The sharp uptick in cyberattacks on connected medical devices is alarming. Such threats can disrupt entire device fleets, prevent providers from accessing critical patient information and offering the right care, as well as threaten patients’ lives.

In response, the FDA and MITRE updated their Medical Device Cyber Response Playbook (first published in 2018). This revision defines the roles and responsibilities of medical device manufacturers (MDMs). They’re given a central role that directs them to collaborate with and support health delivery organizations (HDOs) in improving cyber incident preparedness, management, containment, and reporting.

One of the new playbook’s main goals is to address limitations HDOs face in managing device-level threats. The updates serve to ensure that HDOs can obtain baseline and ongoing medical device cybersecurity information while improving their emergency readiness and response frameworks.

Tackling cyber risks requires a deep understanding of a given device, its components, and its vulnerabilities. Only a respective manufacturer has access to and mastery of this, hence the requirement that they use that information to lower device risks and improve safety and security.

What has changed since 2018?

Much has changed since the pre-pandemic world of 2018. “Things” have become much more connected—including medical devices—thus presenting threat actors with new attack surfaces. The number of zero-days is growing with every device, attackers are innovating ways to exploit them, and regulators and society are demanding more be done to close the staggering expansion of cyber exposure.

Within a short time, cybersecurity concerns have shifted from patient data protection and privacy to medical device protection coupled with quality of patient care and safety. MDMs play an essential role in addressing these concerns across their R&D, engineering, product security, quality, and safety disciplines. Ultimately, success means solving for the root cause—exploitability of their medical devices.

The potential for connected devices to undergo cyberattack and manipulation poses a serious threat the continued development and adoption of these devices. Indeed, the problem of IoT security is the #1 risk to this industry’s continued growth.

2023 – Device security means patient safety

In a 2022 private industry advisory, the FBI stated that unpatched and outdated medical devices provide opportunities for cyberattacks. It noted: “Medical device vulnerabilities predominantly stem from device hardware design and device software management..."
The stage is now set for MDMs to be more proactive. One way is to offer built-in self-protection along with continuous real-time insights regarding device security and performance. After all, they’re responsible for their device designs and are best positioned to ensure they have security built in. Specifically this equates to passive and active security to address current understanding of threats and unknown future threats.

This reinforces the central role of manufacturers by identifying vulnerabilities as a root cause and attributing them to device design. Here, the cyber gap stems from HDOs having the best intentions for patient outcomes, but they cannot control pre-existing vulnerabilities in a connected world and often aren’t able to patch systems. Moreover, devices are often used for decades, outliving both their design and controls in place today.

The updated recommendations – an MDM call to action

The updated playbook makes strong recommendations for more support, collaboration, and communication between MDMs and HDOs. Along with the growing number of cyberattacks, the recommendations turn the timely ability to mitigate, contain, and report on cyberattacks into a critical component of HDOs’ device decision-making processes. Cyber factors that play into procurement decisions include:

- HDOs’ need for proactive protection from zero days and unknown vulnerabilities. While patching is an accepted fix, quickly applying them is nearly impossible and doesn’t cover third-party software. A core principle of IT security is ‘assume breach.’ For MDMs and HDOs, this should be ‘assume no patch.’ Medical device owners and operators should be assured of protection from new and unknown exploits, even when there is no patch and devices are connected.
- HDOs don’t have visibility into IoMT device and fleet performance, software flaws, and operational problems.
- They have limited information and no universal solution across IoMT devices.

Across all stages—procurement (when purchasing), inventory (once purchased), and detection (when a cyber event occurs)—the emphasis is increasingly on MDMs’ ability to provide HDOs with advanced protection in conjunction with meaningful information.

In this context, MDMs have an opportunity to establish themselves as security partners and leaders, collaborating on solutions to common problems and acquiring ‘go-to’ status for cybersecurity.

Sternum helps MDMs meet new playbook recommendations and HDOs’ growing needs

<table>
<thead>
<tr>
<th>HDOs’ Needs – 3 Stages</th>
<th>With Sternum, MDMs meet the need by:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Procurement</strong></td>
<td>Providing tangible fixes to contain threats</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability mitigation</td>
</tr>
<tr>
<td></td>
<td>• Transparency and visibility</td>
</tr>
<tr>
<td></td>
<td>• Proactive response</td>
</tr>
<tr>
<td><strong>Inventory</strong></td>
<td>Providing one centralized place for device information</td>
</tr>
<tr>
<td></td>
<td>• Continuous monitoring</td>
</tr>
<tr>
<td></td>
<td>• Granular visibility</td>
</tr>
<tr>
<td></td>
<td>• Device and fleet-wide data</td>
</tr>
<tr>
<td><strong>Detection &amp; Analysis</strong></td>
<td>Recording all activity, from incident discovery to containment and post-incident activity</td>
</tr>
<tr>
<td></td>
<td>• Early alerts</td>
</tr>
<tr>
<td></td>
<td>• Real-time intelligence</td>
</tr>
<tr>
<td></td>
<td>• Detailed attack forensics</td>
</tr>
</tbody>
</table>
How Sternum works

Here’s how Sternum helps MDMs meet HDOs’ growing needs as outlined in the playbook recommendations:

- **Mitigate unknown, known, and future threats**

  Proactively and directly protects all code in firmware (including third-party and OS libraries), thus reducing the need for patching and autonomously protecting a device from known and zero-day attacks.

