ANTICIPEZ LA MENACE : LA CYBERSÉCURITÉ OFFENSIVE AU SERVICE DE VOTRE RÉSILIENCE

Testez vos défenses avant que les attaquants ne le fassent

CGI BUSINESS CONSULTING

INTRODUCTION

Dans un contexte de menaces numériques en constante évolution, il ne suffit plus de se protéger, il faut également se mettre dans la position d'un attaquant : imaginer les vecteurs d'attaques qu'il va exploiter et, afin de rester pragmatique, prévoir ses cibles d'attaque privilégiées comme le décrivent les ateliers 3 et 4 de la méthode d'analyse de risques EBIOS Risk Manager.

Les cybercriminels innovent sans relâche, exploitant la moindre faille pour infiltrer les systèmes, compromettre des données sensibles ou interrompre vos activités. Ils mettent en place de véritables stratégies d'attaque. C'est pourquoi le Laboratoire de Cybersécurité de CGI Business Consulting propose une approche offensive de la sécurité : en testant vos défenses dans des conditions réelles d'attaque, nous révélons vos points faibles avant qu'ils ne soient exploités.

Nos services de tests d'intrusion et de simulation offensive vous aident à :

- *Évaluer votre niveau d'exposition en démontrant les vecteurs de compromission exploitables*
- *Prioriser les correctifs en fonction des risques en tenant compte du profil de l'attaquant et des conséquences sur les métiers si l'incident se produisait*
- *Renforcer vos défenses face à des menaces ciblées et sophistiquées*
- *Répondre aux exigences de conformité et de gouvernance*
- *Proposer un service régulier pour vous alerter en cas de dérive des moyens de défense*

01

CYSLAB, LE LABORATOIRE DE CYBERSÉCURITÉ DE CGI

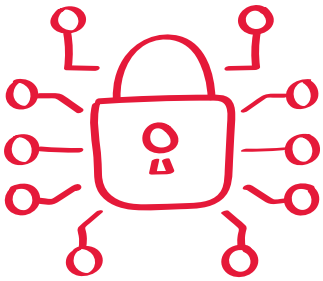
Qualifié PASSI RGS et PASSI LPM depuis 2015, le CysLab répond aux exigences les plus élevées de sécurité et réunies des compétences d'auditeurs de premier plan

Équipe de 25 consultants disposant de certifications reconnues (OSCP+, OSEP, OSWP, AWS, EBIOS-RM, CEH…)

Activité de recherche et développement en outillage (Ligolo-ng, Filet-o-Phish) et découverte de vulnérabilités de type zero-day (Nokia, SAP, …)

Des **livrables didactiques et adaptés à votre écosystème**, destinés tant aux équipes techniques que managériales. Chaque chemin d'attaque est illustré pour comprendre les conditions du scénario et ses conséquences.

Notre force : l'investissement dans la recherche et développement



Le CysLab s'investit pleinement dans la communauté cybersécurité. Nos experts et auditeurs consacrent une part importante de leur temps à la recherche et au développement, explorant des vulnérabilités zero-day et contribuant au développement open source. Nous partageons nos découvertes et nos connaissances à travers des publications dans des revues spécialisées, participant ainsi à l'avancement de la sécurité numérique. Nous sommes également impliqués dans la direction du Club EBIOS.

Publication de vulnérabilités zero-day (Nokia, SAP…)

Développement d'outils de cybersécurité reconnus mondialement

Ligolo-ng Chashell

Publications dans des revues spécialisées (MISC)

02

NOTRE GAMME DE SERVICES

1. Audit sur mesure : révélez les vulnérabilités là où les outils s'arrêtent

Grâce à son expertise et en privilégiant les tests manuels en complément des outils de test et d'audit automatisés, le CysLab effectue des audits **personnalisés et approfondis**, permettant de détecter un **large éventail de vulnérabilités**, y compris les failles zero-day. Nous analysons en détail les chemins d'attaque potentiels tant sur le plan technique, fonctionnel et physique pour une évaluation complète.

