Validation offensive continue de la sécurité

CGI combine les tests d'intrusion autonomes, l'expertise en sécurité offensive et un accompagnement pratique à la remédiation afin d'aider les organisations à évaluer les environnements TI du point de vue d'un attaquant et d'en augmenter la résilience.

Soutien flexible selon vos termes

CGI s'adapte à vos besoins en vous offrant des services gérés au complet ou co-gérés avec votre équipe, ainsi qu'une expertise précise pour renforcer des sections spécifiques de votre programme.

Nos experts utilisent des méthodes et des outils éprouvés en sécurité offensive pour vous aider à passer de tests périodiques à une validation continue fondée sur des preuves, tout en adaptant le service à votre tolérance au risque, à votre modèle opérationnel et à vos priorités d'affaires.

- **Tests d'intrusion autonomes internes et externes**
  Valider les risques exploitables selon une perspective externe, de l'extérieur vers l'intérieur, ainsi que selon une approche de compromission présumée.
- **Tests infonuagiques et d'identité**
  Évaluer les mauvaises configurations infonuagiques, les faiblesses IAM, la sécurité des mots de passe Entra ID/ Active Directory et l'exposition liée aux identités hybrides.
- **Tests d'impact de l'hameçonnage**
  Mesurer ce qu'un identifiant compromis pourrait réellement exposer, au-delà du simple taux de clics.
- **Validation de l'EDR et des contrôles**
  Évaluer si les contrôles de protection des terminaux et les contrôles défensifs détectent ou empêchent les comportements d'attaquants.
- **Validation de la segmentation**
  Évaluer si les contrôles réseau limitent les déplacements des attaquants comme prévu.
- **Validation de la remédiation**
  Retester des faiblesses précises après l'application des correctifs afin de confirmer que le risque a bien été réduit.

Tests d’intrusion autonomes:
« Exploiter, corriger, vérifier, répéter » avec la plateforme NodeZero de Horizon3.ai

Une gestion traditionnelle peut générer de longues listes de vulnérabilités, dont plusieurs ne sont pas nécessairement exploitables dans l’environnement réel de votre organisation.

La solution NodeZero de Horizon3.ai change la donne. Il s’agit d’une plateforme pratique de validation de sécurité continue, fondée sur des preuves. Elle analyse de manière combinée les mauvaises configurations, les identifiants par défaut, les mots de passe faibles, la réutilisation des mots de passe, les services exposés, les problèmes liés à l’identité et les vulnérabilités exploitables afin de cibler les menaces réelles et de vous aider à prioriser les actions.

- Prise de décision de base propulsée par l’apprentissage automatique
- Visualisation de la façon dont les faiblesses se combinent en véritables chemins d’attaque
- Exécution de tests d’intrusion illimités pour prioriser, corriger et vérifier la remédiation
- La fonctionnalité NodeZero Tripwires™ permet de notifier en temps réel toute détection d’activité potentiellement malveillante.

Ce qui distingue Horizon3.ai NodeZero

Plateformes traditionnelles	Horizon3.ai
Analyse statique prédéfinie — Testent ce que vous connaissez déjà.	**Attaques autonomes et complètes** — Apprend et s’adapte à chaque test.
Risque théorique — Fournissent des scores de risque fondés sur des opinions.	**Impact démontré** — L’exploitation réelle révèle l’exposition concrète de l’entreprise.
Volume paralysant — Génèrent des listes de tâches bruyantes et volumineuses qui submergent vos équipes.	**Clarté d’action** — Vous donne confiance quant à ce qu’il faut corriger maintenant et ce qui peut attendre.
Tests périodiques — Produisent des résultats qui deviennent rapidement obsolètes.	**Validation continue** — Permet de connaître l’impact de chaque changement dans votre environnement.
Fondées sur des hypothèses — Reposent sur l’espoir que vos efforts et vos outils suffisent.	**Ancrée dans les preuves** — Fournit une preuve continue de votre posture de sécurité.

Pourquoi faire confiance à CGI pour la validation de sécurité

Réduire le risque exploitable – Concentrez les efforts de remédiation sur les faiblesses qui peuvent réellement être utilisées par des attaquants.

Raccourcir les cycles de remédiation – Utilisez des tests et des vérifications reproductibles pour réduire le temps moyen de remédiation (MTTR).

Renforcer la confiance dans les contrôles – Vérifiez le bon fonctionnement des contrôles liés à l'identité, à la segmentation, à la détection et réponse aux menaces sur les points terminaux (EDR), à l'infonuagique et à l'infrastructure.

Remplacer les tests manuels – Prolongez la valeur des tests d'intrusion traditionnels grâce à une validation continue et reproductible.

Prioriser selon l'impact – Passez d'une priorisation fondée uniquement sur les scores du système d'évaluation standard des vulnérabilités (CVSS) et la sévérité à une priorisation basée sur les chemins d'attaque et l'impact métier.

Renforcer les rapports destinés à la direction – Fournissez aux dirigeants des preuves plus claires de l'exposition, des progrès réalisés et de la réduction des risques.

Contactez nos spécialistes dès maintenant

Amitabh Chakravorty
Directeur, services- conseils
amitabh.chakravorty@cgi.com

Gowrishankar Raju
Conseiller en cybersécurité
gowrishankar.raju@cgi.com

À propos de CGI

Allier savoir et faire

Fondée en 1976, CGI figure parmi les plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde.

Nous sommes guidés par les faits et axés sur les résultats afin d'accélérer le rendement de vos investissements. À partir de centaines de bureaux à l'échelle mondiale, nous offrons des services-conseils complets, adaptables et durables en TI et en management. Ces services s'appuient sur des analyses mondiales et sont mis en oeuvre à l'échelle locale.

Écrivez-nous à
cybersecurity.ca@cgi.com

Pour plus d'information
cgi.com