VELENTIUM

Medical Device Cybersecurity

Supported Platforms

- Embedded Medical Devices
- Sensors
- Smartphones (iOS & Android)
- Supporting Infrastructure
- WebApps

Industry Leading Experts In:

- Secure Development Lifecycle
- Secure Design at the System and Product Levels
- Formal Threat Modeling
- 'Right sizing' Security Mitigations
- Vulnerability Assessment
- Penetration Testing
- Fuzz Testing of Communication Mediums
- Regulatory Submission 510k / PMA Review
- Source Code Security Static Analysis (SAST)
- Post Market Surveillance
- Cybersecurity Training for Staff

MAKE YOUR DEVICE SECURE

Email: nextstep@velentium.com

How We **Solve For Our Clients**

Our team brings a technical understanding of embedded design & development processes and tools, right-sizing security mitigations for constrained resources, and artifact production in compliance with regulatory guidance.

Velentium utilizes a Secure Development Lifecycle. We believe the best way to guarantee a secure system is to weave security throughout the entire development process.

Velentium Core Values

Honorable
We do Right for Right's sake

Results ++
We do the job and then some

Humble Charisma
We strive to be the kind of people others want to be around

Post Market **Surveillance**

Overview

In 2016 the FDA released its guidance on "Postmarket Management of Cybersecurity in Medical Devices," creating a regulatory expectation for device manufacturers to monitor all third-party software components (TPSCs), e.g., libraries, frameworks, operating systems, utilized in your medical device system for disclosed threats. This ongoing monitoring effort continues for the life of the medical device. This ongoing vigilance burdens device manufacturers with monitoring, investigating, and assessing the impact of these TPSC vulnerabilities upon your medical device system. This effort can be highly disruptive to current development projects. Therefore, Velentium's team of highly skilled cybersecurity professionals have stepped up to the challenge of providing this cybersecurity oversight for all of your utilized TPSC items. We provide quarterly reports on each product's TPSC vulnerabilities for manufacturer review, thus freeing manufacturers to return to the business of creating medical devices, not focusing on product implementations of the past.

Subscription Service **Includes**

- **Quarterly Review** — Every quarter, Velentium will review the product's thirdparty software components and documentation delivered for new exposed vulnerabilities using a multitude of resources including, but not limited to, CVE, NVD, H-ISAC's SIR, ThreatStream, Vulners, media outlets, and the software component manufacturer.
- **Software Bill of Materials** — Review of software projects to create the essential "software bill of materials" for all utilized TPSC items with revision utilized and OEM details.
- **Product-Specific Vulnerability Assessment** — When vulnerabilities are discovered, Velentium can perform an in-depth analysis to assess the impact on the product and its essential clinical performance. Our report also recommends detailed mitigations customized for your product's unique requirements.

Our team brings a technical understanding of embedded design & development processes and tools, right-sizing security mitigations for constrained resources, and artifact production in compliance with regulatory guidance.

Velentium utilizes a Secure Development Lifecycle. We believe the best way to guarantee a secure system is to weave security throughout the entire development process.