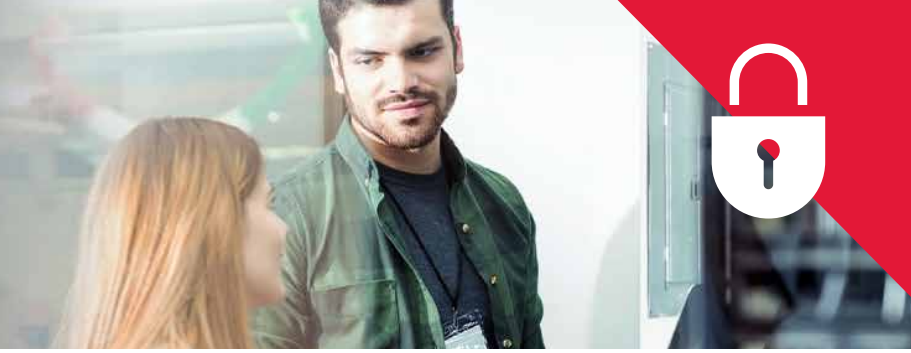
PENETRATION TESTING & ADVERSARY SIMULATION

Risk Advisory Services



HOW SECURE IS YOUR ORGANIZATION?

In today's fast-moving technology environments and rapidly changing risk landscape, the security of information assets is not always a forethought.Security and privacy breaches are making headlines; can you risk being one of them? Whether for compliance, security posture or contractual reasons, CDW can help ensure your organization is cybersecure.

HAVE YOU DONE A PENETRATION TEST OR VULNERABILITY ASSESSMENT?

CDW has conducted thousands of assessments and has been specializing in cybersecurity for over 12 years. We use the knowledge we've gained through ongoing training and development to thoroughly assess if your defences can withstand an attack like those your organization would face from a real-world threat actor. By the end of our assessment, we will identify security vulnerabilities and misconfigurations in your environment to give you a comprehensive understanding of your organization's security posture. Our detailed report will not only provide you with all the vulnerabilities but will also provide you with an issue resolution based on the risk and threat to your organization.

FEATURES

- Manual penetration (automated tools only go so far)
- The team is 100% based in Canada
- Discipline-focused, expert testers
- Risk-based reporting
- Prioritized findings
- Testing can be performed remotely

BENEFITS

- Understand the current security posture
- Identify poor practices & controls
- Engage directly with testers
- Identify & prioritize risks
- Comply with industry standards and regulations

WHAT WE DO

Our services come in three tiers, dependent upon your requirements:

ADVERSARY SIMULATION

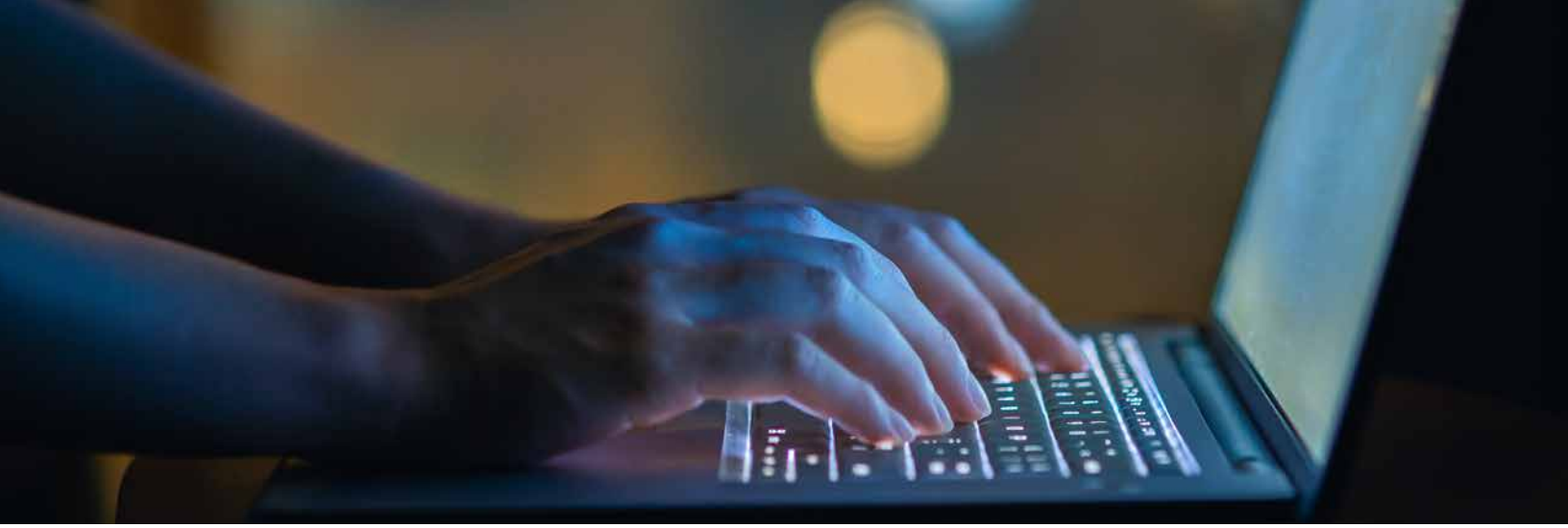
Assess your organization's detection and response capabilities to real-world cyberattacks.

