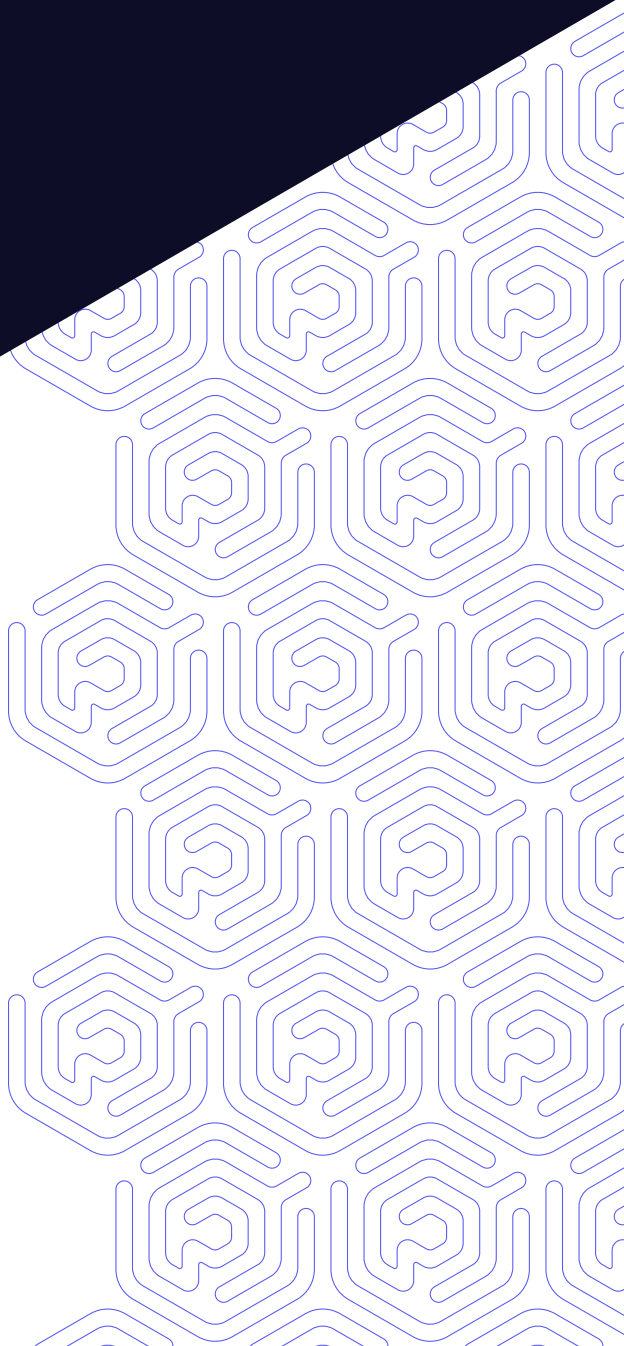
WHITE PAPER

Medical Devices Need Offensive Security

Robust cybersecurity leads to greater patient impact.



praetorian

A holistic offensive cybersecurity approach will ensure products remain secure postmarket.

INSIDE THIS REPORT

Medical devices have changed significantly since 1976, when the FDA first began regulating them. The related sciences have progressed, leading the medical device industry away from purely mechanical products and toward technologically advanced, cloud-connected devices. A doctor who wanted to adjust a pacemaker before 2009 had to perform surgery to access the mechanical device within their patient. Today, wireless enabled pacemakers permit healthcare professionals to monitor their patients' heart rhythms over the internet and make adjustments with external computers.

The FDA, being a government behemoth, has been slow to change their regulations in order to handle the implications of the direction the medical device industry has taken. Perhaps the classic example is those very same wireless pacemakers, which underwent a recall in 2017 over concerns that the devices were vulnerable to hacking attacks. This cybersecurity vulnerability profoundly damaged the reputation of the manufacturer involved, cut into their revenue, and most importantly, posed a serious threat to human life. Cybersecurity has since become a critical element of ensuring the overall safety of medical devices, and now the industry is one of the most heavily regulated in the world.

In March 2023 Congress granted the FDA authority to enforce cybersecurity regulations. The strategies organizations adopt for their premarket submissions and postmarket monitoring will now directly affect the likelihood of their medical devices receiving market release approval from the FDA. While various cybersecurity approaches and implementations exist, selecting a holistic offensive security strategy that covers the full lifecycle will be the most effective way manufacturers can ensure their device not only makes it to market, but remains secure into the future.

