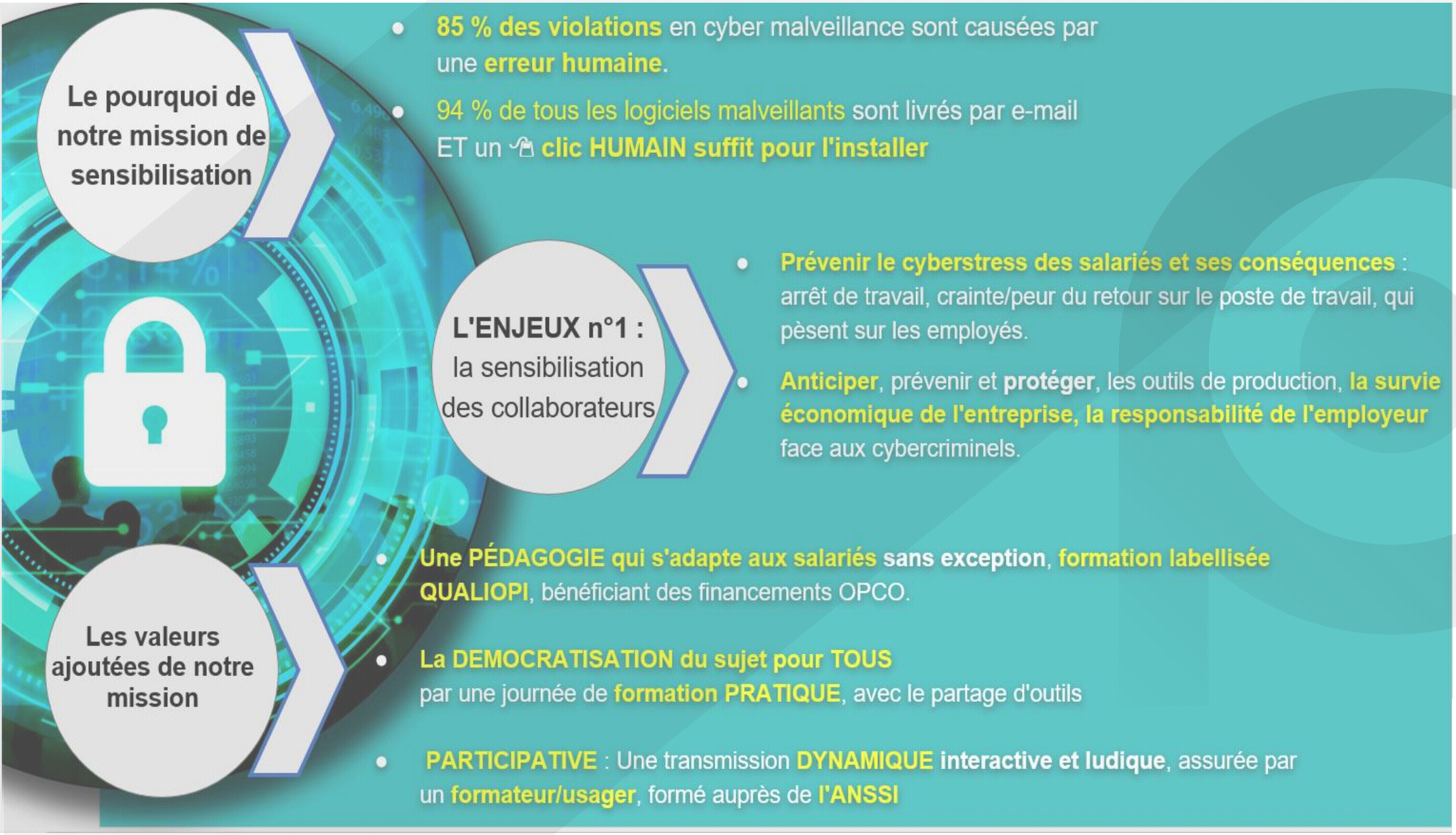
Personwall
PRIVACY BY DESIGN

Pourquoi nous ?



Le pourquoi de notre mission de sensibilisation

- **85 % des violations** en cyber malveillance sont causées par une **erreur humaine.**
- 94 % de tous les logiciels malveillants sont livrés par e-mail ET un **clic HUMAIN suffit pour l'installer**

L'ENJEUX n°1 : la sensibilisation des collaborateurs

- **Prévenir le cyberstress des salariés et ses conséquences** : arrêt de travail, crainte/peur du retour sur le poste de travail, qui pèsent sur les employés.
- **Anticiper**, prévenir et **protéger**, les outils de production, **la survie économique de l'entreprise, la responsabilité de l'employeur** face aux cybercriminels.

