SERVICE SHEET

Penetration Testing

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organization – your people, your operations, and your reputation.

FTI Cybersecurity offers high-value, intelligence-based penetration testing services that simulate the activities of real-world attackers to find vulnerabilities in target systems and exploit them under controlled circumstances.

The objectives of a penetration test are to assess a security team's readiness, cooperation between internal teams and outsourced security providers, security vulnerabilities and gaps, security tools and defenses, and incident response capabilities and processes.

Our Capabilities

- Internal Network Penetration Test
- External Network Penetration Test
- Application Penetration Test
- Wireless Penetration Test
- Red Team Simulation

Our Deliverables

- Tactical and strategic recommendations for immediate and long-term security enhancement, prioritized to add the maximum, immediate impact to your security program
- Fact-based risk analysis to prioritize decisions regarding validating specific assets or implementing measures to remediate vulnerabilities
- Technical details that include information to recreate our findings
- Summary of findings for executive and senior management

BENEFITS OF PENETRATION TESTING

- **Provide intelligence and insight on whether critical assets are at risk**
- **Identify and mitigate complex security vulnerabilities before they are exploited**
- **Understand the tactics, techniques, and procedures deployed by most sophisticated attackers**
- **Attain real-world results and comprehensive recommendations**
- **Discover high risk concerns that could lead to a costly data breach or cybersecurity incident**
- **Ensure in-house security teams and tools are up-to-date and "battle-tested"**

External Network Penetration Test

Our external network penetration test is designed to test the effectiveness of perimeter security controls in preventing and detecting attacks, as well as identifying weakness in Internet-facing assets, such as web, mail, and remote services.

Application Penetration Test

Our application penetration test analyzes the architecture, design, and configuration of web and mobile applications. Assessments identify security risks that could lead to unauthorized access, data leakage, or compromised assets.

Wireless Penetration Test

Our wireless penetration test is designed to identify unsecured wireless networks, such as rogue access points, weak passwords, Bluetooth, and default router configurations that can lead to unauthorized network access.

Internal Network Penetration Test

Our internal network penetration test simulates a malicious insider or an attacker who has gained access to an end-user system. Using automated breach tools and manual exercises, we determine how an attacker could move laterally throughout the network, which includes escalating privileges, installing custom malware, or exfiltrating critical data.

Red Team Simulation

Our red team simulation is performed by a team of qualified ethical hackers, leveraging the latest hacking tools and techniques to launch a simulated cyber attack. The purpose is to thoroughly test security maturity and threat detection and response capabilities.

CASE STUDY

SITUATION

FTI Cybersecurity was engaged by a global manufacturer of highly specialized, government and private grade connected devices to conduct a holistic vulnerability assessment. The scope included a low-level source code security review, API security assessment, cloud-based server infrastructure security assessment and penetration testing, hardware exploitation assessment, web-based and app-based control panel security assessment, and web application security scanning.

OUR ROLE

Our experienced source code reviewers, penetration testers, and hardware engineers identified security vulnerabilities and gaps that impacted data privacy, availability, and confidentiality, and made recommendations to improve the resiliency of the organization's infrastructure, products, and services.

OUR IMPACT

Using our independent analysis, the client implemented source code changes that altered how, when, and where the devices communicate.

