wurldtech
A GE Company

Device Security Assessment Datasheet

Business Challenge

As the threat of cyber attack against industrial control, automation and real-time systems grows, device manufacturers are under increasing pressure to provide robust and reliable products to their customers.

Solution

Wurldtech's **Device Security Assessment** is a comprehensive, in-depth evaluation and test that identifies device and system weaknesses and vulnerabilities to help manufacturers address issues throughout the product development lifecycle

Benefits

- **Enhances product security** by minimizing misuse of devices by cyber attackers and device failures caused by network anomalies
- **Reduces operational costs** by discovering and addressing device weaknesses during the development lifecycle, and by reducing public disclosures, field calls, and product recalls
- **Improves customer confidence** by showing measurable value by improving device robustness and reliability
- **Reduces liability exposure** by adhering to industry best practices for risk mitigation and ensuring proper documentation of implemented preventative security measures

Device Security Assessment

Cyber attacks on critical infrastructure are increasing and they are a growing concern for both system operators and the device manufacturers who supply equipment to these systems.

However, protecting these systems can be difficult. SCADA network devices are often located in areas that are challenging to physically access (e.g. on oil rigs or on industrial machinery). They are also difficult to patch due to access limitations, concerns over downtime, the need to re-certify and use of proprietary or special protocols.

To help reduce the risk of a public breach and to help enable compliance, Wurldtech's Device Security Assessments can be conducted throughout the development lifecycle. Ideally, the analysts will discover weaknesses before the device is deployed in the field. The assessments are based on technical expertise developed over many years as a leader in industrial security assessments, protection and certification.

Challenge

Critical Infrastructure is increasingly targeted for cyber attack and system operators are experiencing cyber incidents at an ever-expanding rate. They need to understand the risks to the systems they are deploying and the weaknesses that attackers may exploit. A comprehensive risk mitigation plan must include robust device security across all equipment and devices.

In the face of changing end-customer needs, device manufacturers are under pressure to deliver innovative products, but are often pushed by competitive forces that prompt expedited delivery that increases the risks of device bugs and vulnerabilities. Manufacturers need to understand the security vulnerabilities of their products, as well as their customers' compliance requirements with industry standards and security best practices.

Solution

Wurldtech's Device Security Assessment identifies device weaknesses and vulnerabilities to help manufacturers address issues early in the product development lifecycle. This comprehensive, in-depth assessment also provides mitigation recommendations to help prevent the exploitation of devices already deployed in the field. The Device Security Assessment is designed to offer flexibility in scope, allowing for customization for each embedded device assessment to meet specific customer needs and prioritized concerns. Wurldtech's security analysts use a lab environment to mimic malicious attackers to fully evaluate hardware and software for components, devices and the overall system.

Features

Each assessment includes:

- In-depth assessment analysis of device
  - > Focus on quality
  - > Discover and analyze vulnerabilities, even ones not immediately exploitable
  - > Test areas of greatest customer risk and need
  - > Evaluate attacker-accessible interfaces and high impact areas

- Process*
  - > Hardware teardown
  - > Identify internal targets of interest (attack interfaces, stored memory devices processors, etc.)
  - > Memory/Firmware extraction
  - > Reverse engineering
  - > Vulnerability analysis and discovery
  - > Protocol/Communications analysis
  - > Management and monitoring system evaluation

- Findings Report

**This is a sample only – process may vary depending on device under test.*

BENEFITS	
Enhances product security	Improves device security and reliability and reduces need for product patching
Protects brand reputation	Reduces the risk of a breach in your product and avoid public vulnerability disclosures
Lowers product maintenance costs	Reduces costs by addressing product weaknesses during development; service calls to the field to address security vulnerabilities are very expensive
Increases customer confidence	Delivers improved product security

DELIVERABLES	
Regular status calls	• Provides detail on discovered vulnerabilities so that clients can immediately plan mitigation steps
Actionable report	Includes: • Executive Summary • Overview of Assessment • Components under test/test bench • Description of methodology, test process and results for each component including vulnerabilities discovered and the skill of attacker required to identify and exploit each vulnerability • Description of system-level issues and impacts (e.g., how does a vulnerability in one component affect the system) • Description and prioritization of remediation steps to address weaknesses • Conclusions and next steps
Closeout calls	• Covers the weaknesses/vulnerabilities found, the priority in which they should be addressed and strategies to mitigate the risk of each weakness

The Wurldtech Advantage

Wurldtech's deep experience in critical infrastructure includes the detailed analysis of the most extensive set of devices and systems from all of the major critical infrastructure manufacturers. The security analysts' experience includes penetration tests on devices from more than 25 manufacturers in the areas of industrial control, PLC, DCS, Smart Grid and medical. The analysts' broad skillsets includes hardware reverse engineering, tool development, non-IT and OT communications, extensive security and ICS domain knowledge, as well as analysis from local and remote perspectives, vulnerability analysis and exploit development. Wurldtech customers include 9 of the top 10 automation vendors.

Wurldtech device assessments include comprehensive reports with actionable insights: clear descriptions of vulnerabilities discovered and mitigation steps to address each weakness, to help get you started on immediately improving the security of your products.

Wurldtech customers include 9 of the top 10 automation vendors

Summary

Wurldtech's Device Security Assessments help manufacturers discover and resolve device weaknesses early in the product development lifecycle, ensuring customer confidence and saving money, time and brand image by reducing the risk of a public vulnerability breach. Detailed reporting with actionable insight provides clear descriptions of all vulnerabilities discovered, the level of attacker skillset required to exploit each vulnerability and steps to address and mitigate each weakness. Mitigation advice considers product design limitations and recommends reasonable steps for implementation.

COMPARISON OVERVIEW

Device Security Assessment vs. Device Security Health Check

	Device Security Assessment	Device Security Health Check
Methodology	Comprehensive, in-depth assessment	Rapid, economical penetration testing
Size and scope	Tailored for system under test	Pre-set
Report length	Comprehensive	Overview
Areas of focus	Customer and analyst scoping	Analyst scoping only
Regular update calls	Yes	No
Mitigation advice	Yes	No
Multi-device systems	Yes	One device and one firmware /software version only
Report distribution	Client and client's customers	Client only (no report distribution rights)*

**For system operators, can distribute to the respective device manufacturer*

NEXT STEPS

For more information or to schedule training, please contact Wurldtech sales:
Toll free: 1 877 369 6674
Email: sales@wurldtech.com
or visit **wurldtech.com**