opentext™

SERVICE OVERVIEW

OpenText Vulnerability Assessments and Penetration Testing methodology

Using OpenText Security Testing to identify and address weak points in your security posture

Benefits

- Mitigate financial risks
- Comply with legal and regulatory requirements
- Protect your brand reputation
- Safeguard your data

When you partner with OpenText for security testing, you're being supported by a team of industry experts with backgrounds spanning information management technology, security operations, data security, application security, and identity and access management. Our tools and methodology safely mimic behaviors and strategies of today's most sophisticated malicious actors, performing full-spectrum vulnerability, penetration and. performing full-spectrum vulnerability, penetration, and other security assessments to test your organization's systems with a single goal—to identify areas of weakness and provide clear, prescriptive guidance to remediate any issues that pose a risk.

Industry-standard methodology, plus drive for excellence

Our primary security testing and assessment methodology is based on the Penetration Testing Execution Standard—a seven-part approach that follows industry best practices and ensures consistent, timely engagements with impactful outcomes. Then we go beyond what's expected, identifying and navigating individual security components and vectors, exploring all avenues for entry.

A curated experience with customized outcomes

With years of expertise, we understand every organization's network and infrastructure is unique. We have curated our service to allow our delivery to align to the specific security objectives the engagement with business. Our deliverables will include customized reports giving you detailed, specific information that facilitates a higher level of success. Our commitment is to your business highest standards.

Secure data practices

The OpenText Attack Team uses isolated servers to guarantee data is secure and preserved throughout the assessment process. All Deliverable data, both at rest and in transit, is encrypted.

Every component, every inroad

Security testing is more than just breaking into your external and internal infrastructure. Our OpenText Attack Team goes beyond conventional technology stack assessment, we offer comprehensive testing services for web & mobile applications, and code reviews, as well as on-site wireless assessments.

Take on the future with confidence

As your organization changes over time, so will your security needs and requirements. OpenText collaborates with your team, working from the foundational standards we've developed in partnership to improve and mature your security posture in alignment with your business evolution to reduce risks against the ever-changing threat landscape.

Main "Out of Box" Services	
Vulnerability Assessment	Identifying vulnerabilities within the scoped infrastructure, potentially including workstations, servers, 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.
Penetration Testing	Penetration tests simulate 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.
Social Engineering Assessment	Either as an augmentation to Penetration Testing or as a separate scoped engagement, this assesses 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.

> "The clarity of your reporting and the depth of your analysis ensured that we not only understood the vulnerabilities identified but were also equipped with practical steps to address them effectively."

Seth Yeack,
IT Manager, DazPak

> "[OpenText] delivered detailed assessments, identified critical vulnerabilities, and provided actionable, tailored recommendations that addressed our unique requirements. The OSINT analysis offered valuable insights into external threats, greatly supporting our efforts to mitigate risks effectively."

Davor Barac,
Senior IT consultant,
Delecsys AB

Resources

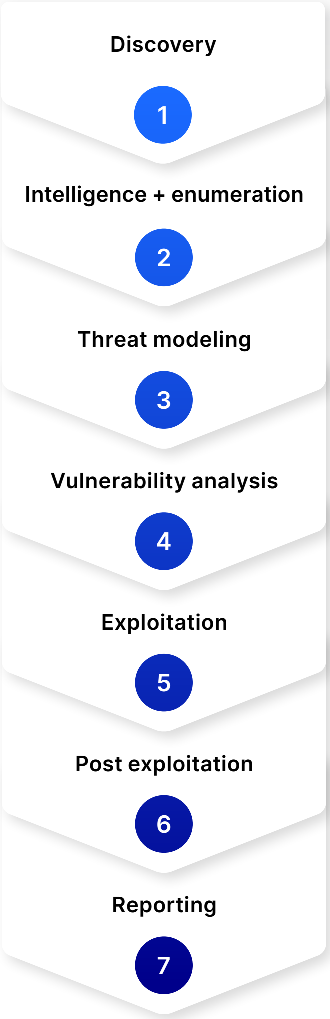
To learn more or book a demo, contact your OpenText account representative