CASE STUDY

SITUATION

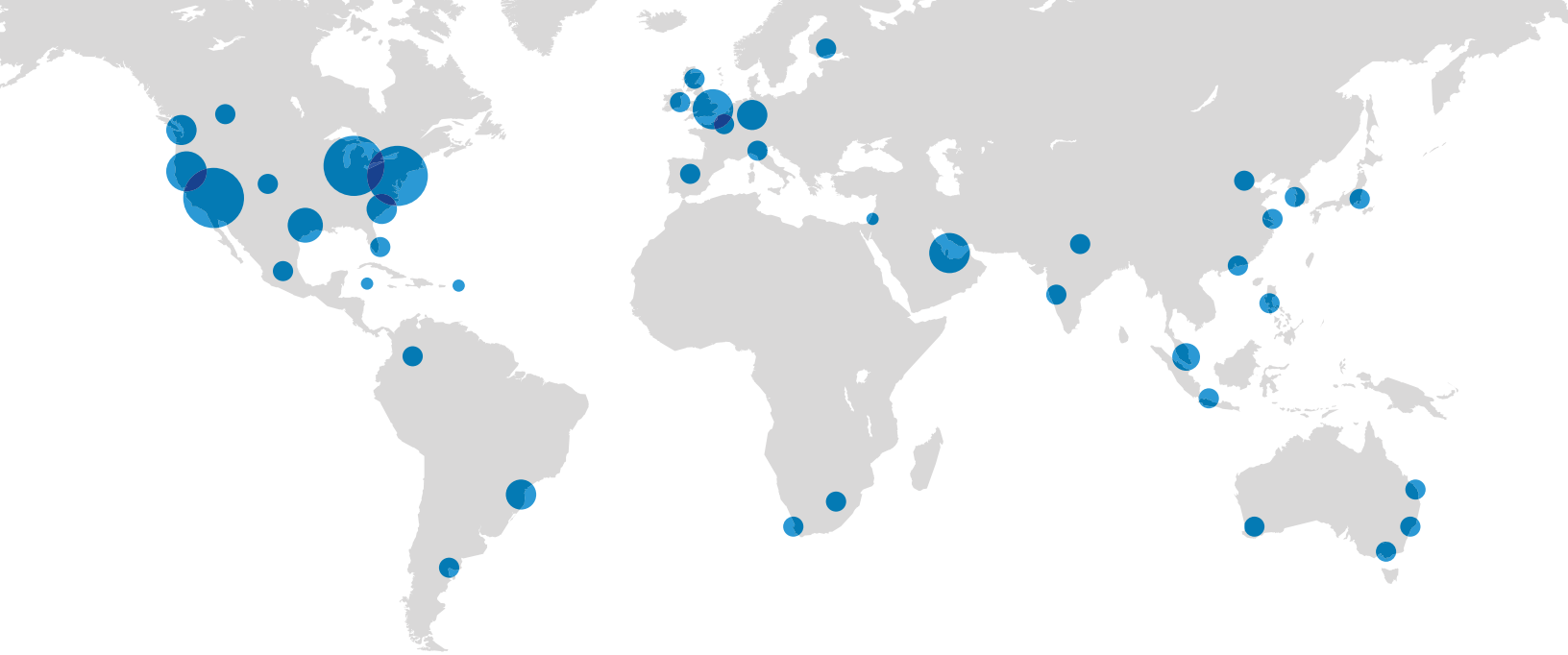
FTI Cybersecurity was engaged by a leading provider of ambulatory electrocardiogram (ECG) monitoring for patients at risk for arrhythmias. The company created a unique platform to quickly diagnose arrhythmias and was aware of the broader cybersecurity challenges affecting the bio-sensing technology. They were concerned that a cyber-attack could lead to the exposure of sensitive medical data.

OUR ROLE

We were engaged to execute a penetration testing program, which covered a web and mobile-based security assessment as well as testing of physical, networked devices. We evaluated the security concerns by effectively intercepting and manipulating web and mobile communications between the application and back-end services in an attempt to bypass security restrictions and identify potential methods of intrusion.

OUR IMPACT

Our analysis led to concrete and prioritized recommendations that enabled client's management to mitigate cyber risk and improve device security.



Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

1982

Year Founded and $5.7B equity market capitalization*

9/10

Advisor to 9 of the world's Top 10 bank holding companies

7,000+

Employees

NYSE:FCN

Publicly traded

98/100

Advisor to 98 of the world's top 100 law firms

59

59 of Fortune Global 100 corporations are clients

**Number of total shares outstanding as of July 21, 2022, times the closing share price as of July 28, 2022.*

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA & APAC
Senior Managing Director
+44 7816 251410
david.dunn@fticonsulting.com

FTI CONSULTING