EYRAPPROACH

Prévenir
Culture et sensibilisation à la sécurité

Votre challenge :

Comment former notre personnel à faire face à des attaques innovantes et ciblées ? Comment les encourager à signaler les incidents de sécurité ? Comment les faire se sentir responsables de la cybersécurité ?

Une cybersécurité efficace repose sur des personnes, des processus et des technologies. Vos collaborateurs sont votre dernière ligne de défense et **les piliers de votre sécurité**. Leur implication dans votre plan de cybersécurité et votre implication dans les opérations commerciales sont des facteurs clés de succès de votre plan de sécurité. Pour atteindre cette situation idéale, il ne suffit pas de sensibiliser les gens aux risques, il faut qu'ils se sentent concernés, qu'ils prennent leurs responsabilités et qu'**ils changent leurs habitudes pour en adopter de plus sûres**.

Comme Bruce Schneier l'a si bien dit : "*Security is a process, not a product*". C'est encore plus vrai pour la sensibilisation à la cybersécurité. Au-delà de la sensibilisation, l'objectif est de changer les comportements et l'état d'esprit pour assurer la sécurité de nos organisations et de notre société.

Construisons **une défense humaine efficace** pour votre organisation ; c'est l'un des projets de cybersécurité les plus difficiles mais nécessaire pour avoir un plan de sécurité efficace et durable.

Pourquoi maintenant plus que jamais ?

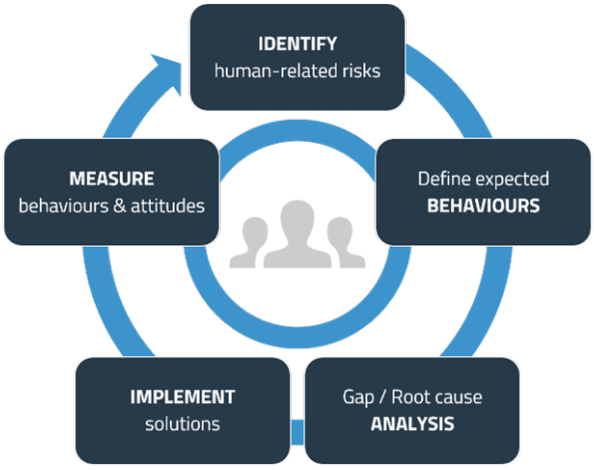
- Les travailleurs à domicile sont la cible idéale : l'environnement a **un impact direct sur la vigilance des travailleurs** et, avec le télétravail, la distance nuit au temps de réaction et à la communication avec le service informatique.

- La cybersécurité devient de plus en plus **un travail d'équipe**. L'implication de tous, de l'informatique à l'entreprise, est primordiale pour atteindre le niveau de protection dont vous avez besoin. Favoriser la collaboration prend du temps et, compte tenu de l'augmentation des attaques, vous ne pouvez pas vous permettre d'attendre plus longtemps.

- Le phishing est l'une des cyberattaques les plus faciles et rapides, dont l'impact est le plus dangereux. **Les organisations non formées ont 40 % de chances d'être la proie** d'attaques de phishing, même si elles utilisent les bonnes technologies.

Vos bénéfices avec nos solutions centrées l'humain :

- **Réduisez rapidement** les risques d'erreur humaine, qui ont un impact sur votre activité, en renforçant les connaissances de vos équipes en termes de sécurité.
- **Déploiement rapide** d'un programme de sensibilisation à la sécurité.
- **Adoption et engagement efficients** de vos équipes
- **Une culture de la cybersécurité** solidement ancrée dans votre organisation.
- **Meilleur retour sur investissement** pour vos défis en matière de cybersécurité.



Approach Human-Centric Cybersecurity Framework (HCCF)

Pour parvenir à une culture de sensibilisation à la cybersécurité, nous avons élaboré un cadre de cybersécurité centré sur l'humain - en nous concentrant sur le facteur le plus important : «L'attention humaine est limitée». Vous devez donc hiérarchiser vos actions et commencer par les risques les plus critiques.

Notre cadre de travail a prouvé son efficacité et nous permet d'identifier vos besoins en matière de cybersécurité tout en favorisant la meilleure expérience utilisateur.

Nous travaillons en partenariat avec des plateformes de sensibilisation à la sécurité de premier plan, telles que "KnowBe4 security awareness & training".

Notre objectif : vous bénéficiez d'une utilisation plus rapide et plus adaptée à votre organisation.

Nous sommes des experts en cybersécurité tout en utilisant un vocabulaire adapté qui facilitera une adoption efficiente de notre solution. Avec notre **approche centrée sur l'humain** et notre soutien sur le terrain, nous vous aiderons à impliquer vos équipes et à les préparer, quel que soit leur environnement - ce sont des facteurs clés pour réduire les risques avec succès.

Nous prenons soin de votre sensibilisation à la cybersécurité à l'aide de notre programme sur le long terme et nous vous fournissons des résultats sur le court terme avec des suggestions d'améliorations en continues.

Notre solution complète répondra à vos défis en fonction de vos priorités et de vos risques :

- **Evaluation et tests de phishing :** Le phishing est l'une des cyberattaques les plus courants et les plus réussis, et elles constituent un élément important à la sensibilisation de la sécurité. Nous pouvons évaluer la sensibilisation de vos équipes et simuler des attaques réalistes pour les mettre à l'épreuve et les maintenir vigilantes.

- **Formations de sensibilisation à la sécurité :** Formez régulièrement vos utilisateurs à comprendre les risques de sécurité et de cybersécurité, à identifier les attaques ciblées et à réagir de manière appropriée. Nous adaptons notre grande bibliothèque de contenus de formation à la sécurité à votre organisation (langue, culture, priorités...).

- **Culture de la cyber-sécurité** : Nous changeons les attitudes, les croyances, les attentes et les façons de faire pour intégrer une gouvernance solide, complète et centrée sur l'humain. Nous vous aidons à définir votre culture de la cybersécurité : comment vous gerez la sécurité dans votre organisation. En conséquence, les personnes incluront la cybersécurité dans les postes, les collaborations et la communication. Afin de s'aider mutuellement à être plus sûr et de se sentir en sécurité, ils signaleront les incidents au moindre doute.

Pourquoi nous choisir

- **20 ans d'expertise en cyber-sécurité** et dans la confidentialité des données
- **Équipe de psychologues** pour comprendre les changements comportementaux et culturels nécessaires au renforcement de votre cyber-résilience.
- **Diriger des recherches universitaires** sur la psychologie de la cybersécurité
- **Notre méthodologie est conforme** aux recommandations de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour un cadre de changement de comportement.
- **Approche globale et holistique** prenant en compte les personnes, les processus et les technologies pour un impact à long terme.
- **Une assistance locale pour adapter le programme de sensibilisation** à la sécurité à vos besoins et à la culture de votre entreprise afin d'obtenir le meilleur retour sur investissement.
- **Les meilleurs outils sur le marché**, qui sont abordables et disponibles.