

Strategies for Mitigating Medical Devices Cyber-Security Threats

Amir Magner, CEO, CyberMDX

Connected medical devices are one of the weakest links within clinical networks, yet the most critical assets. Healthcare providers rely on connected medical devices for their clinical workflows and life-saving treatments; however, unlike other IT assets, these devices reside in the shadows, hardly visible by IT control systems and are poorly protected. 77% of healthcare organizations are primarily concerned about non-secure medical devices and the potential risk they create to patient's safety and operational continuity, yet most of them lack proper solutions in their toolbox to address the problem. As part of this presentation, we will demonstrate a short medical device hacking demo as well as the root causes of why medical devices are so vulnerable, why long vulnerability periods are inevitable, and what is so different in protecting medical devices versus generic enterprise IT assets. These are the main drivers to seek new paradigms and solutions outside the generic security solutions space. We propose fundamental strategies that can help healthcare providers to mitigate threats and manage the cybersecurity risk related to medical devices and the clinical networks.

About CyberMDX

CyberMDX provides healthcare centers with cybersecurity technology to protect their connected medical devices and clinical networks. We combine our attacker perspective and rich defense experience to create a new, revolutionary solution to the problem. CyberMDX has successful deployments in multiple healthcare facilities.