praetorian

DATA SHEET

Medical Device Penetration Testing

KEY BENEFITS

Understand the entire medical device ecosystem, from backend systems and business processes to hardware and mobile devices

Identify security risks associated with design & implementation before going to market

Quantify known risks in accordance with FDA requirements

Mitigate identified vulnerabilities with expert remediation solutions

YOUR CHALLENGE

Your organization's medical devices handle sensitive medical data, and severe vulnerabilities can arise anywhere along the transmission flow from the hardware itself to backend systems or other data aggregation points. You need assurance that the data your device ecosystem handles–whether your own corporate secrets or confidential patient information–is as secure as possible every step along the way. You also need to prove that your products meet FDA requirements for pre- and post-market submissions.

OUR SOLUTION: CAPABILITIES OVERVIEW

Praetorian's Internet of Things practice follows data flows that begin at hardware devices and terminate in a backend cloud environment, potentially transiting mobile devices, Wi-Fi access points, or cellular gateways along the way. For premarket devices, we can orient to all aspects of the product lifecycle including design, threat modeling, code review, penetration testing, and cybersecurity controls definition & verification. For postmarket devices, we can extend those same activities with verification of software/firmware updates, CBOM review, and risk mitigation review. We orient our activities around the FDA's standards and our team uses an offensive approach to identify attack paths to critical assets.

For each engagement, our engineers review source code (subject to availability), API specifications, and technical standards or whitepapers to understand where weaknesses are likely to arise, and tailor their testing accordingly. We then use tools–both commercially available and bespoke from Praetorian Labs–to identify vulnerabilities, demonstrate attacks, analyze protocols, and enumerate the attack surface.

- **A core of hardware security.** Our engineers use your exemplar hardware to simulate usage conditions and carefully tap into debugging, network, or wireless interfaces. This provides us a detailed understanding of the device's inner workings and how it might be attacked.
- **Optional destructive testing.** Depending on your security needs, the team can perform light-touch disassembly of devices to expose additional interfaces and attack surface. We use optional destructive testing to exploit the exemplar hardware more thoroughly but may render a device inoperable.
- **Optional backend attacks.** Praetorian can scope an engagement to include attacks against both data in transit and data at rest in the backend cloud environment. Our engineers have expertise related to numerous IoT PaaS and cloud IoT registries, as well as the asynchronous messaging systems commonly used in conjunction with them.

SPECIFIC SERVICE OFFERINGS

Pre-Market	Design Review / Threat Modeling / Cybersecurity Controls (Advisory): design controls that map back to risks in the threat model, verify and document correct implementation
Post-Market	CBOM Review (Advisory): perform due-diligence on all components, accounting for known CVEs and LOAs from third parties / Update Verification (Optional Add-On): Review new software releases in primary or third-party code
Either or Both Stages	Code Review: ensure code maps to design, review third party libraries incorporated to code base, run SAST and DAST tools / Risk-Informed Security Assessment

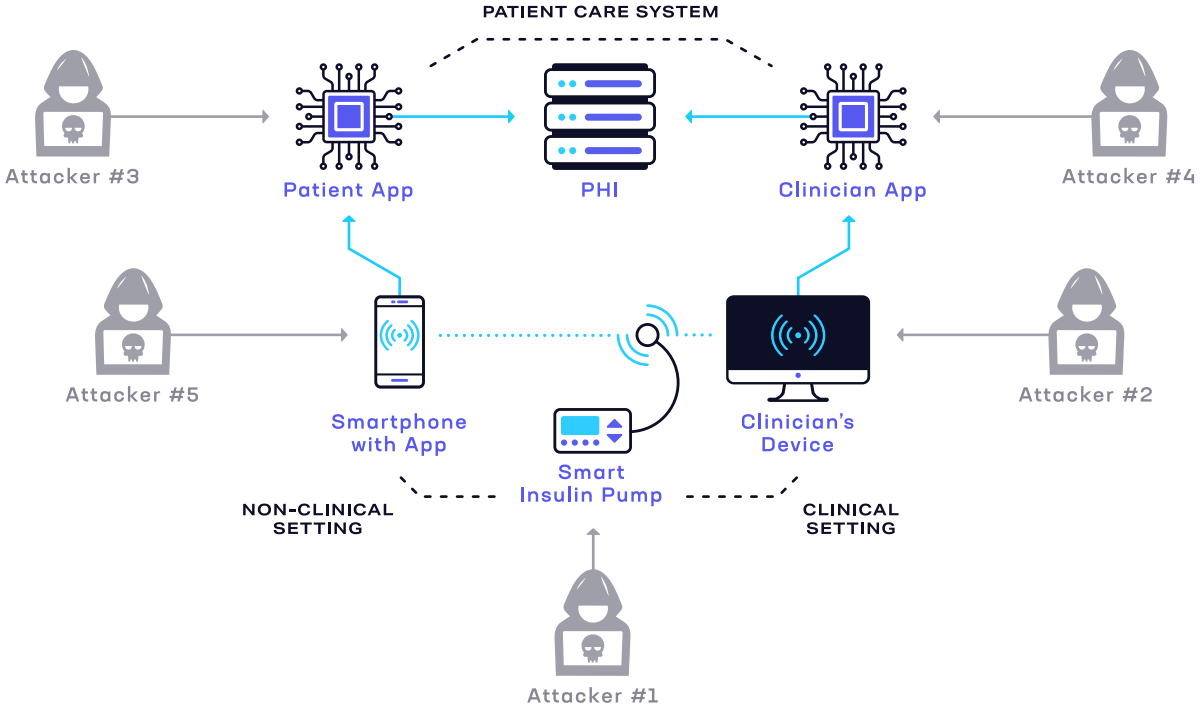
WHY PRAETORIAN

At Praetorian, we provide a timely, tailored, and thorough assessment of your product's cybersecurity from the backend to the user interface and everywhere in between. We have industry-specific experience involving medical devices in a premarket or postmarket setting. You can rely on us to emulate attackers to provide you with an offensive perspective and direct, actionable feedback on what we find. Our team focuses on delivering the best possible client experience while partnering with you to strengthen your security posture.

WHO NEEDS THIS SERVICE

- **Medical device manufacturers** that want an experienced partner to navigate the FDA's cybersecurity requirements in an efficient and reliable way.
- **Device development teams** that embrace cybersecurity as a critical element of a medical device's overall safety.

SAMPLE THREAT MODEL



DELIVERABLES

Executive Summary

Concise explanation of engagement goals, significant findings, business impacts, and strategic recommendations

→ Upon request, a letter of attestation

Engagement Outbrief Presentation

Similar to the executive summary, presented to the audience of your choosing

Technical Findings Report

Detailed description of issues and the methodology used to identify them, as well as an impact assessment for each

→ Custom reports tailored to specific service offerings

Praetorian Security, Inc.
6001 W Parmer Ln, Ste 370, PMB 2923
Austin, TX 78727 USA
info@praetorian.com

To learn more about Praetorian, visit: www.praetorian.com

ABOUT PRAETORIAN

Praetorian is an offensive security engineering company whose mission is to make the digital world safer and more secure. Through expertise and engineering, Praetorian helps today's leading organizations solve complex cybersecurity problems across critical enterprise assets and product portfolios.