POST WEBINAR Q&A

Cybersecurity & Hidden Threats in Medical Devices

1. TIR57 suggests doing a cost/benefit analysis to determine if the overall benefit risk is acceptable. Could you touch upon how this would or should be linked to the residual safety benefit risk? What would be the recommendation to merge this if it would be the suggestion?
TIR57 emphasizes that cybersecurity risks should not be evaluated in a vacuum. Instead, they should be integrated with the device's overall safety and performance risk profile — the same way you would evaluate any residual risk after mitigation in traditional safety engineering. TIR57 Section 6.6: suggests that if residual cybersecurity risks remain after applying controls, manufacturers should perform a benefit-risk assessment to determine if the residual risk is acceptable. You can reference ISO 14971 for help mapping residual risks to potential safety or clinical performance harms.

2. What technical challenges can we face with interoperability between different SBOM standards?
The two most prominent SBOM formats are CycloneDX and SPDX. There are open-source tools available to translate from one format to another (https://github.com/spdx/cdx2spdx?utm_source=chatgpt.com). If you are looking to integrate two SBOMs of different formats, you can import both in the Vigilant Ops platform and link them through the interface. Vigilant Ops handles formatting differences and interoperability behind the scenes.

3. Can you please discuss PenTesting as part of the CybSec requirements, and what may be expected for SaMD manufacturers, and/or what is typically seen?
Penetration testing simulates real-world attacks on a device or its supporting ecosystem to identify exploitable vulnerabilities. It is typically manual or semi-automated and goes beyond static scanning. FDA does not mandate pentesting, but recommends that manufacturers consider using it. For SaMD manufacturers, pentesting reports are usually included in the premarket submission documentation. In regions outside the US, there has been discussion about including pentesting reports in cases where identified product vulnerabilities are beyond a certain level of criticality.

4. Where can you read more about cybersecurity on a high level? Can you recommend any platforms or publications?
If you're looking for high-level cybersecurity insights (not too technical but still insightful), here are some great platforms and publications to follow: Cybersecurity & Infrastructure Security Agency (CISA) – Government resource for cyber threats, best practices, and guidelines. Cyber Defense Magazine - Covers global cybersecurity trends and best practices. Help Net Security - Covers cybersecurity trends, vulnerabilities, and industry news. Gartner - Business and strategy-focused security research.

5. What additional security risk does using AI in the software pose?
AI introduces new and increased cybersecurity risks that can affect data integrity, system trustworthiness, and even patient safety. Check out AAMI TIR34971:2023 – Application of ISO 14971 to Machine Learning in Artificial Intelligence for how to apply the risk management framework to AI/ML devices.

6. How do you delineate between a vulnerable that is 'critical' and a vulnerability that is minor, if there are 70+ vulnerabilities a day - do you have a framework suggestion for this?
Vulnerabilities are analyzed and scored by NVD or the vendor of the software component, but this score might not actually reflect your product's use of the given software component. We recommend examining the utilization of the software component in your product to assess a criticality that makes sense. This is accomplished through an understanding of your product functionality and the presence of mitigation controls to address any vulnerabilities that might arise in the software component. Security architecture diagrams, data workflows, and risk assessments can all aid in this process.

7. What CybSec certificates are applicable for Quality Assurance and/or Regulatory roles, as part of the different functions within a medical device manufacturer?
HCISSP (Healthcare Information Security and Privacy Practitioner) - covers risk management, privacy, and regulations related to PHI and devices, CISSP (Certified Information Systems Security Professional) - high-level, broad content coverage, meant for QA/RA, CRISC (Certified Risk and Information Systems Control) - focused on IT and cyber risk management, practical for those overseeing submissions, and others such as CSF (NIST Cybersecurity Framework) practitioner, and ISO/IEC 27001 Lead Implementer or Auditor.

8. What are some essentials to SBOMS other than Name, Version, Description, Download Location, Homepage, License, Summary, EOL date. Also is it okay to manage a separate excel sheet specific to the CVE's associated with the packages on the SBOM? **Besides the minimum SBOM elements (https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom), you should consider including associated vulnerabilities and corresponding information. It's OK to manage the CVEs in a separate sheet, but it is not efficient and can be fraught with manual errors. I would suggest that you look for a tool to automate the linking of the CVEs to SBOM components and the automatic updating of the vulnerability information, when available. Vigilant Ops offers automation support for the lifecycle of the SBOM, checking for minimum elements and matching and continuously updating vulnerabilities.**

9. Are there specific cybersecurity standards or certifications that medical device manufacturers need to comply with to enter the Medical Device Single Audit Program (MDSAP)? How do these cybersecurity requirements align with global regulatory frameworks like ISO 13485 and FDA cybersecurity guidelines? **No, there are no cybersecurity-specific standards or certifications that are explicitly required to participate in the Medical Device Single Audit Program (MDSAP) — but cybersecurity expectations are increasingly embedded in the Quality Management System (QMS) and are aligned with key global standards.**

10. For IVD instruments that rely on integrated software and are connected to systems like LIS or cloud platforms, what has your experience been in managing cybersecurity risks—especially when off-the-shelf components like Windows OS or devices like Epson scanners are involved? How do you recommend addressing these in the risk assessment, particularly with regard to device classification, design controls, and post-market surveillance under IVDR? And how should manufacturers approach updates, patching, and vulnerability management for these components over the product lifecycle?
For risk management, include COTS in threat modeling, and link CVEs to risk. For design controls, document update plans, system authentication and link an SBOM, if available. Take a look at MDCG 2019-16 – Guidance on cybersecurity for medical devices and IVDR Annex I, GSPR 17.2 - Cybersecurity protection expectations for additional help and guidance.

