PeopleSight

Mesurer, prioriser et piloter le risque cyber humain

Public cible : Direction générale, COMEX/CODIR, RSSI, DSI, Risk Managers, équipes IAM/GRC.

PeopleSight donne aux dirigeants, RSSI et DSI une vision factuelle de l'exposition numérique des collaborateurs et des tiers, telle qu'elle peut être exploitée par un attaquant.

L'objectif : rendre le risque humain visible, mesurable et actionnable.

VISIBILITÉ
Cartographie du risque cyber humain à l'échelle de l'organisation

PRIORISATION
Identification des populations et identités les plus exposées

PILOTAGE
Indicateurs exploitables pour RSSI, DSI, COMEX et métiers

POURQUOI ?

- **Les attaques ciblées commencent souvent par une phase de reconnaissance :** données professionnelles, données personnelles, corrélations et effets pivots.
- **Les protections techniques classiques protègent les accès, mais voient mal l'exposition numérique disponible hors du SI.**
- **Les dirigeants, fonctions financières, administrateurs, métiers sensibles, prestataires et tiers exposés deviennent des points d'entrée crédibles pour l'ingénierie sociale.**
- **La sensibilisation générique ne suffit pas :** il faut objectiver le risque, le suivre dans la durée et orienter les actions vers les personnes réellement exposées.

FONCTIONNALITÉS CLÉS

Tableau de bord du risque humain
Vue consolidée par population, identité, période et scénario de menace : compromission de compte, hameçonnage ciblé, smishing, contournement MFA et SIM swapping.

Analyse individuelle
Lecture du score et des facteurs de risque utiles au pilotage. Les données personnelles détaillées restent accessibles selon les droits et le cadre de confidentialité définis.

Surveillance continue
Détection et mise à jour des signaux d'exposition : emails professionnels fuités, données compromises, sites tiers, comptes exposés, sources OSINT et dark web utilisées par les attaquants.

Segmentation métier
Ciblage par groupes sensibles : direction générale, finance, paie, RH, IT, administrateurs, projets stratégiques, prestataires ou comptes tiers.

Plans d'action
Actions recommandées selon les facteurs détectés : traitement des comptes exposés, renforcement de l'authentification, information des utilisateurs et suivi des corrections..

Exports & rapports
Rapports exploitables pour comités de pilotage, tableaux de bord de maturité, revues RSSI/DSI, exigences de conformité et arbitrages budgétaires.

BÉNÉFICES PAR DÉCIDEUR

DIRECTION GÉNÉRALE
Transformer un risque invisible en indicateur de pilotage, **anticiper** les crises cyber et **protéger** l'image de l'organisation.

RSSI
Prioriser les remédiations selon le niveau d'exposition,le profil de la personne et les scénarios de menace associés, puis suivre leur évolution.

DSI
Compléter MFA, IAM, SIEM, EDR et sensibilisation par une **vision externe**, contextualisée et actionnable du risque humain.

CAS D'USAGE

Cartographie initiale
Identifier rapidement les populations les plus exposées et établir une base de référence cyber-humaine.

Protection des VIP
Surveiller dirigeants, COMEX, finance, RH, administrateurs et personnes manipulant des données sensibles.

Gouvernance cyber / GRC
Produire des indicateurs exploitables sur le risque cyber humain : score global, populations exposées, niveaux de menace, fuites d'emails professionnels et exports CSV.

Gestion des tiers
Suivre les comptes, prestataires ou partenaires exposés lorsqu'ils représentent une porte d'entrée vers l'organisation.

Prévention fraude & usurpation
Réduire les opportunités de spear-phishing, fraude au président, prise de contrôle de compte, SIM swapping et ingénierie sociale.

GOUVERNANCE, CONFORMITÉ & SÉCURITÉ

- Approche fondée sur la **mesure du risque humain et l'intérêt légitime de cybersécurité**, avec séparation entre données utiles au pilotage et données personnelles visibles uniquement par l'utilisateur concerné.
- Données issues de sources ouvertes, clear web, deep web ou dark web, **sans aucun achat de données**.
- **Hébergement européen, DPO dédié et conformité RGPD.**
- **Possibilité d'intégration** avec les processus IAM, GRC, SIEM, SOAR, XDR via les APIs HRM.

DÉPLOIEMENT TYPE

1. Cadrage
Domaines, population cible, groupes sensibles, objectifs, niveau de confidentialité et KPI de pilotage.

2. Configuration
Définition des populations à analyser, import du périmètre concerné, tags éventuels, lancement du scan et paramétrage des vues de suivi.

3. Restitution
Rapport d'exposition, recommandations priorisées, plan de remédiation et arbitrages RSSI/DSI.

4. Suivi continu
Revues mensuelles, évolution des scores, nouvelles expositions, pilotage COMEX/CODIR.

À retenir
PeopleSight identifie, qualifie et priorise le risque. **SelfProtect aide** ensuite chaque **collaborateur** à consulter son exposition et à traiter les actions qui le concernent. Ensemble, les deux modules constituent une boucle complète : **mesurer > décider > agir > suivre l'évolution.**

ÉVALUEZ VOTRE EXPOSITION SUR LES PROFILS LES PLUS SENSIBLES

Un audit ciblé pour identifier les risques et prioriser les actions

Évaluation des risques • Synthèse exécutive • Priorisation des remédiations • Restitution RSSI/DSI