© Copyright 2023 Praetorian Group, Inc. All rights reserved. | praetorian.com

March 2023 FDA Regulatory Changes

Since 2018, medical device manufacturers have been aware of the guidelines in "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." In this document, the FDA emphasized the importance of cybersecurity risk management throughout the product lifecycle and included suggestions for the following:

- **Addressing vulnerabilities,**
- **Implementing design controls, and**
- **Establishing a coordinated vulnerability disclosure policy.**

Yet, for the five years that version of the document was in effect, the FDA lacked authority to enforce these guidelines. The document neither provided instructions on how to perform recommended penetration testing, nor outlined consequences for any manufacturer that chose not to plan for their medical devices' cybersecurity. Medical device manufacturers could determine for themselves whether to develop a cybersecurity risk management plan, and how to incorporate any testing into it.

The key shift in March 2023, then, occurred when the Consolidated Appropriations Act of 2023 granted the FDA the authority to enforce the erstwhile guidelines as requirements (see article). The basic steps to ensure compliance are essentially the same; the difference is that the FDA now can reject medical devices that do not meet their baseline cybersecurity standards. To facilitate successful medical device development and release, the FDA has set clear expectations for manufacturers to demonstrate their commitment to cybersecurity throughout the product lifecycle.

Importance of a Third Party Partner

The cybersecurity regulations now emphasize the need for manufacturers to collaborate with third-party security experts in order to achieve robust enough security. Medical device manufacturers that want to ensure their products make it to market will need to conduct comprehensive risk assessments and implement security controls to mitigate threats. Yet, internal cybersecurity teams that have a compliance focus will not have

© Copyright 2023 Praetorian Group, Inc. All rights reserved. | praetorian.com

the attacker perspective needed to be effective in those tasks. Partnering with a third-party cybersecurity provider in both the premarket submission process and postmarket monitoring efforts can provide manufacturers an offensive security strategy that is more likely to satisfy the FDA.

In addition to crafting and executing an offensive security strategy for a medical device, the right third-party experts can help manufacturers' internal teams manage the implications that accompany that strategy. Areas of potential additional impact correlate to the following FDA requirements:

- **Robust premarket testing and comprehensive risk assessments.** A third-party partner with an offensive security focus can provide increased confidence that the cybersecurity strategy takes into account the full range of potential threats.

- **Continuous offensive security (COS) postmarket integration.** A partner who specializes in COS appreciates the need for ongoing vigilance to address evolving threats, and will maintain their focus so an internal team can attend to other priorities.

- **Collaboration with third-parties.** Maintaining a strategic partnership with a single offensive security vendor minimizes the internal team's burden of onboarding new vendors.

- **Security control implementation.** A third-party partner with an attacker focus can advise internal security teams on controls that actually mitigate threats rather than simply checking a box.

© Copyright 2023 Praetorian Group, Inc. All rights reserved. | praetorian.com

Offensive Security Strategy for the Full Medical Device Life Cycle

An important distinction to make when discussing medical device cybersecurity is that the environment is what changes. To return to our original example, a pacemaker inside a patient's body does not change. Instead, what changes is the environment to which it connects. The traditional approach of using one-off penetration testing to "secure" medical devices fails to account for the dynamic nature of everything that actually makes the device function: the applications, the databases, the cloud itself, and more.

Planning an offensive security strategy for the full medical device life cycle acknowledges that the device is one small element of a holistic environment that must be secured in its entirety for perpetuity. Manufacturers who embrace this concept end up with a robust two-part strategy that folds together risk-informed assessments premarket and COS postmarket.

Premarket Submissions: Cybersecurity in Development

The FDA requires manufacturers to provide various documents depending on the medical device being submitted for market approval. Among them are the 510(k), Premarket Approval (PMA) Application, and De Novo, and the review process can take an average of eight months. The earlier a project incorporates a cybersecurity strategy, the more time the device team has to mitigate any vulnerabilities the process uncovers.

From the FDA's perspective, this approach to cybersecurity demonstrates the manufacturer's commitment to risk management. Undertaking a comprehensive risk assessment beginning in the development phase, then documenting follow-on penetration testing and control implementation throughout the cycle, also can help streamline the approval process. Fewer material vulnerabilities in a submission translates to fewer issues requiring resolution before the FDA can grant approval. Therefore, this approach to preparing for the premarket submission process constitutes the first half of an effective offensive security strategy for medical devices.

