Product Brief

Accedian Cyber Resiliency Services: Penetration Testing (Pentest)

Determine your resilience to cyber attacks and validate the security of your digital infrastructure

The maxim, “you can’t protect what you don’t understand” is especially true when it comes to securing today’s complex networks. The only approach to identifying where security gaps exist is to perform regular testing of the network. Not doing so leaves the entire organization susceptible to attack, and if a threat actor has already compromised the network, recovery can be both time-intensive and costly.

Acccedian’s Penetration Testing Services help you fully validate the security of your organizations digital infrastructure end-to-end. This includes the network, its resources, web applications, and more. We offer a full suite of pentesting services that meet your needs and budget requirements. Simply put, we help you find security weaknesses before the cyber criminals do.

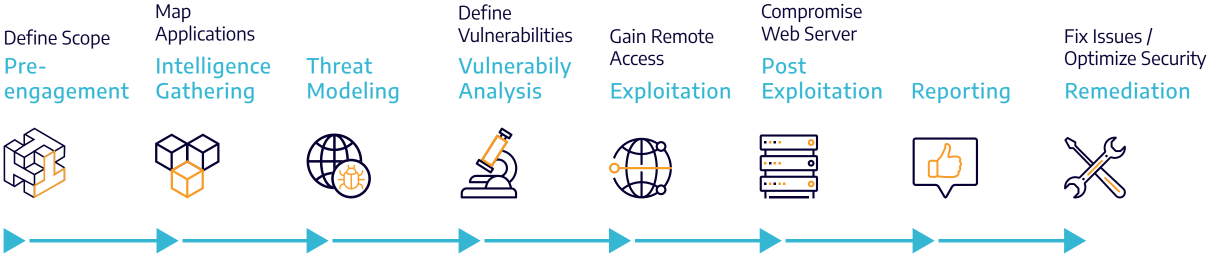
Confidence: Reduce risk and gain visibility and control of your network and its resources

Control: Prioritize your cyber defense goals and spend

Peace of mind: Meet and maintain regulatory compliance

Brand protection: Protect company reputation and maintain trust

Penetration Testing Approach



Define Scope
Pre-engagement

Map Applications
Intelligence Gathering

Threat Modeling

Define Vulnerabilities
Vulnerabily Analysis

Gain Remote Access
Exploitation

Compromise Web Server
Post Exploitation

Reporting

Fix Issues / Optimize Security
Remediation

Range of Customizable Penetration Testing Services

Penetration Test	Objective	Benefits
External Penetration Test and Vulnerability Assessments	Identify exploitable vulnerabilities or misconfigurations.	• Identify exposure and risk • Meet compliance • Validate security investment (ROI)
Internal Penetration Test and Vulnerability Assessments	Determine how an attacker could move laterally throughout the network and how deep the attacker or the malicious insider can reach. Test data exfiltration and MITRE coverage of your SOC/MDR.	• Shows the impact of compromised endpoints • Live Attack-Defense exercises determine business readiness in the event of a cyber attack • Demonstrate risks to C-level
Web Application Assessments	Test for possible data leakage points and vulnerabilities according to OWASP top 10. Assess source code and API security. Ensure customer data is safe. Test your WAF solution.	• Validate the security of your applications
Mobile Application Assessments	Test for platform-specific vulnerabilities. Audit the security of applications in the Android/iOS environment. Validate API and code-obfuscation.	• Avoid potential mobile attacks and identify at-risk mobile clients
Social Engineering	Social testing of employees to include phishing emails, verbal communication, office security.	• Validate your Security Awareness program and competency of your employees
Internet of Things (IoT)/ Embedded Device Security Assessments	Security assessment of various devices by attempting to exploit the embedded firmware, gain control by passing or injecting unsolicited malicious commands, or modify data sent from the device.	• Ensure new or existing IoT systems are safe to be used in your controlled environment • Meet IoT regulatory requirements • Ensure the legitimacy of IoT device communications
Security Controls Audits	Attestation of the assessments based on Industry Standards like PCI/DSS and NYDFS.	• Ensure your organization is meeting stringent regulatory requirements
Cloud Security Testing	Manual and automated scans for cloud security infrastructures such as AWS, GCP, Azure, etc.	• Validate the security of your cloud deployments
Elite Team of Certified, Experienced and Vetted Cyber Professionals	Our team is comprised of security professionals with decades of security experience and global certifications such as ISO, OSCP, OSCE, CEH, ISACA, OWASP, and more.	• Trusted experts with security clearances for your classified networks • Innovative ethical hackers identify vulnerabilities that machines may miss

Service Deliverables:

- Executive report detailing detected vulnerabilities and their business impact
- Detailed technical report detailing all evidence and artifacts, including videos and screenshots, providing the information needed to recreate our findings with IT and development teams
- Letter of Attestation validating compliance requirements
- Retesting Services that provide a “clean report” and confirms that all vulnerabilities and defects were fixed
- Itemized risk analysis confirming all critical findings are relevant to the targeted environment
- Actionable deliverables and tactical recommendations for immediate improvements
- Long-term security strategy with recommended actions to harden cyber resiliency and develop a more mature security posture
- Diverse open source and commercially available tools sets to ensure optimum test coverage

The only way to ensure your network’s cyber resiliency is to validate your digital security through expert penetration testing. Contact Accedian to get started today.

About Accedian

Accedian is the leader in performance analytics, cybersecurity threat detection, and end user experience solutions, dedicated to providing our customers with the ability to assure and secure their digital infrastructure, while helping them to unlock the full productivity of their users. **Learn more at accedian.com**