

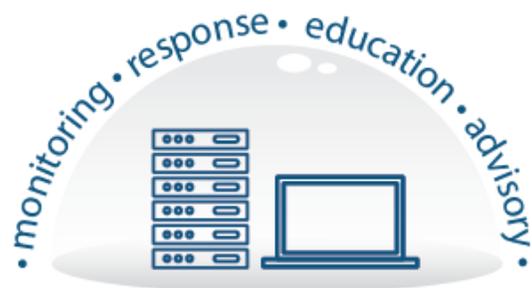
Penetration Testing Services

Proactively Mitigate Cyber Risks and Manage Threats

Every business understands the need for secure networks and the danger that hackers pose to their customers, their industry reputation and ultimately, their bottom line. Threats range from malware and viruses to phishing and denial-of-service (DoS) attacks. In response to these threats, businesses have implemented sophisticated security controls and incident response plans to counter the exponential growth of cyber attacks. But unless security and incident response is tested for potential weaknesses, hackers can exploit hidden vulnerabilities and inflict greater harm to your business. Companies need a complete understanding of their risk and exposure.

SecureIT's penetration testing services test and verify the effectiveness of currently deployed security measures.

Unfortunately, many so-called "pen tests" are actually nothing more than cookie-cutter vulnerability scans performed by unskilled resources. Such limited reviews add little value to clients since they fail to provide the desired insight into the real-life level of exposure that a pen test is intended to provide. SecureIT's approach deliberately goes beyond what automated tools can provide. Although we use scanning tools to help identify promising avenues of attack and use Metasploit and other published exploits that attackers leverage, we have found that manual testing, which requires more technical knowledge and sophistication to craft customized and nuanced attack scenarios, is always more effective than using automated tools alone.



SecureIT Penetration Testing Offerings

SecureIT provides a range of penetration testing offerings, based on our extensive knowledge of security risks and vulnerabilities.

SecureIT Offering	Description
External and Internal Network Testing	Both types of testing involve port scanning, vulnerability scanning, exploitation, and pivoting. External tests identify vulnerabilities or misconfigurations of internet-accessible systems and use those to gain access to internal systems. Internal testing centers on Adversarial Tactics, Techniques, & Command Knowledge (ATT&CK), a framework describing tactics an internal adversary may exploit.
Web Application Testing	SecureIT leverages the Open Web Application Security Project (OWASP), a comprehensive framework for assessing the security of web-based applications, as the core of our web application testing methodology.
Mobile Application Testing	We test mobile applications and the services they communicate with. The tests evaluate the same elements as Web Application Testing with emphasis on exploits of device data storage, permissions to access application resources, communication channels used, and many more.
Wireless Testing	A wireless penetration test maps out wireless access points and the strength of their encryption. Testing determines if there are mitigating controls in place to prevent unauthorized access.
Red Team Testing	Red teaming is a comprehensive test of physical, network, wireless, social engineering, and applications security. Testing simulates a real-world attack and focuses on discovering the weakest path to exploiting a vulnerability.
Vulnerability Identification and Management	SecureIT's vulnerability detection services inform owners of misconfigurations of services and can be used to meet certain regulatory compliance requirements. Included is a signature-based scan tailored to determine your exposed vulnerabilities. Outcomes go beyond a scan report as you gain command of the risks facing your business and prioritized remediation solutions.
Phishing/User Awareness Testing	We design a customized solution to test employees' ability and effectiveness in identifying suspicious emails. Emails containing links, attachments, and executable files will be sent to assess user awareness.
Periodic and Continuous Monitoring	In addition to point-in-time penetration testing projects, SecureIT offers managed external/internal service penetration testing and phishing tests to provide periodic or "real-time" visibility into areas of greatest security risks and vulnerabilities. Continuous external perimeter monitoring alerts you to any changes to your external addresses.

When engaging SecureIT for penetration testing services, you will always gain a comprehensive evaluation of your current security implementation. In addition, we will work closely with your staff to understand findings, provide prioritized improvement strategies, and recommend tools to help improve the security posture of your network and applications.

Our Penetration Testing Difference: Higher Confidence

SecureIT understands the need for stakeholder and regulator trust in your business because we are experts in both security and compliance. We design and carry out the most realistic penetration tests, which provide the most assurance that your security defenses are operating as intended. We understand that penetration tests are not simply pushing 'GO' on a scanning tool, rather they should be a real-world combination of tools and techniques leveraged by skilled security professionals, just like your adversaries. Don't just 'check the box', get a penetration test that delivers higher confidence.

About SecureIT

SecureIT provides risk, compliance, and cybersecurity services to enterprises, government entities, and cloud service providers. Our certified professionals assess cyber risk, conduct targeted security assessments, and ensure compliance with regulatory requirements. Every day, we partner with our clients to deliver solutions critical to protecting and growing business.

SECURE | IT

1818 Library Street
Suite 500
Reston, VA USA 20190
703.464.7010