

Medical Device Cybersecurity Analysis

An Engineering Approach to Security

- Determine security objectives
- Establish a control and baseline
- Define assessment plan
- Apply test criteria to the device
- Utilize reverse engineering and forensic techniques
- Report and rank vulnerabilities and risks
- Make recommendations to improve security posture

How well do you know your medical device security?

You should have security goals for every medical device and application you use. In order to meet these goals and security best practices, you have to understand how well-protected and resilient to attack each medical device you have deployed is, including in relation to the networks the medical devices are on.

This means you need to understand the threats you face and configure systems appropriately for your environment. This can be a daunting task for any enterprise, much less the increasingly mobile and resource-strapped medical environment. To fully understand the risk associated with your medical devices, you'll need a comprehensive assessment of your medical devices and your medical device network environment, in the context of their potential vulnerabilities, as well as your organizational guidelines, compliance needs, and use cases.

What can Owl do for you?

We help you secure your medical devices and network, protecting your clinical assets and enabling you to deploy and operate with confidence. Our experienced medical device cybersecurity research team evaluates your medical devices and network to identify vulnerabilities and then recommends solutions.

We go beyond standard lists of security controls to define your specific security objectives. We will work with you to understand your security goals, rank vulnerabilities and determine the best methods to harden your security with the least impact on cost and schedule.

By approaching your medical devices and network like an attacker would, we evaluate if your medical devices and network environment is secured appropriately, while allowing your system to function as designed. In addition, we ensure that your solution complies with best cybersecurity practices, standards, and regulations, such as from HHS, NIST, FDA, SANS, and DHS.

Trusted Experience

Why Owl?

Owl Medical Device Cybersecurity Analysis helps you confidently design, build, and implement a secure network of medical devices, ensuring the security architecture is appropriate for the intended use of the medical devices and medical device network.

Our services include white box, gray box, and black box testing. Using proven methodologies, our experienced cybersecurity professionals find what you don't know. By dissecting your product and analyzing it for vulnerabilities against agreed-upon security objectives, we uncover the unknowns related to security posture, risk, liability, and regulatory compliance.

For your analysis, we deploy a team of subject matter experts in multiple technologies, including:

- System and architectural security
- Operating system internals
- Network security
- Secure mobile operating system development
- Authentication and authorization technology
- Forensics inspection and analysis
- Penetration testing
- Threat Modeling
- Exploit development and fuzzing
- Wireless, Bluetooth, and Near Field Communications (NFC) inspection
- Black-box, Gray-box, White-box testing
- Reverse engineering
 - Computers (servers, laptops, workstations, etc.)
 - Mobile devices (phones, tablets, NFC endpoints, Bluetooth, WiFi, etc.)
 - Infrastructure hardware (routers, switches, firewalls, IDS/IPS, etc.)
- Security Enhanced Linux (SELinux)
- Pre-certification security audit

OWL Cyber Defense

We are a leader and trusted partner in cybersecurity. Our in-depth solutions are vital to helping our defense, intelligence, federal civilian agency and critical infrastructure customers meet ever-evolving cybersecurity threats. From network and perimeter defense, to product security analysis, to the practical application and hardening of SELinux operating systems, we deliver solutions that protect and connect the world's most critical networks.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com



@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com