Network Penetration Testing

Our network penetration testing services are designed to assess your organization's security by simulating real-world cyberattacks, such as phishing and ransomware, using the same tools and techniques employed by threat actors. This testing helps you gain a comprehensive understanding of your cybersecurity strengths, weaknesses, and priorities.

As an impartial third party, we identify critical vulnerabilities across both internal and external networks. Our tests also evaluate whether these vulnerabilities are exploitable, providing a clear picture of the actual risks they pose to your IT security posture.

How Network Penetration Testing Works

We stay ahead of evolving cyber threats, uncovering current vulnerabilities and predicting future risks. Our scenario-based testing provides actionable insights that help you make informed security decisions. Our approach includes:

Continuous Threat Alignment
We adapt our testing methods to stay ahead of evolving threats.

Strategic Insights
Gain long-term strategic insights to improve your overall security posture.

Tactical Recommendations
We provide actionable, tactical recommendations to immediately address vulnerabilities.

What to Expect From Our Network Penetration Testing Services

- Access top-tier cybersecurity experts to protect your systems.
- Boost end-user security awareness to reduce threats.
- Confirm critical security controls are effective in real time.
- Empower your IT team with hands-on security training.
- Get continuous support and education to stay ahead.
- Receive a customized action plan to enhance security.
- Strengthen defenses against cyberattacks with immediate improvements.

Why Choose Schneider Downs?

Accurate Risk Diagnosis: Our detailed reports provide clear, actionable insights into your actual risks, helping you prioritize remediation efforts.

Comprehensive Risk Assessment: We identify both known and unknown risks, offering continuous partnership and support beyond the initial testing engagement.

Hacker Mentality: We simulate attacks with the mindset of a real-world cybercriminal, ensuring our tactics closely mirror actual threats.

Proven Expertise: Our team combines deep technical expertise with real-world experience across various industries.

Tailored Solutions: Every engagement is customized for your organization's unique risks, resources, and industry needs.

24x7x365 Network Incident Hotline

If you suspect your organization is under attack, the Schneider Downs Incident Response Team is available 24x7x365 at 1-800-993-8937.

Ready to Get Started?

Contact the team at contactsd@schneiderdowns.com or learn more at www.schneiderdowns.com/cybersecurity.

About Schneider Downs Cybersecurity

The Schneider Downs cybersecurity practice consists of experts offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team.