Prestations pouvant être qualifiées PASSI RGS ou PASSI LPM

TESTS D'INTRUSION

- Simulation d'attaques réelles pour améliorer votre niveau de sécurité.
- Évaluation de votre résistance et réactivité face à des intrusions externes et internes.
- Mise en évidence des failles de sécurité exploitables par des attaquants.

AUDIT DE CODE

- Analyse du code source d'une application pour détecter les failles de sécurité.
- Identification des erreurs de programmation pouvant être exploitées par des attaquants.
- Vérification du respect des bonnes pratiques de développement sécurisé.

AUDIT D'ARCHITECTURE

- Évaluation de la conception et de la structure d'un système pour limiter sa surface d'exposition aux attaques.
- Identification des points faibles dans l'implémentation de l'architecture et des moyens de maintien en condition de sécurité.
- Analyse des flux de données et des interactions entre les composants.

AUDIT DE CONFIGURATION

- Analyse des configurations des équipements réseau, systèmes et applications.
- Identification des configurations non sécurisées ou obsolètes.
- Assurance que les systèmes sont configurés conformément à l'état de l'art.

AUDIT ORGANISATIONNEL ET PHYSIQUE

- Évaluation des politiques, procédures et pratiques de sécurité d'une organisation.
- Identification des lacunes dans la gestion de la sécurité de l'information.
- Analyse de la sensibilisation et de la formation des employés aux enjeux de sécurité.

2. Campagne de RedTeaming : la simulation d'attaques réalistes pour tester vos défenses dans des conditions extrêmes.

Afin de renforcer votre posture de sécurité face aux menaces sophistiquées, nos campagnes de RedTeam simulent des attaques ciblées et réalistes. Grâce à notre investissement continu en Recherche et Développement, nos experts ont développé des techniques et des outils d'attaque de pointe, présentés lors de conférences publiques.

1.

RECONNAISSANCE

Évaluation des points d'entrée externes (présence en ligne, fuites de données) et internes (sécurité physique, réseau sans fil).

2.

INTRUSION EXTERNE

Exploitation et maintien d'accès des services exposés publiquement (VPNs, Extranet, applications externes, Cloud…).

3.