  - Acting as an extended detection and response solution, Sternum’s patented EIV™ (Embedded Integrity Verification) technology provides agentless runtime protection for connected and isolated devices—delivering continuous exploit prevention even when a device is off the network.

  - For every attack, Sternum provides detailed attack forensics to conduct a root cause analysis and address the issue at the source.

- **Provide preemptive threat intelligence**

  (1) Indicators of exposure and compromise, (2) early alerts on emerging issues, as well as (3) tracing unusual behavior back to overlooked security gaps enables Sternum to surface hidden threats and activities that could lead to added exposures. It provides a correlated view of both security and quality to quickly resolve issues.
How Sternum Helps MDMs Meet The New Roles & Responsibilities

<table>
<thead>
<tr>
<th>Medical Device Procurement</th>
<th>FDA-MITRE Playbook Readiness &amp; Response Activities</th>
<th>How Sternum Helps MDMs Support HDOs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actionable and product-specific information to enable a timely response</strong></td>
<td>Sternum enables manufacturers to maintain a fleet-wide inventory along with detailed device profile information such as firmware/software/OS version, alert and deployment status, 'last seen' time stamp, location, connectivity status, etc.</td>
<td></td>
</tr>
<tr>
<td>In addition, alerts on attack attempts, departures from expected performance specifications, and malfunctions are shown in Sternum’s cloud analytical and visibility solution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tangible patches/fixes to contain and eradicate the threat.</strong></td>
<td>Sternum stops zero-day attacks, safeguarding the integrity of the device including third party software, protecting HDOs from known and unknown exploits of vulnerabilities. Vulnerabilities are neutralized, obviating the need for a security patch. A vulnerability which cannot be exploited is not a risk.</td>
<td></td>
</tr>
<tr>
<td><strong>Timely notifications of newly discovered vulnerabilities or of successful incidents against infrastructure that can impact HDOs' clinical operations.</strong></td>
<td>Sternum uses its on-device presence to monitor device activity, notifying in near-real time of attacks, exploits, departures from normal operations, and other incidents. Along with the forensic steps leading up to the notification. It prevents exploit attempts in real time and alerts on them, even before the vulnerabilities are discovered.</td>
<td></td>
</tr>
<tr>
<td>Once vulnerabilities are discovered, MDMs can notify HDOs that their devices are protected from the exploitation of a given vulnerability, avoiding a need to patch. Sternum also provides a software bill of materials (SBOM) to inventory all components and identify vulnerabilities within third party software.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Response/recovery support to the HDOs such as recommendations for mitigation and continued operations.</strong></td>
<td>Sternum gives manufacturers a live view of its device fleet, enabling real-time assessment of the security and functional condition of different devices and groupings of devices, and providing real-time awareness and data for recommendations on incident response. Knowledge of an attempted or unfolding incident at the level of the device gives the MDM info to know if an attack has been attempted, if it is prevented, and what steps need to be taken to contain it, if any, with minimal disruption to operations.</td>
<td></td>
</tr>
<tr>
<td>In the case of an attempted exploit, the MDM would be able to advise the HDO that the exploit is prevented by Sternum, with no imperative to remove the device from operation or patch it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In the case of a discovered vulnerability, from CISA for example, the MDM would be able to advise the HDO that the vulnerability is protected from exploitation by Sternum.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Medical Device Inventory**

| Provide HDOs a Software Bill of Materials (SBOM) for HDOs to identify and address vulnerable device components and have a query capability to maintain the device asset inventory. | Sternum closes the gap of SBOM by preventing zero-day exploits of vulnerabilities in both inventoried and un inventoried software. With or without SBOM, there is a need to actively mitigate vulnerabilities. |

**Detection and Analysis**

| Manufacturers must communicate emerging cyber issues and/or solutions to HDOs on a timely basis and provide additional insights on mitigation. | Sternum provides MDMs with real-time alerts on cybersecurity attack attempts and IoCs, as well as contextual data. This arms them with information to help HDOs identify events, characterize risk, and determine mitigation. |

| Be an external source and provide additional insights on the vulnerability, malware, and/or potential exploits. | Sternum provides a continuous real-time view of the security state of all devices, allowing it to identify attack attempts at the level of the device, the HDO, or the fleet. With this information, MDMs can advise the HDOs immediately, permitting a resolution before a disruption can impact the device, the end user, or the deployment environment. |