InterSec
Ignite . Inspire . Innovate

Enhancing IIoT Security Through Penetration Testing: A Major IoT Provider Secures Over 2,000 Products

The Client: A Global IOT Provider

Established in 2010, our client is a major force in the Internet of Things (IoT) industry, boasting over 52,000 global customers, more than 39 billion data readings, and over 2,000 product SKUs. They specialize in delivering high-value IoT data to businesses worldwide.

This Industrial Internet of Things (IIoT) leader serves 52,000+ global customers and generates more than 39 billion data points, relying on industrial control protocols (ICS) like Modbus and RS-232. Traditional pen tests often miss ICS-specific vulnerabilities. Facing the immense challenge of securing an extensive IoT network, they recognized the need for rigorous security evaluation and engaged us for penetration testing.

InterSec deployed an advanced ICS Pentesting Strategy, unearthing hidden vulnerabilities while preserving the integrity of thousands of deployed devices.

Better security procedures now protect high-value IoT data and maintain uninterrupted service.

- 2,000+ distinct IIoT devices across sensors, gateways, and ICS protocols
- 52,000+ global customers requiring reliable data streams
- Billions of real-time data points influencing critical operational decisions
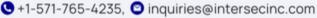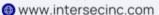
🔲 Problem/Challenges

Securing a huge inventory of IoT devices, many of which run specialized ICS protocols, required an approach that went deeper than typical penetration testing methods. Missing these intricacies could devastate critical data flows.
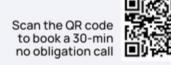
Capabilities Demonstrated:

ICS/IoT Penetration Testing, ICS/Industrial Control Protocol Expertise (Modbus, RS-232), Specialized Lab-Based Hardware/Firmware Analysis, Risk-Based Vulnerability Prioritization, Minimizing Downtime/Operational Disruption

Business Contact
📞 +1-571-765-4235, ✉ inquiries@intersecinc.com
📍 13800 Coppermine Road, Herndon, VA 20171 I Work Area: Nationwide
🌐 www.intersecinc.com

Scan the QR code
to book a 30-min
no obligation call

- **Expansive Attack Surface:** Thousands of devices across diverse environments
- **ICS Protocol Complexity:** Standard scanning overlooks specialized industrial channels

- **High-Value Operational Data:** Reliability and uptime are crucial for client success

⊕ Approach & Strategy

InterSec leveraged extensive ICS expertise to tailor penetration tests specifically for these protocols, ensuring no hidden vulnerabilities escape detection.

- **Custom ICS Pentesting:** Created targeted scenarios for Modbus, DNP3, and RS-232
- **Risk-Based Prioritization:** Focused first on devices carrying the highest operational impact

- **Coordinated Downtime Minimization:** Collaborated with IT and DevOps to reduce business disruption

🎁 Solutions and Implementation

We deployed a specialized testing lab that emulated real industrial environments, conducted thorough hardware and firmware analyses, and shared actionable remediation recommendations.

- **Specialized Testing Lab:** Mirrored real-world ICS conditions for accurate threat simulations
- **Comprehensive Pen Tests:** Probed hardware, firmware, and network flows for potential breaches

- **Knowledge Transfer:** Delivered detailed remediation steps and ICS security best practices
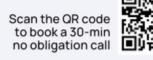
💰 Results & Outcomes

This deep-dive approach uncovered critical vulnerabilities before they could be exploited, securing data streams for tens of thousands of global customers.

- Focused remedial actions **reduced major exploitable flaws by 90%**
- **Minimized device security across 52,000+ customers**

- **Demonstrated commitment** to safety and reliability in competitive IIoT markets

Worried about ICS vulnerabilities in your IIoT ecosystem?

Contact InterSec for specialized penetration testing that safeguards high-value data flows and devices at global scale.

Business Contact

📞 +1-571-765-4235, ✉ inquiries@intersecinc.com

📍 13800 Coppermine Road, Herndon, VA 20171 I Work Area: Nationwide

🌐 www.intersecinc.com

Scan the QR code
to book a 30-min
no obligation call