CYLANCE CONSULTING

Medical Device Security Assessment

Secure and Protect Patient Care Systems

Benefits

- Identify potential threats to networked medical devices
- Ensure proper safeguards are in place to reduce the risk to patients due to a cyber attack
- Limit medical device access to only trusted users
- Protect individual components from exploitation
- Maintain a device's critical functionality

Data breach cost in the healthcare segment, the highest among 17 verticals studied.

Source: Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview

The capabilities of modern medical devices continue to radically transform patient care, but also can present a danger to patients through ever-present cyber threats. For years, security researchers have been uncovering security flaws in medical devices, raising concerns of tampering. All medical devices that use software and are connected to networks have vulnerabilities which can be proactively protected against while others require vigilant monitoring and timely remediation. Better patient care is the goal for all healthcare institutions.

Cylance® Consulting's Medical Device Security Assessment helps medical device manufacturers and healthcare organizations to **better secure and protect patient care equipment and systems from cyber attacks**. Our dedicated team of IoT and Embedded Systems experts helps to **assess vulnerabilities and develop a plan for responding to them**, starting with the design phase.

Service Overview

Cylance Consulting will perform a black-box assessment of the medical device, including both manual and automated testing techniques. The in-depth analysis of embedded vulnerabilities will be covered at a technical level, focusing on the common vulnerability types that can be found in embedded applications.

Specific areas of the assessment include:

- **Data Flow Analysis —** Trace data points from input to output, including storage and destruction, to identify potential weaknesses
- **Control Flow Analysis —** Identify threats by stepping through logical conditions and identify all possible paths through which code may traverse
- **Structural Analysis —** Evaluate the security of high-level architecture at multiple tiers and the composition of the application and its subsystems, including physical deployment characteristics
- **Configuration Analysis —** Assess the security configuration of all relevant components to identify vulnerabilities
- **Semantic Analysis —** Analyze the code base within the application's context to identify vulnerabilities unique to the application and environment

About Cylance Consulting

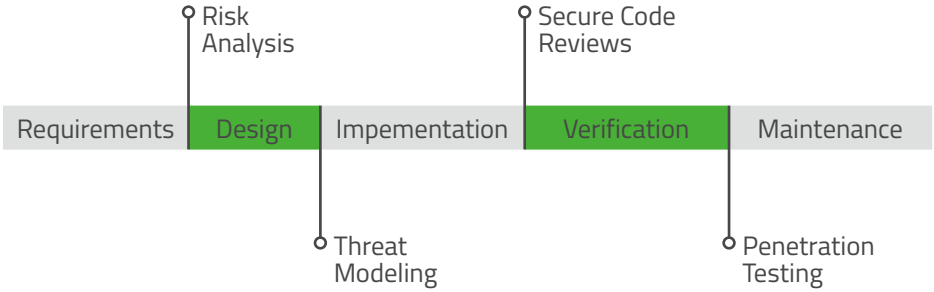
- World-renowned experts work synergistically across practice areas to deliver consistent, fast, and effective services around the world
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to *prevent* attacks from happening
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to not impact operations in any way
- Integrated practice areas: ThreatZERO™ Services, Incident Containment and Forensics, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, Strategic Services, and Education

Deliverables

As part of the security assessment, Cylance Consulting will provide a comprehensive report detailing:

- Our findings with any potential indicators of compromise
- A graphical summary of testing results
- A strategic remediation roadmap, including:
  - Finding name with details
  - Vulnerable host/IP
  - Vulnerability severity
  - Detailed recommendations
  - Screen shots
  - Assigned owner and remediation priority

Improve the security posture of your healthcare ecosystem. Contact Cylance Consulting or your technology provider to discuss your needs.



+1-877-973-3336
proservices@cylance.com
www.cylance.com/consulting

CYLANCE

20181108-2773