PENETRATION TESTS

Controlled exploitation of identified vulnerabilities to further uncover weaknesses in environments, such as active directory misconfigurations and attack paths which can lead to an organizational compromise.

VULNERABILITY ASSESSMENTS

Assessments are performed from both a manual and automated perspective to evaluate vulnerabilities in an environment. This includes discovery, research and validation.



WHAT WE DO

NETWORK

Our network assessment tests for network weaknesses, misconfigurations and mismanagement of devices. We offer a variety of network-related assessments, including:

- External Network Penetration Testing
- Internal Network Penetration Testing
- Wireless Network Penetration Testing
- Cloud Penetration Testing
- Active Directory Assessments
- Network Vulnerability Assessments

WEB APPLICATION

This service includes testing for application weaknesses, technical flaws or vulnerabilities, and web API testing.

MOBILE APPLICATION

Our services include testing for mobile application weaknesses, technical flaws or vulnerabilities, and the entire multi-tier mobile application architecture.

ADVERSARY SIMULATION/RED TEAM

Through this service, we assess a company's readiness to withstand and respond to a simulated real-world cyberattack. The service includes a goal-based, time-boxed approach to uncover weaknesses in an organization's security posture, which could lead to a compromise of an environment.

SOCIAL ENGINEERING

Social engineering is a manipulation strategy designed to trick individuals into performing an action that is not in their best interest. It is often used by attackers to obtain sensitive information, capture a user's credentials or to remotely compromise machines. We prepare and educate our clients by offering:

- Email Phishing (General & Targeted) Campaigns
- Telephone (Vishing) Campaigns
- In-Person (Physical) Social Engineering, including USB Drops

INTELLIGENCE GATHERING

Open-source intelligence gathering (OSINT) involves finding, selecting and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. OSINT is used to determine what information an organization has that could be leveraged by an attacker.

OUR TESTING APPROACH

Depending on the specific objectives of your business, we offer several methods of testing:

- Zero-knowledge testing: Testing with no prior information about the target, network or application.
- Partial-knowledge testing: Testing with some information about the target, network or application.
- Full-knowledge testing: Testing with full information about the target, network or application.

OUR METHODOLOGY

We use industry best standards for performing penetration tests. The following methodologies are used:

- **Open web application security project (OWASP) testing guide:** Standard utilized for web application vulnerability assessments and penetration tests.
- **OWASP mobile top 10:** Standard utilized for mobile vulnerability assessments and penetration tests.
- **Penetration testing execution standard (PTES):** Standard utilized for intelligence gathering, social engineering, wireless and network penetration tests.
- **NIST technical guide to information security testing & assessment (sp800-115):** Used as a general approach for conducting security testing and assessments.

WHY CDW?

CDW is uniquely qualified to provide high-quality services specific to this engagement.

- **Depth of Experience** – Extensive experience conducting network and infrastructure penetration tests in complex and highly sensitive environments. We have been doing penetration testing for over 12 years.
- **Continuous Improvement** – We invest in our people: training them in the latest techniques to keep up with North America's changing threat landscape.
- **Breadth of Experience and Knowledge** – We've done testing in all industry verticals across North America and bring you the knowledge of all our resources. Not just the resource is working directly with your organization. Our consultants hold the following designations: OSCP, OSCE, OSWP, OSWE, CRTP, CEH, RHCE, RH413, GSEC, eJPT and eWAPT.
- **Security Experts** – Our consultants have experience in aiding different sized organizations; meaning we can help design security controls and processes that are tailored to your organization.

For more information, contact your CDW account team at 800.972.3922 or visit CDW.ca/security

CDW PEOPLE WHO GET IT™