PRAETORIAN

DATA SHEET

Medical Device Penetration Testing

Comprehensive security assessments for medical devices, from pre-market design review to post-market vulnerability management. Ensure FDA compliance and protect patient safety.

CONTENTS

Key Benefits

- **Understand Your Ecosystem:** Gain comprehensive visibility into your medical device ecosystem, including hardware, software, network communications, and cloud integrations.
- **Identify Risks:** Discover vulnerabilities before attackers do, from insecure firmware to weak authentication protocols.
- **Quantify for FDA:** Meet FDA cybersecurity guidance requirements with documented evidence of security testing and risk assessment.
- **Mitigate Vulnerabilities:** Receive actionable remediation guidance prioritized by risk and business impact.

Your Challenge

Medical device manufacturers face unique cybersecurity challenges. Your devices handle sensitive patient data, connect to hospital networks, and directly impact patient safety. Regulatory requirements from the FDA demand rigorous cybersecurity assessments throughout the product lifecycle.

> **The Stakes Are High:** A compromised medical device can lead to data breaches, regulatory penalties, product recalls, and most critically, risks to patient health and safety.

Whether you're preparing for FDA submission or maintaining security for deployed devices, you need a partner who understands both cybersecurity and the unique constraints of medical device development.

Capabilities Overview

- **IoT Security Practice:** Dedicated team with deep expertise in connected device security
- **Postmarket Services:** Ongoing security monitoring and vulnerability management
- **Destructive Testing:** Optional chip-level analysis and advanced hardware attacks
- **Premarket Services:** Design review, threat modeling, and premarket submission support
- **Hardware Security:** Firmware analysis, JTAG debugging, and hardware exploitation
- **Backend Assessment:** Cloud infrastructure, APIs, and supporting systems testing

Service Offerings

Our medical device security services are tailored to your product lifecycle stage, from initial design through post-market deployment.

PRE-MARKET

- Design Review
- Threat Modeling
- Cybersecurity Controls Assessment
- SBOM Review
- FDA Submission Support

POST-MARKET

- CBOM Review
- Update Verification
- Vulnerability Monitoring
- Incident Response
- Security Patch Validation

EITHER PHASE

- Code Review
- Risk-Informed Security Assessment
- Penetration Testing
- Architecture Review
- Compliance Validation

Why Praetorian

- **Healthcare Expertise:** Deep understanding of FDA requirements, HIPAA compliance, and medical device standards.
- **Full-Stack Capability:** From hardware to cloud, we assess every component of your device ecosystem.
- **Research-Driven:** Our team actively researches medical device vulnerabilities and presents at leading security conferences.
- **Collaborative Approach:** We work alongside your engineering teams, providing knowledge transfer and training.
- **Regulatory Experience:** We've supported numerous FDA submissions with security documentation and attestations.

Who Needs This Service

- Medical device manufacturers preparing for FDA submission
- Companies with deployed devices requiring post-market security monitoring
- Organizations responding to FDA security feedback or warning letters
- Healthcare technology vendors seeking to demonstrate security maturity
- Device manufacturers integrating with hospital networks
- Companies building connected medical devices (IoMT)

Deliverables

Every engagement delivers comprehensive documentation suitable for both technical teams and regulatory submissions.

1. **Executive Summary**
   High-level findings and risk overview for leadership and regulatory stakeholders
2. **Engagement Outbrief**
   Interactive presentation of findings with technical and business context
3. **Technical Findings Report**
   Detailed vulnerability documentation with evidence, impact analysis, and remediation guidance
4. **Letter of Attestation**
   Formal documentation for FDA submission confirming security assessment completion

Sample Threat Model

Our threat modeling process identifies potential attack vectors across your device ecosystem. Common threat categories we assess include:

- **Physical Attacks:** Device tampering, JTAG exploitation, firmware extraction
- **Application Attacks:** API abuse, authentication bypass, injection attacks
- **Network Attacks:** Man-in-the-middle, protocol analysis, wireless exploitation
- **Supply Chain:** Component vulnerabilities, third-party risks, update mechanisms

About Praetorian

Praetorian is a leading cybersecurity company dedicated to helping organizations build and maintain secure products. Our team of experts combines deep technical expertise with industry-specific knowledge to deliver comprehensive security assessments that meet the highest standards. We work with Fortune 500 companies, innovative startups, and healthcare organizations to secure their most critical systems.

Website
www.praetorian.com

Email
info@praetorian.com

Phone
+1 (512) 686-2292

Ready to Secure Your Medical Device?

Contact us today to discuss your medical device security needs and learn how we can help you achieve FDA compliance while protecting patient safety.