

Vulnerability Assessments and Penetration Testing

Bring in the experts to find defense weak points before attackers do

Benefits

- Pro-actively identify weaknesses
- 24x7x365 SOC team

Learn more

SecurityServices@opentext.com ›

The OpenText Attack Team consists of industry experts with specialized backgrounds in IT, software development, and security operations. Our ability to mimic behaviors and strategies of actors from around the globe is what allows us to be the leaders in vulnerability and penetration testing.

The OpenText Attack Team performs more than just routine vulnerability scans; our team works with you on strengthening your security posture. An active approach sets us apart from competing services. Rather than simply asking, “can we break into your system?” we move beyond to “what happens if attackers come from different vectors?” or “what if X/Y/Z fails?”

We consider overlooked portions in your organization to ensure no weak points or faults. Every component, layer, and access vector within your network is on our radar.

A range of services, customized for your organization

Not all networks and infrastructure are built the same. We customize and curate long-term plans to guide you toward a mature network security system. The OpenText Attack Team acts as an extension of your team with the same goal: striving for a network that will continue to protect your data and ecosystem.

Vulnerability assessments aim to identify, classify, and prioritize known vulnerabilities using automated and human testing. While penetration testing simulates real-world cyberattacks to identify vulnerabilities in systems, networks or applications, and exploit them, demonstrating a level of risk.

Annually retest, supported by OpenText Security Services

An established baseline and valuable insights on security posture changes are more reasons to stick with OpenText for your organization’s penetration testing through an annual program.

Security testing is more than merely breaking into your internal and external infrastructure. In-house web apps, mobile apps, cloud architecture, vishing/smishing (social engineering via voice/SMS), and accommodating employees working from home have greatly expanded areas of concern for network security. All these facets need to be considered. OpenText includes all components for a full spectrum and in-depth security testing regime beyond vulnerability assessments and penetration testing. Ask about all our OpenText cybersecurity services today!