program management.

Vice President of EMEA Business Development & Technical Sales

Maciej Halasz

Maciej has more than 25 years of experience in embedded computing with a focus on embedded Linux and real-time systems. The creator of Timesys University embedded Linux workshops and the co-host of LinuxLink Radio, Maciej has also authored numerous embedded Linux and industry articles.

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

Timesys is a leader in embedded computing, particularly embedded Linux and real-time systems.

SELF-ASSESSMENT QUIZ

The following is a series of questions to help identify where you're at in the cybersecurity and regulatory process. You can fill these out here or during the webinar when the polls appear. We'll share the results of the polls during the webinar as well, so you can see industry trends.

01 **Are you familiar with the details of Section 524B of the FD&C Patch Act and its implications for medical device cybersecurity?**

- ○ Yes, fully aware
- ○ Somewhat aware
- ○ Not aware

02 **Which mitigation technique do you find most effective in your current cybersecurity practice?**

- ☐ Threat modeling
- ☐ Architectural controls
- ☐ Penetration testing
- ■ Other

03 **What is your biggest challenge in meeting and complying with evolving global cybersecurity regulations?**

- ☐ Staying updated and informed about the changes
- ☐ Understanding the regulations
- ☐ Implementing the necessary controls
- ☐ Lack of resources
- ☐ Other

04 **How prepared is your organization to meet the FDA's new cybersecurity reporting requirements?**

- ○ Fully prepared
- ◉ Adequately prepared
- ○ Unprepared

SELF-ASSESSMENT QUIZ CONTINUED

03 **Does your organization use open-source software in the development of medical devices?**

- ○ Extensively
- ○ Understanding the regulations
- ○ Not at all and not considering
- ○ Not at all but considering
- ◉ I don't know

02 **Have you produced a Software Bill of Materials (SBOM) for any of your products?**

- ○ Yes, produced internally
- ○ Yes, outsourced
- ◉ No, we don't have an SBOM
- ○ N/A

02 **Do you have a process for managing CVES (Common Vulnerabilities and Exposures)?**

- ○ Yes, we check CVEs internally
- ○ Yes, we outsource CVE management
- ◉ Penetration testing
- ○ N/A

03 **What are your biggest concerns and challenges complying with section 524B of the FD&C act?**

- ☐ Creating SBOMs
- ☐ Implementing an SPDF
- ☐ Achieving FDA cybersecurity compliance
- ☐ Understanding cybersecurity standards
- ☐ Preventing your system from being hacked

OVERVIEW OF CYBERSECURITY REGULATIONS

Key Takeaways:

Recent legislation, specifically [_____] of the [_____] , mandates [_____] cybersecurity measures for medical devices.

Understanding these regulations is crucial to ensuring your medical products are [_____] and [_____] with the latest FDA mandates.

Notes:

What are your initial thoughts on the impact of these regulations on your current projects?

ANSWERS: Section 524B / FD&C Patch Act / stringent / secure / compliant

MANAGING VULNERABILITIES

Key Takeaways:

Key processes for managing vulnerabilities include identifying [_____] of vulnerabilities and solutions.

It's essential to describe methods for [_____] mitigations with depth around the software bill of materials.

Notes:

Reflect on the vulnerability management techniques you currently employ:

ANSWERS: Categories / applying

THE ROLE OF SBOMS

Key Takeaways:

The [_____] (SBOM) plays a crucial role in your cybersecurity strategy by providing a comprehensive list of all software in your product.

SBOMs help organizations respond quickly when [_____] are known against any components listed.

Notes:

How do you foresee implementing or improving SBOM usage in your workflow?

ANSWERS: Software Bill of Materials / vulnerabilities

CYBERSECURITY REPORTING TO THE FDA

Key Takeaways:

Navigating cybersecurity reporting involves organizing and presenting information on how vulnerabilities are [_____] and [_____].

This reporting is crucial for demonstrating compliance and securing product approval from the FDA.

Notes:

Consider any potential challenges you might face in this reporting process:

ANSWERS: Mitigated / justified

VULNERABILITY MITIGATION TECHNIQUES

Key Takeaways:

Effective vulnerability mitigation techniques include [_____], [_____], and applying [_____].