Postmarket Management: Continuous Offensive Security

The FDA's expanded regulatory authority includes assessing medical device manufacturers' plans for postmarket monitoring, to ensure the ongoing safety and

© Copyright 2023 Praetorian Group, Inc. All rights reserved. | praetorian.com

efficacy of the devices it approves. The now-enforceable regulations emphasize the importance of continually monitoring for, identifying, and remediating cybersecurity vulnerabilities as part of postmarket device management. This particular task is an ideal use case for COS, which involves attack surface management (ASM), continuous red teaming, and managed offensive security.

Attack Surface Management. By constantly monitoring the attack surface (various entry points attackers can use to gain access to a medical device) via automated tools, manufacturers can understand their true exposure and effectively prioritize remediation.

Continuous Red Teaming. By simulating real-world attack scenarios on a regular cadence, medical device companies can validate threats to stay ahead of attackers.

Managed Offensive Security. By partnering with an offensive security provider, internal teams can augment their capabilities while reducing their costs.

COS with a third-party partner, therefore, should comprise the second half of any effective offensive security strategy. For further details on COS, specifically, see our white paper on the topic.

Praetorian's Approach to Medical Device Cybersecurity

Praetorian's team of product security engineers has worked extensively with manufacturers developing and bringing medical devices to market. For every project

© Copyright 2023 Praetorian Group, Inc. All rights reserved. | praetorian.com

since 2018, we have treated the FDA's guidelines as enforceable requirements, and we have encouraged our clients to do the same. We have shepherded over 64 medical devices to the market, and are familiar with the FDA's regulations, the ins and outs of their process, and the potential roadblocks device teams might encounter. Furthermore, we stay current with updates from the FDA, so are always prepared to help clients evaluate and adjust their strategies to account for new developments.

Tailor the Solution

Every medical device is unique, as are its cybersecurity requirements, so Praetorian customizes the offensive security strategy we suggest for each device. Yet the goal remains the same for every partnership: to ensure comprehensive protection and, through that, compliance with the FDA's requirements. Manufacturing partners gain access to our experts in medical device security. Our team's two-part focus is providing clear, actionable feedback about preventing security vulnerabilities during development, and continuously identifying and mitigating emerging threats postmarket.

Reduce Cybersecurity Costs

Our offensive security strategy for securing medical devices has a proven track record of identifying and remediating vulnerabilities across the entire life cycle, which has helped manufacturers accelerate the FDA approval process. Given the depth of expertise we bring to the table, our partners' internal teams have been able to outsource cybersecurity

© Copyright 2023 Praetorian Group, Inc. All rights reserved. | praetorian.com

tasks to our team while focusing on their own core competencies. Between shortening the time to market and allowing internal teams to focus their efforts elsewhere, manufacturers who have partnered with us have minimized expenses associated with managing the cybersecurity risk for their devices.

Increase Market Share

Protecting patients' safety and data is vital to maintaining brand reputation and increasing customer loyalty. A robust cybersecurity posture, such as the one medical device manufacturers can build with an offensive security strategy, results in more secure devices. When healthcare providers and their patients feel confident that a manufacturer has taken the FDA's requirements seriously–and will continue to do so–then their medical devices ultimately gain more of the market share.

Offensive Security Strategy Yields Compliance

March 2023's expansion of the FDA's ability to enforce cybersecurity requirements for medical devices means manufacturers need a strategy to apply as they develop and release new products. Internal teams are not adequately resourced to meet this new mandate, so choosing a third-party partner can be a force multiplier in the premarket submission and postmarket monitoring stages. However, to maximize the value a third-party can add, manufacturers will want to select a partner with an offensive security focus that can customize a full lifecycle strategy for each unique medical device coming to market. Adopting this strategy ultimately will lead to devices the manufacturer can bring to market more quickly because they satisfy the FDA's requirements more efficiently.

More importantly, though, applying an offensive security strategy to medical device cybersecurity is about embracing the holistic nature of the technology and the industry. Complying with requirements only takes a manufacturer part of the way to genuine security, because doing the bare minimum will merely check the FDA's boxes. Manufacturers that instead focus on developing a robust cybersecurity strategy will produce more secure devices and have a more profound impact on patients' lives while inherently satisfying the FDA's requirements.

© Copyright 2023 Praetorian Group, Inc. All rights reserved. | praetorian.com