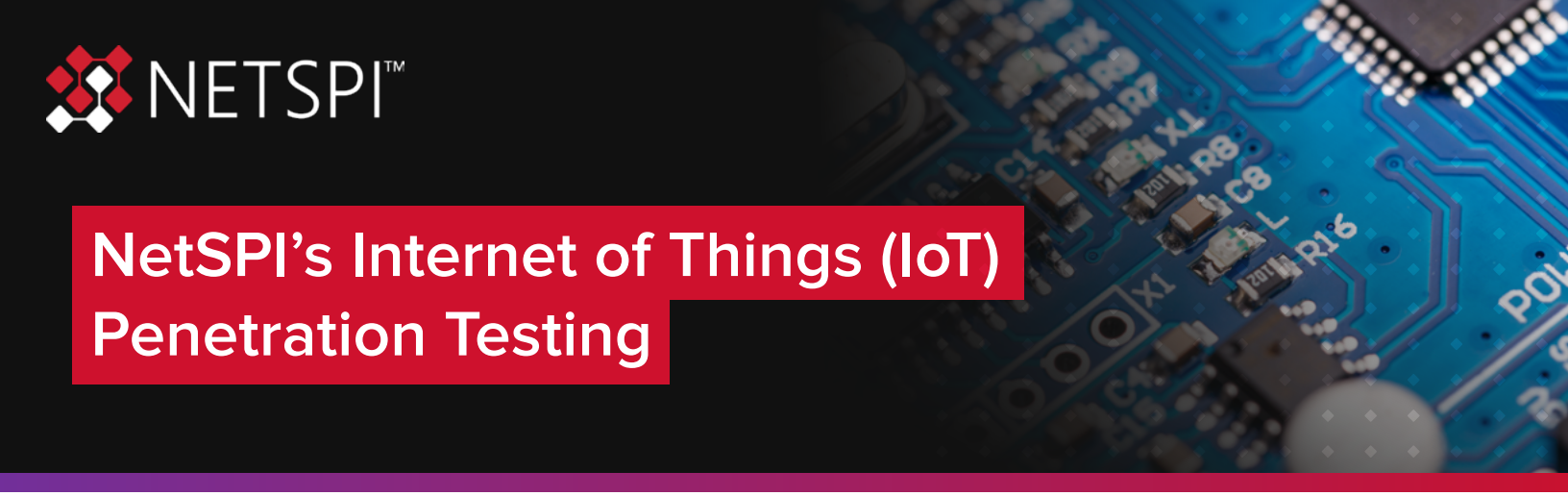
NETSPI™



NetSPI's Internet of Things (IoT) Penetration Testing

Secure ATMs, Automotive Technology, Medical Devices, Operational Technologies, and other embedded devices at risk of a cyber-attack.

With immense IoT adoption over recent years, and anticipated continued growth in the future, IoT device penetration testing has become critical for companies that want to understand, assess, and improve overall security and accountability of their devices and systems.

NetSPI's IoT Penetration Testing is specifically designed with a proven pentesting methodology from over 15,000 engagements and decades of manual testing experience, along with a deep understanding of Threat Analysis and Risk Assessment methods to ensure standards such as ISO, SOC2, and more aren't just met, but exceeded.

NetSPI IoT Testing Categories:

ATM – During ATM Penetration testing we will identify security vulnerabilities through assessing a combination of thick client applications, hard drive encryption, kiosk escape, peripheral security, secure memory configuration, breach simulation, vulnerability enumeration, sensitive data and critical system access, physical security controls, peripheral firmware, and sensitive information storage.

AUTOMOTIVE – Identify security issues on relevant vehicles at any stage of automotive development. NetSPI's approach to identifying automotive vulnerabilities focuses on the individual components as well as how those components interact with each other and the outside world. The testing approach includes the assessment of mobile applications, thick client applications, connected environments, internet connectivity, hardware, internal networks, sensor data, and containers and hypervisors.

MEDICAL DEVICE – IoT innovation in healthcare can be game-changing, but only if done securely. Medical device penetration testing determines possible design flaws in the software, hardware, and communication methods that could weaken the security of the device as well as determine if current FDA security standards and recommendations are met. The testing approach includes a combination of threat modeling and penetration testing of the firmware, hardware, wireless configuration, default failure, the network, thick client applications, mobile applications, sensor data, privacy/tracking, and potential health and safety issues.

NETSPI

OPERATIONAL TECHNOLOGY – NetSPI identifies industrial control system (ICS) vulnerabilities with a focus on the OT processes in a Defense in Depth strategy. We use an information gathering approach, working from packet capture, architecture review, and interviews to establish both an asset inventory and better knowledge of your systems and processes. The testing approach includes architecture review, passive asset inventory, active asset inventory, active network testing, programming review, main system hardening, thick client application testing, threat vectors, and attack simulation.

EMBEDDED – During an embedded penetration test, NetSPI looks for security vulnerabilities at all stages of embedded development that may affect each layer of the device. NetSPI's approach to identifying embedded system vulnerabilities is a multi-tiered penetration test across multiple disciplines, including firmware, tamper protection, hardware, reverse engineering, destructive testing, wireless configuration, principle of least privilege, thick client application pentesting, secure storage, and peripheral security.

Results Delivered in NetSPI's PTaaS Platform

Real-Time Reporting
Get notified of vulnerabilities in platform as they are found.

Remediation Guidance
Vulnerabilities are delivered with remediation instructions and consultant support.

Project Management & Communication
Effortlessly assign responsibilities, track remediation status, communicate with teams, and more.

Track & Trend Data
Analyze findings and discover trends over time.

To learn more about NetSPI's IoT Pentesting, or any of our other offerings, visit www.netspi.com or contact us.

Platform Driven, Human Delivered

ASM | BAS | RESOLVE

Attack Surface Management • Breach and Attack Simulation • Penetration Testing as a Service
Application Pentesting • Cloud Pentesting • Network Pentesting • AI/ML Pentesting • IoT Pentesting
Blockchain Pentesting • SaaS Security Assessment • Secure Code Review • Cybersecurity Maturity
Red Team Operations • Social Engineering • Strategic Advisory

About NetSPI:

NetSPI is the global leader in offensive security, delivering continuous and scalable penetration testing, attack surface management, and breach and attack simulation solutions to the world's most prominent organizations.