

Federal government networks are prime targets. Persistent threats that are more sophisticated and continually adapting exploit weaknesses. Agencies must protect data and maintain availability while ensuring compliance with rapidly evolving security standards and policies.

OVERVIEW

SecureIT partners with the best in the industry to offer network security assessment services to identify security vulnerabilities and weaknesses which can be exploited in your network. We leverage our experience and knowledge of Federal government agencies, its processes and security policies together with our security experts and those of our partners to provide valuable and responsive analysis and actionable recommendations for remediating vulnerabilities. We deliver analysis using standards-based ratings to help our customers prioritize and support actions and risk-based decisions. We have constructed our services and deliverables to enable our customers to meet security control testing requirements to achieve and maintain Federal security certification and accreditation (C&A) as defined in NIST SP 800-37 and DIACAP. As an independent security services firm, we have assisted and are experienced in audits.

We work closely with your organization's personnel to ensure comprehensive, non-intrusive testing and to provide responsive assessment reports and remediation recommendations. We offer a team of security consultants with extensive Federal government experience in both operations as well as audit, and that hold security clearances and industry certifications.

SERVICES

Penetration Testing: SecureIT provides network penetration testing services to determine if, and to what degree, an organization's network assets can be breached. Through the use of automated tools, we gather system/network domain(s), IP addresses, host/network names, DNS records, operating system versions, hardware platforms, enabled TCP/UDP ports and services, and applications. This information is used to identify avenues of attack. We evaluate the existing network security processes and technology by attempting to circumvent implemented controls to gain access to critical assets.

Through identifying weaknesses, we provide your organization with factual information to focus resources and gain support for security-related initiatives. To meet Federal requirements for independent penetration security testing, we provide security testing to support certification and accreditation (C&A) based on NIST SP 800-37 and DIACAP as well as the ongoing security control continuous monitoring required to manage risk and maintain C&A. These services are performed from our facility.



Vulnerability Assessment: Using a combination of automated network-based scans and root-cause analysis, we assess an organization's internet security posture. This provides your organization with the critical network and operating system vulnerabilities. Our analysis identifies the potential root-cause of any identified weaknesses. We brief our customers to explain our methodology, the weaknesses and root cause and typically work directly with network and system administrators to determine the most effective mitigation for these weaknesses. We can perform configuration evaluations of an operating system, patch levels, and running services and make recommendations to lower risk and increase compliance with security baseline standards such as NIST, NSA and DISA.

Wireless Network Assessment: If your organization permits and uses wireless networking, SecureIT can provide assurance that they are deployed free of security vulnerabilities and in compliance with national and your agency security policies. If your organization does not permit the use of wireless networking, we can detect the unauthorized or unintended wireless access points and associated vulnerabilities.

War-Dialing: Many organizations still use modems for communications. Sometimes these modems are connected to systems that reside on the enterprise network. Additionally, many devices embed modems for remote access for maintenance. Frequently, these services are left open when not intended and pose security risks to an organization. SecureIT identifies these rogue modems, devices and instances where your organization may be vulnerable. We can perform an automated phone-based scan of a fixed set of phone numbers to identify any known, unauthorized, or unsecured access points that could pose a point-of-entry into your network.

CONTACT

SECURE | IT

Phone: 703.464.7010

Email: info@SecureIT.com

Web: www.SecureIT.com