BLUE GOAT CYBER

Medical Device Cybersecurity Assessment & Penetration Testing Services

Medical Device Cybersecurity Assessment & Penetration Testing Services for Compliance and Patient Safety

Blue Goat Cyber understands that often the key objective of testing medical devices is to assist with meeting FDA cybersecurity requirements, such as the Premarket Notification 510(k) and Postmarket Submissions. Our methodologies for medical device cybersecurity assessments and penetration testing are designed to follow the guidelines detailed in industry-accepted standards, including NIST, ISO, Center for Internet Security, etc. Specific to the requirements of the FDA, Our test framework references the following standards:

- The Open Source Security Testing Methodology Manual
- U.S. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment
- FDA Premarket Notification 510(k)
- FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2018 Draft)
- EU Medical Devices Regulation (MDR)
- UL 2900 set of standards (UL's Cybersecurity Assurance Program)

Steps to schedule your medical device cybersecurity assessment:

- Schedule a 30-minute Discovery Session
- We determine IF and HOW we can help
- We provide a Tailored Proposal
- Together, we review the Proposal

Based on our FDA medical device cybersecurity compliance experience, our cybersecurity assessment protocol consists of the following activities:

- Assess risk pertaining to confidentiality, integrity, and availability
- Assess entry points to systems
- Assess existing controls
- Assess data flows
- Assess use cases
- Assess and assist with the Threat Tree development
- Assess and assist with the Traceability Matrix
- Assess and assist with standard operating procedures
- Assess and assist with software architecture cybersecurity
- Recommend revisions to or new security controls
- Recommend design changes to reduce risk
- White Box Medical Device Penetration Test

Blue Goat Cyber's Methodology for Medical Device Cybersecurity Assessment and Penetration Testing

For optimal outcomes, Blue Goat Cyber proposes a two Assessment Evolution, test/retest approach. Within each Evolution, in addition to the actual testing component, we dedicate access to our cybersecurity team for report clarification and knowledge exchange, assisting in your understanding of the test findings and the remediation strategies.

Post-remediation of Evolution 1, we will again conduct the cybersecurity assessment and penetration test to assess the efficacy of addressing identified vulnerabilities. This second set of reporting demonstrates a more robust security posture and, therefore, a more impactful Letter of Attestation.

Assessment Evolution 1

1. Preparation (Offsite). Before we travel to your facility in we will prepare for the onsite visit. Our preparation will consist of document reviews and discussions with your team. The intent is for us to get familiar with your product and formulate a plan of action ahead of our onsite visit. This allows us to optimize our time onsite.

2. Testing (Onsite or at Blue Goat's facility). We will travel to your facility to perform the cybersecurity assessment and penetration test against your product. Testing can also be performed at Blue Goat's facility if you ship the equipment to us. Our testing will consist of identifying all entry points into the system, such as Ethernet, Fiber, WiFi, USB, Serial, HDMI, (and will look for others), vulnerabilities associated with each entry point, and exploitation of initial and subsequent vulnerabilities. Any critical findings discovered will immediately be brought to your attention. In addition, due to the nature of this engagement, we can share with you our test results on a daily-basis as an end-of-day update.

3. Reporting (Offsite). At the end of testing, we will generate a penetration test report that rank orders our findings based on criticality. The report will include exploitation steps, step-by-step, described with screenshots. The report also includes remediation guidance for each finding.

4. Report Presentation (Offsite). Once the report is completed, we will send it to you and review it via a Zoom session.

Between Evolution 1 and Evolution 2, you will work on fixing issues identified in Evolution 1.

Assessment Evolution 2

When you are ready for us to retest the medical device, we will repeat the applicable steps of Evolution 1 in Evolution 2. This will be completed onsite at Blue Goat or at your facility.

At the end of Evolution 2, we will generate a Letter of Attestation that summarizes the scope, findings, and overall risk rating for the medical device. The Letter of Attestation is intended to be shared with clients, auditors, regulators, etc.

Blue Goat Cyber
PO Box 20310
PMB 45092
Cheyenne, Wyoming 82003-7007

(307) 317-8884
info@bluegoatcyber.com