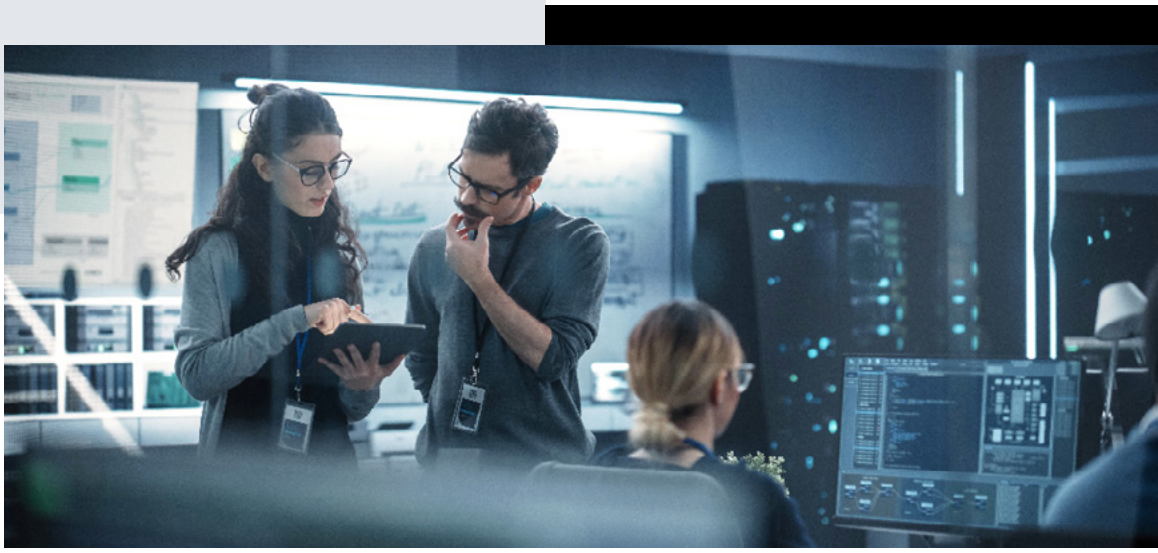
INTRUSION INTERNE - PHYSIQUE

Intrusion dans les locaux (copie de badge, accès parking…), dépôt de portes dérobées sur le réseau, compromission des accès sans-fil.

4.

HAMEÇONNAGE

Création de faux sites d'authentification, utilisation de macros malveillantes, et usurpation d'identité pour tromper les victimes.



3. Audits cybersécurité des intelligences artificielles

L'intelligence artificielle transforme les entreprises, mais elle introduit également de **nouveaux défis en matière de sécurité**.

Notre gamme de services spécialisés est conçue pour vous aider à naviguer dans ce paysage complexe. Nous proposons des **évaluations techniques approfondies** pour identifier les vulnérabilités de vos modèles d'IA, des services de conception et d'implémentation de solutions de sécurité sur mesure, et un accompagnement pour assurer la conformité et l'éthique de vos projets IA. Nos experts vous aident à construire des systèmes d'IA robustes, fiables et dignes de confiance. Ensemble, sécurisons l'avenir de l'intelligence artificielle.

SÉCURITÉ IA – CONCEPTION ET IMPLÉMENTATION

- Audit d'architecture
- Audit de code source
- Qualité et protection des données d'entraînement

SÉCURITÉ IA – ÉVALUATION TECHNIQUE

- Test d'intrusion visant les applications
- Revue de configuration des serveurs
- Évaluation de la robustesse des modèles

SÉCURITÉ IA – CONFORMITÉ ET ÉTHIQUE

- Analyse conformité légale (EU AI Act)
- Analyse des potentielles problématiques éthiques

4. Audit des réseaux et infrastructures

- **Externe** : Vos points d'accès Internet et services exposés.
- **Interne** : Votre réseau d'entreprise, pour prévenir les menaces venant de l'intérieur, qui représentent une part significative des incidents.
- **Wi-Fi** : La sécurité de vos accès sans-fil.
- **Cloud & Conteneurs** : Audit de vos environnements AWS, Azure, GCP et de vos architectures Docker/ Kubernetes.
- **Systèmes Industriels (OT/SCADA)** : Évaluation de la sécurité des systèmes qui pilotent vos opérations critiques.
- **Objets Connectés (IoT)** : Analyse de la sécurité de vos appareils connectés et de leurs écosystèmes.

CGI BUSINESS CONSULTING

CONTACTS

Jean OLIVE

Vice Président - Responsable des activités d'audits de sécurité et de gestion des risques

jean.olive@cgi.com

Nicolas CHATELAIN

Directeur du Pôle Audit Technique Cybersécurité

n.chatelain@cgi.com

Chez CGI Business Consulting, cabinet de conseil majeur en France, nous sommes audacieux par nature.
Grâce à son intimité sectorielle et à sa capacité à mobiliser des expertises diverses, CGI Business Consulting apporte aux entreprises et aux organisations des solutions de conseil audacieuses et sur mesure, pour une réussite stratégique et opérationnelle de leurs projets de transformation.
Nos 1 000 consultants accompagnent nos clients dans la conduite et la mise en œuvre de leurs projets de transformation, dans une relation franche et de confiance, pour leur permettre de prendre les bonnes décisions.
Fondée en 1976, CGI figure parmi les plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde. Elle aide ses clients à atteindre leurs objectifs, notamment à devenir des organisations numériques axées sur le client.

cgi.fr/conseil

L'audace par nature