SelfProtect

Aider chaque collaborateur à identifier et réduire son exposition numérique

Public cible : Direction générale, COMEX/CODIR, RSSI, DSI, équipes communication interne et managers métiers.

SelfProtect transforme les signaux d'exposition en actions de remédiation personnalisées : chaque utilisateur consulte les données qui le concernent, comprend les risques associés et suit des recommandations concrètes. Côté administration, SelfProtect permet de suivre l'adoption et la progression sans donner accès aux données personnelles détaillées.

UTILISATEUR
Application mobile et web pour visualiser sa propre exposition numérique

REMÉDIATION
Plan d'actions personnalisé selon les données exposées

ADOPTION
Suivi de l'enrôlement et de la progression via SelfProtect Manager

POURQUOI ?

- **Le collaborateur reste la cible privilégiée des attaques d'ingénierie sociale :** phishing, SMS frauduleux, usurpation, chantage, vol d'identifiants et contournement MFA.
- **Pour agir, il doit voir concrètement ce qui est exposé le concernant :** emails, téléphones, comptes, mots de passe, IBAN ou indices de compromission selon les sources détectées.
- **La remédiation devient efficace quand elle est contextualisée, individualisée et directement reliée** à l'exposition réelle de l'utilisateur.
- **SelfProtect complète PeopleSight :** le RSSI pilote le risque, le collaborateur consulte ses propres données et effectue les actions correctives.

FONCTIONNALITÉS CLÉS

Exposition personnelle
Vue utilisateur des données exposées qui le concernent, avec distinction des sources et catégories quand elles sont disponibles.

Plan d'action personnalisé
Actions à faire, ignorées ou corrigées : changement de mot de passe, activation MFA, vérification de comptes, traitement des sources exposées.

Niveau de protection
Indicateur individuel qui évolue au fil des corrections. L'administrateur suit les tendances globales et l'adoption, sans accéder aux données personnelles détaillées.

Vérification de données compromises
Recherche ponctuelle d'une adresse email, d'un numéro de téléphone, d'un pseudonyme ou d'un IBAN dans les données compromises, selon l'offre souscrite.

Tutoriaux & fiches d'aide
Guides pratiques pour sécuriser comptes, messageries, réseaux sociaux, MFA et situations d'usurpation.

SelfProtect Manager
Console de pilotage permettant de suivre l'activation des licences, les utilisateurs actifs, les groupes, les déploiements, les invitations, les niveaux de protection, les taux de remédiation et de générer des exports CSV.

BÉNÉFICES PAR DÉCIDEUR

DIRECTION GÉNÉRALE
Réduire l'exposition des collaborateurs clés sans alourdir l'expérience de travail ni créer de rupture opérationnelle.

RSSI
Passer d'une sensibilisation générale à une **sensibilisation ciblée** couplée à une remédiation mesurable et suivie dans le temps.

DSI
Renforcer l'efficacité de l'IAM, du MFA et de la sécurité cloud/SaaS par un engagement utilisateur concret.

CAS D'USAGE

Onboarding collaborateurs sensibles
Équiper dirigeants, finance, RH, IT, administrateurs, vendeurs et fonctions exposées avec une application de remédiation.

Campagnes de sensibilisation ciblées
Remplacer ou compléter les tests phishing génériques par des actions contextualisées sur l'exposition réelle.

Remédiation post-audit
Transformer le diagnostic PeopleSight en actions utilisateurs et mesurer la progression.

Protection sphère pro/perso
Tenir compte de la réalité de l'attaque : l'attaquant utilisera toute donnée à sa disposition qu'elle soit d'origine personnelle ou professionnelle.

Suivi managérial et gouvernance
Mesurer l'adoption, relancer les populations concernées et piloter l'amélioration globale.

GOUVERNANCE, CONFORMITÉ & SÉCURITÉ

- **Les données personnelles détaillées ne sont accessibles qu'à l'utilisateur concerné**. L'administrateur dispose des indicateurs nécessaires au suivi du déploiement et de la progression.
- **Le déploiement peut être organisé par vagues :** groupes sensibles, directions métiers, utilisateurs exposés ou volontaires.
- **La progression des actions est suivie** afin de relier adoption, sensibilisation et évolution du niveau de protection.
- **Le dispositif doit être cadré avec le responsable de traitement et le DPO**, notamment pour l'information des collaborateurs, les droits d'accès et la conservation des données.

DÉPLOIEMENT TYPE

1. Préparation
Définir les populations à inclure, le message d'accompagnement, le support interne et les objectifs d'activation.

2. Enrôlement
Activation par lien ou QR code, idéalement lors d'une courte session de sensibilisation, puis relance des utilisateurs non enrôlés par groupe ou population cible.

3. Remédiation
Consultation des données exposées, traitement des actions prioritaires, tutoriels et bonnes pratiques.

4. Pilotage
Suivi des licences activées, niveaux de protection, taux de progression et population à relancer.

À retenir
SelfProtect est le volet opérationnel de la démarche PeopleSight : PeopleSight mesure et priorise ; SelfProtect engage l'utilisateur et matérialise les remédiations.
Leur combinaison permet de suivre l'évolution du risque et des actions engagées.

DÉPLOYEZ SELFPROTECT AUPRÈS D'UNE POPULATION SENSIBLE

Une démarche progressive pour engager les utilisateurs

Sensibilisation • Enrôlement guidé • Consultation de l'exposition • Remédiation • Suivi RSSI/DSI