Continuous offensive security validation

CGI combines autonomous penetration testing, offensive security expertise and practical remediation support, to help organizations safely assess IT environments from an attacker's perspective and continuously improve resilience.

Flexible support on your terms

CGI adapts to your needs, whether you need a fully managed service, co-managed delivery alongside your internal team, or targeted expertise to strengthen specific areas of your program.

Our specialists use proven offensive security methods and tools to help you move from periodic testing to evidence-based, continuous validation, while aligning the service to your risk appetite, operating model and business priorities.

- **Internal and external autonomous pentesting**
  We validate exploitable risk from outside-in and assume-breach perspectives.
- **Cloud and identity testing**
  We assess cloud misconfigurations, IAM weaknesses, Entra ID/Active Directory password security and hybrid identity exposure.
- **Phishing impact testing**
  We measure what a compromised credential could actually expose, beyond simple click-rate reporting.
- **EDR and control validation**
  We evaluate whether endpoint and defensive controls detect or prevent attacker behavior.
- **Segmentation validation**
  We assess whether network controls are limiting attacker movement as intended.
- **Remediation validation**
  We retest specific weaknesses after fixes are applied to confirm that risk has been reduced.

Autonomous penetration testing: Hack-Fix-Verify-Repeat with Horizon3.ai's NodeZero platform

Traditional vulnerability management can create long lists of findings, many of which may not be exploitable in your organization's actual environment.

Horizon3.ai's NodeZero solution makes a difference. It is a practical platform for continuous, evidence-based security validation. It chains misconfigurations, default credentials, weak passwords, password reuse, exposed services, identity issues, and exploitable vulnerabilities to pinpoint where the real threat is and help you prioritize actions.

- Core decisioning powered by machine learning
- Visualization of how weaknesses combine into real attack paths
- Run unlimited pentests to prioritize, fix, and verify remediation
- NodeZero Tripwires™ alert in real time when they detect potentially malicious activity.

What makes Horizon3.ai NodeZero different

Traditional platforms	Horizon3.ai
Static pre-defined analysis – Test what you already know.	**Autonomous comprehensive attacks** – Learns and adapts with every test.
Theoretical risk – Deliver opinion-based risk scores.	**Proven impact** – Real exploitation reveals actual business exposure.
Paralyzing volume – Produce noisy, high-volume to-do lists that overwhelm your team.	**Clarity of action** – Gives you confidence on exactly what to fix now, and what can wait.
Periodic testing – Deliver results that become stale rapidly.	**Continuous validation** – Know the impact of every change in your environment.
Based on assumptions – Rely on the hope that your efforts and tools are enough.	**Anchored in evidence** – Provides continuous proof of your security posture.

Why trust CGI for offensive security validation

Reduce exploitable risk
Focus remediation on weaknesses that can actually be used by attackers.

Shorten remediation cycles
Use repeatable testing and verification to reduce mean time to remediation (MTTR).

Improve control confidence
Validate whether identity, segmentation, EDR, cloud and infrastructure controls are working as intended.

Replace manual testing
Extend the value of traditional penetration testing with continuous, repeatable validation.

Prioritize based on impact
Move from prioritizing based on CVSS score and severity only to attack path and business impact.

Strengthen executive reporting
Give leadership clearer evidence of exposure, progress and risk reduction.

Contact our experts today

Amitabh Chakravorty
Director, Consulting Services
amitabh.chakravorty@cgi.com

Gowrishankar Raju
Senior Consultant
gowrishankar.raju@cgi.com

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-focused to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

Email us at
cybersecurity.ca@cgi.com

For more information
cgi.com