PENETRATION TESTING SERVICES
Penetration Testing Services

Protect your organization from cybercrime. With the ever-expanding remote workforce, cybercriminals are finding new corporate vulnerabilities and pathways for hacking into networks. We can help you discover your organization’s weaknesses through penetration testing. We can also show you how to secure your systems and then help you design a continuity plan for the future.

Get help. Penetration testing is a simulated cyberattack that identifies weaknesses within a business and explains what could happen if an attacker were to exploit them. Our services help customers understand their vulnerabilities in-depth. We take the burden of identifying risks and present our findings in a clear report for your business leaders and technical teams; all delivered remotely. We offer three levels of penetration testing from a quick check to a deep investigation.

1. Quick Check+
   - Thorough scanning of infrastructure and applications
   - Open Source Intelligence Gathering (OSINT)
   - Aggregation of information and results
   - Hacker’s view of the system
   - High-quality report

2. Penetration Testing
   - Everything included in Quick Check+
   - Realistic hands-on testing, beyond scanner results
   - Findings are validated and analyzed
   - Report information is filtered and curated

3. Deep Investigation
   - Deep investigation using BlackHat tactics
   - Simulated real-world attacks
   - Tests the reaction time of your security team
   - Custom attacks developed for your organization

Deliverables with each service:

- **Executive Summary** - Summary of the assessment goals, as well as concise explanations of the threats that the organization is exposed to from a business perspective.

- **Findings** - Detailed, technical definition of each finding along with steps taken and proof of the finding.

- **Conclusion & Recommendations** - Recommendations and a summary of the issues found during the security assessment and a prioritization recommendation.