Les valeurs ajoutées de notre mission

- **Une PÉDAGOGIE qui s'adapte aux salariés sans exception, formation labellisée QUALIOPI**, bénéficiant des financements OPCO.
- **La DEMOCRATISATION du sujet pour TOUS** par une journée de **formation PRATIQUE**, avec le partage d'outils
- **PARTICIPATIVE** : Une transmission **DYNAMIQUE interactive et ludique**, assurée par un **formateur/usager**, formé auprès de **l'ANSSI**

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE

CLIENTS

Ils nous font confiance

« adaptabilité, dynamisme, rendre ludique et interactif un sujet qui peut paraître au premier abord ardue. »
Christiane VANNIER : directrice du **Centre De Prévention médical Bien Vieillir Agirc Arrco AURA**

« formation basée sur l'information concrète et la prévention des risques »
Zenab AMIDOU GIUSTI : Notaire

« Très concret, des outils applicables dans la foulée de la formation. Discuter de nos expériences personnelles afin d'avoir de réels conseils et outils adaptés à nos besoins »
Maxime PUECHBROUSSOUX : **Chargé de communication/marketing digital CFA FormaSup ARL**

« Concret, stimulant et efficace en terme de prise de conscience »
Laurent SLUSAREK : directeur Général Appolon Bioteck

Planificateur de formation J1

MODULE 1 - qui sont les hackers (pirates), pourquoi et comment ils attaquent ?

MD1.1: pendant 30 mn : prise en main
exercice d'apprentissage, travail d'équipe en simulation

début de la formation : 09H00

équipe des chapeaux Blancs: elle est composée de collaborateurs du Centre.
Une information circule indiquant que la structure pour laquelle ils travaillent va être attaquée par des hackers (La SpartakTeam). Ils doivent s'organiser ensemble pour définir des actions immédiates de défense, de prévention et de protection qui ne nécessite pas de compétences en informatique.

il s'agit d'inviter les collaborateurs à penser
Les failles éventuelles qu'ils auraient eux-mêmes
Détectés sur leur propre site de travail où
Poste de travail.

équipe des Chapeaux Noirs: la SpartakTeam, composée d'hacker.
Ils ont un projet de cyberattaque sur le l'association GAZ
Leurs objectifs : pirater des emails, prendre la main sur sessions et copier des informations.

L'objectif est de sensibiliser et amener les collaborateurs à penser de manière spontanée aux actions de protection de premier niveau : protection des mots de passe et de complexité, mise à jour des softwares anti-virus,
Utilisation des périphériques sécurisés: clés USB, DDR…
protection des données et sauvegarde

MODULE 1 - qui sont les hackers (pirates), pourquoi et comment ils attaquent ?

MD1.2 : Qui me menace et comment ?

De 09H30 à 10H30

attaques massives : phishing/botnet/DDos/rançonnage

attaques ciblées : APT/Cheval de Troie/spyware/ver/virus

Comprendre les principes et le fonctionnement des types et techniques d'attaques.

Pause de 10H30 à 10H45

MD1.3 : Les sources de motivation des hackers

De 10H45 à 12H00

recherche faille informatique attaques d'influence/notoriété/image

économique / bitcoin défis techniques

QUIZ sur module 1 :
« qui nous menace ? comment ? pourquoi ? »
L'objectif est de s'assurer d'une bonne compréhension de l'environnement, des enjeux et de la sensibilité du sujet. Que chacun se sent à son échelle responsable et concerné.

MODULE 2 - cyberattaques : quelles conséquences et quelles actions défensives ?

Feedback de la matinée et tour de table.
Début de la formation à 13H30

MD2.1 : panorama des attaques

De 13H30 à 14H00

MD2.2 - 14H00 à 15H00 : les conséquences des cyberattaques :

- Pertes financières / perte d'image
- Perte d'exploitation et de chiffre d'affaire
- Perte de données

MD2.3 - 15H15 à 15H45 : protection du cyberespace:

- Quelles actions et protections mettre en place
- Les règles d'or de la cybersécurité (ANSSI)
- Quel rôle jouons-nous en tant que collaborateur ?

MODULE 2 - cyberattaques : quelles conséquences et quelles actions défensives ?

TOUS RESPONSABLES

De 13H30 à 14H00

MD2.4-15H45 à 16H15 :
protection du cyberespace

Le stockage/ importance
obsolescence/accessibilité

Présentation du triptyque de la cybersécurité :
Confidentialité, Intégrité, disponibilité (avaliability)

MD2.5 :15H45 à 16H15 :
protection du cyberespace

Attaques liées à l'authentification et au mot de passe.
notion de cryptographie

Rappel des différentes attaques sur mot de passe :
attaque force brut, attaque par dictionnaire
Un mot de passe fort ? C'est quoi ?

MD2.6 :16H15 à 16H45 : atelier de protection de l'information/data par construction d'une phrase de passe.