OpenText Security Testing

Depth scanning, analysis, and precision testing for security and cyber defense

Benefits

- Address your risk profile and priorities
- Exceed insurance and compliance requirements
- Get high-value insights from advanced technology and expertise

As cyberthreats grow in sophistication and frequency, specialized expertise, advanced technologies, and a proactive approach to security are strategic imperatives for any organization. Unfortunately, they often lack the expertise, tools, and time to get ahead of their expanding attack surface.

With OpenText™ Security Testing, organizations can gain a comprehensive understanding of weaknesses and potential risks in their applications, systems, and network. With this knowledge, they are prepared to plug holes, improve cyber defenses, and increase compliance with insurance and regulatory requirements.

Address your risk profile and priorities with a client-centric approach

OpenText Security Services seamlessly align their work with your business objectives, providing experienced, dedicated support and collaboration. Engagements are provided as either single assessments or continuous improvement programs.

Exceed insurance and compliance requirements with tailored solutions

Benefit from customized testing scenarios designed to address your organization's unique needs and challenges. Our approach drives holistic security enhancement, regulatory compliance assurance, strategic alignment guidance, and transparent reporting.

Learn more

Blogs

- Turn up the volume with Tabletop Exercises ›
- Strengthening higher education institutions against evolving cyberthreats ›
- Cybersecurity Services combat an APT with NDR ›

Videos

- Tabletop Exercises ›

Resources

- Security catalog ›
- Security services ›

Offerings

- Security Health Check ›
- Threat Hunting Service ›
- Cybersecurity Tabletop Exercises ›

Get high-value insights with advanced technology and expertise

Engage with a team of seasoned cybersecurity professionals with a proven track record in delivering high-quality penetration testing and vulnerability scanning services. The team uses the latest tools and methodologies to stay ahead of emerging threats and vulnerabilities.

The key steps in security tests typically include:

1. **Identification:** Identifying assets, including hardware, software, network components, and data, which may be susceptible to vulnerabilities.
2. **Evaluation:** Assessing each asset to determine potential vulnerabilities. This may be done via automated scanning tools, manual inspection, or a combination of both.
3. **Classification:** Classifying vulnerabilities based on severity, potential impact, and likelihood of exploitation. This helps prioritize which vulnerabilities should be addressed first.
4. **Risk assessment:** Assessing the potential risks associated with each vulnerability, considering factors such as the value of the asset, the likelihood of exploitation, and the potential impact of a successful attack.
5. **Mitigation planning:** Developing a plan to address identified vulnerabilities, which may include implementing security patches, configuration changes, or other countermeasures.

Depending on the organization's specific needs, the following security tests can be performed:

- **Network Vulnerability Assessment**
  Identifying vulnerabilities within the network infrastructure, including routers, switches, firewalls, and other network devices. It may involve scanning for open ports, outdated software, misconfigurations, and other weaknesses that could be exploited by attackers.
- **Web Application Vulnerability Assessment**
  Identifying vulnerabilities within web applications, such as SQL injection, crosssite scripting (XSS), and insecure authentication mechanisms. It may involve both automated scanning tools and manual testing techniques to uncover vulnerabilities.
- **Wireless Network Assessment**
  Identifying vulnerabilities within wireless networks, including Wi-Fi networks. It may involve testing for weak encryption, rogue access points, and other security issues that could compromise the confidentiality and integrity of wireless communications.
- **API Vulnerability Assessment**
  Identifying vulnerabilities within application program interfaces (API), such as weak authentication and authorization mechanisms, SQL injection, cross-site scripting (XSS), unprotected data, improper error handling, and general API best practices.
- **Social Engineering Assessment**
  Testing the effectiveness of an organization's security awareness training and policies by attempting to manipulate individuals into disclosing sensitive information or performing unauthorized actions. This may include phishing attacks, pretexting, and physical security breaches.
- **Red Team Penetration Testing**
  Simulating real-world cyberattacks by attempting to breach an organization's security defenses using a variety of tactics, techniques, and procedures (TTPs). It often involves a combination of technical attacks, social engineering, and physical security testing to identify weaknesses across multiple layers of defense.

OpenText Professional Security Services

To talk to an OpenText Professional Security Services expert about this solution or other service offerings, please email SecurityServices@opentext.com or visit opentext.com/services/security.

- **Application Code Review**
  Examination of application source code to detect potential weaknesses introduced in the development lifecycle creating vulnerabilities around input validation, authentication and authorization, data protection, third-party libraries and components (known CVEs), business logic flaw, code security, and noncompliance with best practices.
- **Mobile Application Security Testing**
  Similar to Application Code Review, but adapted for mobile applications. Includes dynamic analysis, network communication review for attacks such as “man-in-the-middle” and mobile platform-specific security controls.

Who are our OpenText Security Services experts?

OpenText is an industry leader in cybersecurity solutions with more than 20 years of professional and technical expertise. Consultants hold certifications such as EnCe (EnCase Certified Examiner), CFSR (Certified Forensic Security Responder), EnCEP (EnCase Certified eDiscovery Practitioner), CISA (Certified Information System Auditor), CISSP (Certified Information Systems Security Professional), and CompTIA Security+.