The FDA expects manufacturers to have comprehensive architectural views, including:

1.
2.
3.
4.

Notes:

What mitigation techniques have been most effective in your organization?

ANSWERS: threat modeling / risk assessment / architectural controls / global system view / multi-patient harm view / updateability view / security use case views

LONG-TERM OS MAINTENANCE & MONITORING

Key Takeaways:

Long-term OS maintenance is vital for ensuring the security of medical devices throughout their lifecycle.

Regular monitoring of the Software Bill of Materials against [_____] (NVDs) helps manufacturers stay ahead of potential threats.

Notes:

How does your organization handle long-term maintenance and vulnerability monitoring?

ANSWERS: National Vulnerability Databases

WEBINAR FAQ

01

What is the most critical factor in maintaining compliance with recent cybersecurity legislation?

Understanding and integrating the requirements into the development and maintenance of medical devices is crucial. The roles of SBOMs and vulnerability management is especially critical.

02

How often should SBOMs be updated?

SBOMs should be updated whenever there is a significant change to the software components of a product, such as updates or patches, or when new vulnerabilities are identified.

03

What are the best practices for threat modeling in medical devices?

Best practices include using standardized methodologies, involving cross-functional teams in the threat modeling process, and regularly updating the threat models as the system evolves.

04

How can I ensure my device remains secure throughout its lifecycle?

Implementing a robust post-market vulnerability management plan, conducting regular security audits, and keeping abreast of the latest security advancements and vulnerabilities are essential strategies.

05

What should I do if I find a vulnerability in a product after the product has gone to market?

It's important to assess the risk associated with the vulnerability, apply interim controls if necessary, develop a mitigation plan, and communicate with customers and regulatory bodies in compliance with your post-market vulnerability management plan.

KEY TERMS GLOSSARY

Section 524B of the FD&C Patch Act:

Legislation mandating cybersecurity measures for medical devices.

Software Bill of Materials (SBOM):

A comprehensive list of all software components in a product, used to manage cybersecurity risks.

Vulnerability Mitigation:

Actions taken to reduce or eliminate the risks associated with cybersecurity threats.

Architectural Controls:

Security measures that are incorporated into the design and architecture of software systems.

Cybersecurity Compliance:

Adherence to laws, regulations, and guidelines put in place to protect the integrity, confidentiality, and availability of information from attack, damage, or unauthorized access.

National Vulnerability Database (NVD):

A U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).

Threat Modeling:

A process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and prioritized.

Risk Assessment:

The overall process of risk identification, risk analysis, and risk evaluation.

Penetration Testing:

A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques an adversary might.

FD&C Patch Act:

Federal legislation that addresses cybersecurity risks in medical devices by enforcing specific security standards and practices.

Post-Market Vulnerability Management Plan:

A strategy that outlines how a company will manage vulnerabilities in its products after they have been released to the market.

Secure by Design

A principle in software and hardware engineering that emphasizes security in the design phases of development, and a requirement of the US National Cybersecurity Strategy.

ADDITIONAL RESOURCES

For further assistance and detailed queries, feel free to contact:

ICS.com

Integrated Computer Solutions (ICS)
Specializes in software architecture and medical device development.

Timesys.com

Timesys, a Lynx Software Technologies company, is an industry leader in open source software security, development tools, and engineering services in embedded computing and cybersecurity.

Visit our websites for more resources and information on available services.

REGULATION REFERENCES

FDA Cybersecurity Guidelines & Updates

Take some time to review in detail the cybersecurity guidelines and updates from the FDA here: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

US National Cybersecurity Stragety

The US National Cybersecurity Strategy can be found here: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

"Refuse-to-Accept" Section 524B of the FD&C Act

For more details on the new "refuse-to-accept" policy, see here: https://www.skadden.com/-/media/files/publications/2023/04/privacy-and-cybersecurity-update/guidancecybersecuritydevicesrta.pdf

Cybersecurity in Medical Devices FAQ

The FDA offers an FAQ on their new cybersecurity policies here: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

FDA Cybersecurity OTS Software Policy

The FDA cybersecurity guidance document for Networked Medical Devices Containing Off-the-Shelf (OTS) Software is found here: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software