医疗器械的网络安全

什么是医疗器械的网络安全?

医疗器械的网络安全对于保护患者的数据和生命以及保护医疗机构免受恶意软件攻击至关重要。随着医疗器械的演变及其连接性的增强，网络威胁也呈现出复杂多变的趋势，不断催生出新型风险挑战。

为什么医疗器械的网络安全如此重要?

医疗器械网络安全所面临的威胁具有多元化的特征，这凸显了遵循前沿认证与标准并开展网络安全评估的重要性。构建全面的风险管理体系，需深度融入产品全生命周期的各个环节，辅以精准的渗透测试手段，旨在精确诊断潜在的安全漏洞，进而实施针对性加固措施，全面提升医疗器械的安全性。

医疗器械的网络安全风险和要求

医疗器械的网络安全风险包括:

- **法规要求:** 医疗器械受到如美国的FDA、欧洲的EMA、中国的NMPA等机构的严格监管。法规要求医疗器械的制造商遵守特定的网络安全标准和指南，以确保器械免受黑客攻击和其他网络威胁。不合规可能导致严重的处罚、召回或禁令。
- **患者安全:** 医疗器械的网络安全漏洞可能对患者造成严重后果。试想心脏起搏器或胰岛素泵被入侵后，可能导致关键时刻失效，或向患者施以错误的治疗剂量，直接威胁患者的生命安全。

- **隐私与中断：** 由于医疗器械通常存储和传输敏感的健康信息，安全漏洞可能会暴露个人健康记录，导致身份信息等敏感数据泄露。此外，恶意攻击者还可能通过勒索软件加密关键数据并要求赎金来解锁，这类攻击不仅会危及患者隐私，还会中断医疗系统的关键操作。这些潜在的风险凸显了网络安全措施的必要性。

医疗器械的网络安全标准和指南

鉴于所涉及的风险，医疗器械的网络安全需要经过严格的国际和国家标准测试。全球各地的监管机构发布了有关医疗器械网络安全监管的指南，并概述了设备上市前需要通过的测试。Applus+ Laboratories可以支持您应对以下标准：

- **MDCG 2019-16 欧盟医疗器械网络安全指南：** 确保欧洲市场上医疗器械数据的完整性和保密性。
- **美国 / FDA 医疗器械网络安全指南 - 质量体系考量和上市前提交内容：** 在美国监管框架下，从设计到部署阶段的网络安全指南。
- **IEC TR 60601-4-5 医疗器械网络安全标准：** 全球范围内医疗器械网络安全标准的技术路线图。
- **IEC 81001-5-1 医疗软件和健康IT系统产品生命周期中的安全活动标准：** 在器械的整个运营生命周期内维护网络安全的策略，适用于全球范围。

为什么选择Applus+ Laboratories进行医疗器械的网络安全测试?

Applus+ Laboratories提供全面的网络安全测试服务，以评估医疗器械，并且我们在进行网络安全评估和对各种评估目标（TOEs）进行渗透测试方面拥有极为丰富的经验。

安全测试

Applus+ Laboratories提供广泛的渗透测试服务，以评估系统对攻击和未经授权访问的抵抗力。通过进行网络攻击模拟，我们评估医疗器械各个组件中的漏洞：

硬件

实验室专家开发的最先进攻击和临时工具：

- 故障注入
- 侧信道
- 逆向工程
- 设计审查
- 逻辑攻击

- IC/SoC 攻击
- PCB 硬件破解
- 生物识别攻击

软件和固件

在嵌入式系统、安全启动、TEE 和白盒加密方面有扎实的背景：

- 二进制逆向工程
- 静态攻击
- 源代码审计
- 调试
- 模糊测试
- 动态篡改 / 挂钩
- 软件定时分析 and CCA
- 符号执行

通信协议

针对 IP 协议栈协议、工业系统和专有协议：

- 所有层次的攻击（OSI 模型），包括定制的硬件以在较低层次进行刺激（有线和无线协议）
- 模糊测试
- 动态篡改 / 挂钩

我们深厚的网络安全专业底蕴，为所倡导的安全策略注入了更为坚实的信心支撑。在Applus+ Laboratories专业的网络安全实验室环境下，我们精心策划的渗透测试将显著提升了产品的网络防护力与韧性。由Applus+ Laboratories的网络安全专家出具的报告符合全球监管机构（如美国FDA）对医疗器械网络安全测试的要求。

合规性验证

我们还可以支持医疗器械制造商验证其产品是否符合全球不同监管机构所要求的特定标准或指南。我们的合规性证书有助于产品在各类市场的审批流程中做好准备。

选择Applus+ Laboratories，携手开启医疗器械网络安全的测试与认证之旅，为您的产品实现尽快上市保驾护航。