11. I would like to know the importance of UL 2900 series of standards used in Cybersecurity risk mitigation in medical devices. **The UL 2900 series of standards is important for cybersecurity risk mitigation in medical devices because it provides structured, testable criteria to evaluate the cybersecurity posture of connected medical systems. The most relevant for medical devices is UL 2900-2-1. It covers areas such as – secure software design, authentication, encryption, malware detection, and static/dynamic/fuzz testing.**

12. What is considered a good percentage for vulnerability reporting when analyzing code? What steps should be taken if the percentage is low, indicating a code vulnerability?
There are no universal benchmarks, but a low reporting percentage of roughly 40-60% could indicate blind spots – tools not catching certain CVEs or untracked components. Check your SBOM and make sure it includes all direct and transitive dependencies, build tools, plugins, and system packages.

13. How can you tell if your malware detection software is doing a good job?
There are some tools available to do benchmarking. Check out MITRE ATT&CK Evaluations (https://attackevals.mitre-engenuity.org/)

14. When performing CVE vulnerability assessments on big software components like Android, how do you triage, manage, and address a huge amount (thousands) of CVEs? **Prioritization of vulnerabilities is the key. Use information in addition to CVSS scores, such as KEV (Known Exploited Vulnerabilities) catalog maintained by CISA and EPSS (Exploit Prediction Scoring System) developed by FIRST.org to get a more holistic view of the actual criticality of that vulnerability. Ideally, using an automation tool that factors this additional information into the vulnerability score will save a tremendous amount of manual effort and potential errors.**

15. If you use off-the-shelf components, how do you know if they have vulnerabilities such as computers?
Request an SBOM from the manufacturer, or if possible, generate an SBOM against the component or system. Use the SBOM to map vulnerabilities to the listed components using a source like the National Vulnerability Database (https://nvd.nist.gov)

16. What should be included in a software threat assessment?

- **System overview and data flows**
- **Identification of assets and trust boundaries**
- **Threat modeling (e.g., STRIDE, attack trees)**
- **Risk assessment (likelihood × impact)**
- **Existing controls and gaps**
- **Recommended mitigations**
- **Residual risks and justification**
- **Documentation and tracking**

17. Please discuss if over the air updates (OTA updates) are considered a good risk mitigation for cyber security threats. **OTA updates are a strong risk mitigation tool, provided that the update process itself is hardened against tampering and misuse.**

18. What tools would you recommend to discover what vulnerabilities are in open-source software?
To discover vulnerabilities in open-source software, you will need an SBOM generator, unless you already have an SBOM for the software. After you have an SBOM, you will need to match component information with known vulnerabilities using a source like the National Vulnerability Database (NVD – https://nvd.nist.gov). Ideally, you would want to automate as much of the process as possible, and Vigilant Ops offers both SBOM generators and vulnerability matching and continuous monitoring.

19. What are the risk assessment methods that are well fit to access cybersecurity threat and if electronic system can manage SSDLC. What are the risk assessment methods suitable for evaluating cybersecurity threats, and can an electronic system manage SSDLC?
NIST SP 800-30 is a widely adopted framework for qualitative and quantitative risk analysis. Of course, you also utilize threat model frameworks such as STRIDE and the Software Bill of Materials (SBOM) with continuous vulnerability monitoring. There are systems that automate much of this manual effort. Vigilant Ops offers an end-to-end lifecycle management platform that supports many of the requirements throughout the SSDLC.

20. FDA indicates to stay away from using likelihood. However, SW96 uses it. How do I recommend reconciling both views.
Here are some steps you can take to reconcile this discrepancy:

- **Use likelihood internally for prioritization (per AAMI SW96:2023 – Standard for Medical Device Security – Risk Management)**
- **Use exploitability + impact externally (as per FDA guidance)**
- **Frame risks as realistic threat scenarios, not probabilities**
- **Document both views in documentation submitted to FDA, for example *"Our internal risk management follows AAMI SW96, using likelihood and impact to support prioritization and planning. However, in accordance with FDA guidance, our submitted risk assessments focus on exploitability, potential for patient harm, and the presence or absence of effective controls."***

If you have further questions or need personalized guidance, don't hesitate to reach out to our team.
We're here to support you every step of the way.
www.vigilant-ops.com or email us at info@vigilant-ops.com