SCORPION LABS

Penetration Testing

Scorpion Labs offerings empower organizations to gain a clear understanding of posture to proactively reduce risk and improve their programs, services and products. Our outcomes focus on both tactical findings and strategic advancement opportunities.

Our team believes in meeting customers where they are with our flexible, white glove approach. We spend time understanding your organization's business direction and vision, your unique organizational structure, technologies and key information security risks to determine the appropriate testing for your needs.

Our People:

- Elite offensive security practitioners with over 10 years average experience
- Adversary mindset, thinking beyond checklists
- Focused on business impact, not noise
- Decades of real-world experience across industries

Our Approach:

- Expert led and manual testing, driven by threats
- Source code driven methodology including deep analysis and end to end evaluation
- Real-world attack simulation with chain exploits that emulate threats
- Proof of exploitation with clear, replicable steps

APPLICATION & PRODUCT TESTING

Source Code-Driven Testing

Exposes impactful issues often missed by automated tools

Threat-Modeled Manual Testing

Simulates attacker techniques and logic flaws

Business Risk Focused Findings

Prioritized insights with tactical strategic guidance

- Web Applications & APIs
- Native Applications
- Reverse Engineering
- Mobile Applications
- IoT Devices
- Consumer and Enterprise Products

SCORPION LABS

Penetration Testing

INFRASTRUCTURE TESTING

Customized Threat Modeling

Scoped to your environment to uncover the most impactful vulnerabilities

Deep Reconnaissance

Enumeration to reveal overlooked attack surfaces

Manual Exploitation

Analysis demonstrating real compromise paths to sensitive systems

- Focus Areas
  - External and Internet Perimeter
  - Internal Network
  - Wireless Network
- Targeted Testing
  - Active Directory
  - Cloud Native
- Industry-Focused Testing
  - PCI, HIPAA

RED & PURPLE TEAMING

- Emulates real-world adversaries to test detection and response controls
- Research-backed techniques along with stealthy, low-detection paths and tradecraft
- Demonstrates compromise of the most critical assets to expose detection and response capabilities
- Surfaces technical and programmatic weaknesses in people, process, and technology
- Collaborative testing with customer/internal blue teams