OpenText Security Testing ›

Vulnerability Assessments and Penetration Testing ›

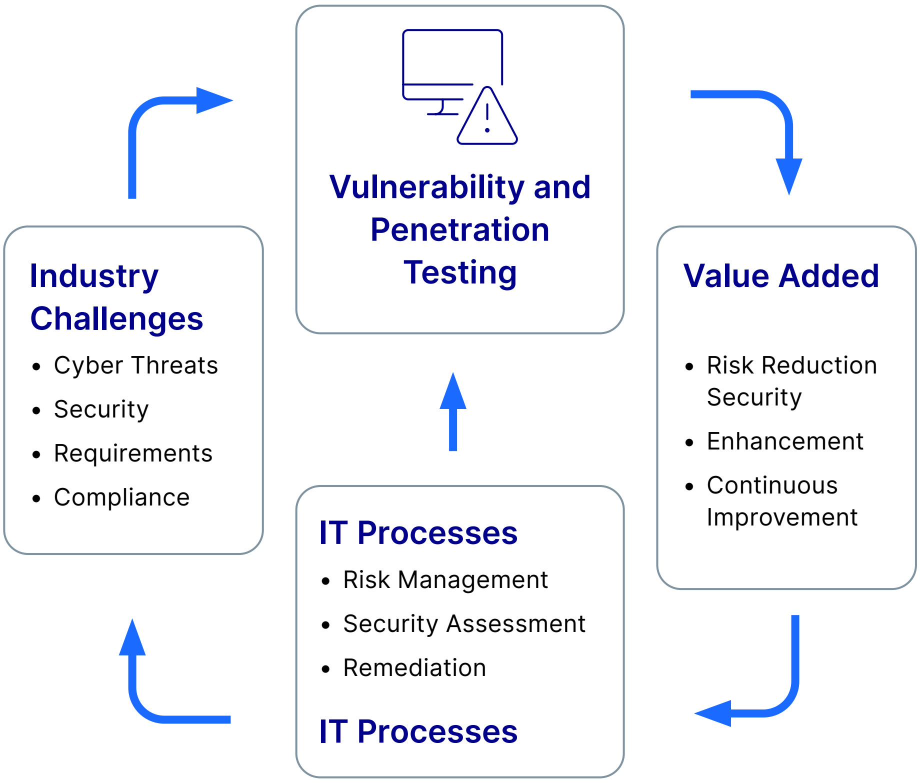
Fortifying your digital fortress - OpenText Blogs ›

OpenText Vulnerability Assessments and Penetration Testing



Discovery
1
Intelligence + enumeration
2
Threat modeling
3
Vulnerability analysis
4
Exploitation
5
Post exploitation
6
Reporting
7

IT Vulnerability and Penetration Testing



Vulnerability and Penetration Testing

Industry Challenges

- Cyber Threats
- Security
- Requirements
- Compliance

Value Added

- Risk Reduction Security
- Enhancement
- Continuous Improvement

IT Processes

- Risk Management
- Security Assessment
- Remediation

IT Processes

The 7 steps of penetration testing execution

1. **Discovery –** Determine scope of the testing engagement, establish the goals and rules of engagement.
2. **Intelligence and enumeration –** Intelligence gathering using provided information and open source intelligence (OSINT) to perform reconnaissance of the scoped targets of the security test.
3. **Threat modeling –** Vulnerability scanning of the target assets is used to identify potential attack vectors for exploitation, as well as using information from the previous steps to map attack vectors and methods for testing.
4. **Vulnerability analysis –** Comprehensive review and analysis of the vulnerability scan data to determine potential exploitable vulnerabilities in the target assets.
5. **Exploitation –** Execution of targeted attacks determined in the previous phases following the scope and rules of engagement.
6. **Post exploitation –** After the execution phase is complete, the vulnerabilities and successful exploitation of the targets will be documented, as well as any sanitation of artifacts/elements of successful exploitation such as root kits, users, or any post-attack altered parameter used in exploitation. Additional remediation recommendations will also be gathered and documented.
7. **Reporting –** Post-mortem review of all phases of the security test with the stakeholders to provide comprehensive information about all phases of testing, risk ranking of results of testing, and detailed plans for remediation.