

# Diagnostic cybersécurité TESTCYBER+ : un nouvel outil RH complémentaire à l'audit

## Pourquoi aller plus loin que l'audit informatique ?

L'audit de sécurité informatique annuel est un socle indispensable pour cartographier les vulnérabilités techniques, les conformités réglementaires (RGPD, ISO 27001...) et les politiques de sécurité de l'entreprise. Il reste cependant centré sur l'infrastructure, les processus et les pratiques "de surface", et il implique souvent une approche descendante pilotée par la DSI ou un cabinet externe.

Mais qu'en est-il **des usages réels, des comportements quotidiens, de la compréhension et de l'implication des salariés** ? Ces facteurs sont aujourd'hui considérés comme la première source de risques (erreur humaine, négligence, manque de sensibilisation...).

## TESTCYBER+ : la vision RH et collaborative de la cybersécurité

Le **Diagnostic Cybersécurité TESTCYBER+** s'adresse à tous les collaborateurs (tous métiers, tous niveaux), sous la forme d'un test rapide, accessible en ligne, qui évalue en 15 à 30 minutes :

- l'attitude informatique (hygiène numérique, réflexes, veille)
- le niveau de culture cyber (pro/perso)
- la compréhension des risques et des bonnes pratiques
- la maîtrise des outils et process (sauvegardes, mots de passe, vigilance phishing, BYOD, RGPD...)
- l'engagement personnel face aux politiques de sécurité de l'entreprise

**Contrairement à un audit technique, il donne la parole à chaque salarié** et permet un état des lieux inédit de la maturité collective et individuelle sur les points essentiels, rarement mesurés lors des audits classiques.

## Les avantages RH et organisationnels

### 1. Lecture humaine et organisationnelle

- Mesure la maturité et la perception de la sécurité dans chaque service
- Met en lumière les freins, les besoins de formation, l'adhésion ou la défiance envers la politique cybersécurité
- Permet d'identifier les "ambassadeurs" et les points d'appui internes pour diffuser la culture cyber

### 2. Gain de temps et simplicité

- Mise en œuvre immédiate, pas d'installation, pas d'intrusion dans les systèmes
- Un questionnaire à remplir individuellement, sur ordinateur ou mobile

- Résultats consolidés, score global et par thème, analyse transversale par métier ou niveau de responsabilité

### 3. Outil de pilotage pour les RH

- Score sur 1000 points, lecture par niveaux (intermédiaire, opérationnel, avancé, expert)
- Rapport synthétique, avec recommandations RH et pistes d'actions personnalisées
- Permet de prioriser les plans de sensibilisation, les formations, les campagnes de rappel et les communications internes

### 4. Complémentarité avec l'audit

- L'audit identifie les failles techniques et process, le Diagnostic TESTCYBER+ révèle les angles morts humains
- La confrontation des deux grilles (technique et humaine) donne une vue à 360° de la cybersécurité d'entreprise

### 5. Valeur économique

- Prévention des erreurs et négligences évitables
- Réduction de l'exposition au risque et des coûts liés aux incidents (fraude, rançongiciels, fuite de données)
- Optimisation des budgets de formation : cibler précisément les besoins

## Synthèse opérationnelle pour la RH

**Le Diagnostic TESTCYBER+ c'est :**

- une "photographie" rapide de la maturité cyber de tous les salariés
- un outil facile à déployer, sans mobilisation technique
- une source d'indicateurs pour ajuster la politique de sensibilisation, mesurer les progrès, renforcer la conformité

**C'est surtout une réponse à une question que l'audit technique seul ne peut pas adresser :**

"À quel point l'humain est-il préparé face à la menace cyber ?"

**En résumé :**

Le Diagnostic TESTCYBER+ complète et amplifie la portée des audits techniques. Il donne aux RH et à la DSI une lecture humaine, collective et ciblée des vrais leviers de sécurité. Un investissement rapide, économique, directement actionnable, et qui contribue à installer une vraie culture de la sécurité au sein de l'entreprise.