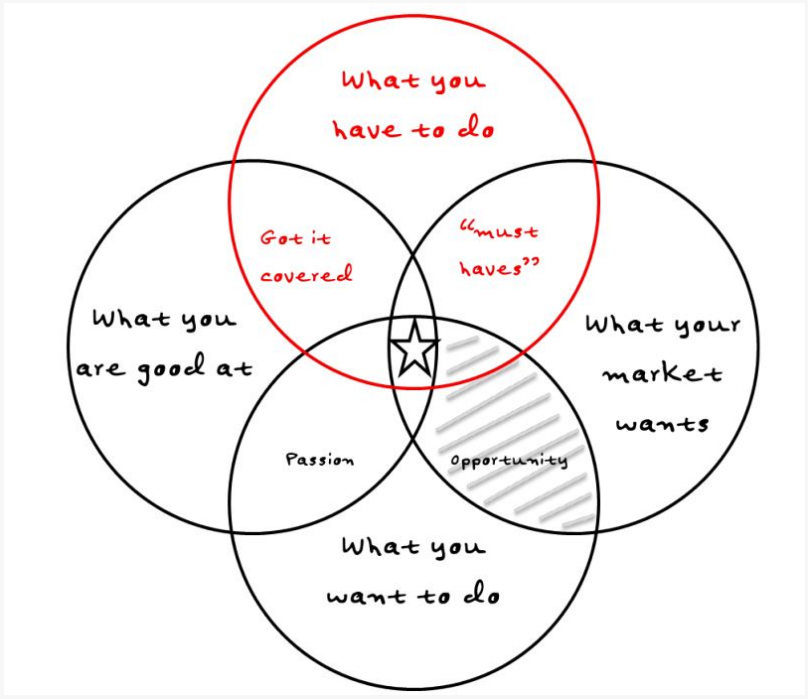
CyberActa Ensures Compliant Medical Device Cybersecurity Design and Development

CyberActa medical device software design and development expertise minimizes vulnerabilities and reduces attack surface of every phase of the development cycle.

CyberActa Medical Device Cybersecurity



CyberActa Regulatory Compliance

BOSTON, MASSACHUSETTS, USA, January 8, 2024 /EINPresswire.com/ -- Heightened awareness about cybersecurity issues has led regulatory agencies and customers alike to demand security and high quality from medical devices. An effective way to protect medical devices against cyber threats is to integrate security — whether that is the FDA's Quality System regulation (QSR), ISO 13485, or ISO 62304 — into every step of an established medical device development process. Medical devices that are secure by design start with that goal before the design process even begins to render products that are secure to use "out of the box" with little to no configuration changes. Furthermore, secure by design eliminates the integration problems, cost, and increased likelihood of vulnerabilities that come with add-on security components.

CyberActa's secure by design and default (SBDD) is an approach to medical device software and hardware design and development that seeks to minimize systems' vulnerabilities and reduce the attack

surface through designing and building security into every phase of the medical device development cycle, including security specifications in the design, continuous security evaluation at each phase, and adherence to best practices. Integrating security into medical device development includes:

CyberActa, Inc.

•Early identification and mitigation of security vulnerabilities and misconfigurations of medical devices.
•Identification of shared security services and tools to reduce cost, while improving security posture through proven methods and techniques.
•Facilitation of informed key stakeholder decisions through comprehensive risk management promptly.
•Documentation of important security decisions throughout the medical device life cycle, ensuring that security was fully considered during all phases.

Many medical devices – from glucose meters and insulin pumps to smart wearable devices, sophisticated software, and hospital equipment – are now deemed cyber medical devices by the FDA, and regulatory bodies around the globe have increasingly pursued medical device cybersecurity as a policy objective. The culture, approach, and regulatory and customer expectations of how cybersecurity is addressed across medical device designers and manufacturers are changing. Cybersecurity was often bolted on at the end of a product's life cycle and did not deliver secure capabilities into the users' or patients' hands.

With the ever-increasing cyber threats that exist in the world, this new approach is essential. The CyberActa approach will lead to the delivery of more secure medical devices and medical systems through clearer accountability, simplified processes, use of security standards, better guidance, more flexibility, and empowered decision-making.

About CyberActa, Inc.
Headquartered in Boston, Massachusetts, providing data-driven digital, regulatory, cyber, and privacy solutions. The company's products and services are used by Fortune 500 companies, government agencies, and startups around the world.

John Giantsidis

CyberActa, Inc.
+1 617-830-3041
john.giantsidis@cyberacta.com
