

ÉVALUATION & SUPERVISION DES RISQUES

Réduire la surface d'attaque **humaine** de son organisation

CHALLENGES

80% des cyberattaques exploitent les vulnérabilités humaines. Aujourd'hui, pour impacter une entreprise, il est plus facile et efficace pour un attaquant d'exploiter les vulnérabilités des dirigeants et collaborateurs plutôt que d'exploiter les vulnérabilités techniques.

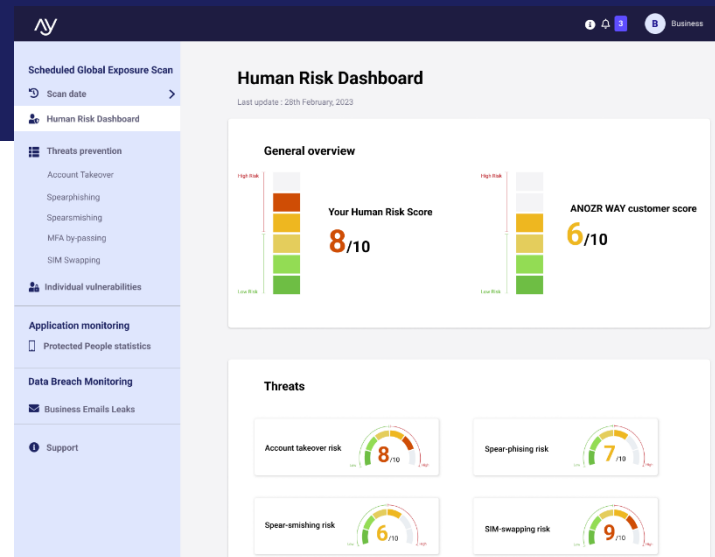
Les équipes SSI et risque ont des difficultés à adresser le « risque humain » et ont peu de contrôle sur cette zone aveugle.

BÉNÉFICES

Connaître les menaces imminentes qui ciblent vos dirigeants et collaborateurs avec une vue globale sur l'entreprise et un scoring individuel

Éliminer le mal à la source en agissant dès la phase de reconnaissance de la Cyber Kill Chain (collecte de vulnérabilités)

Gain de temps et de ressources grâce à une évaluation des risques actionnable et un plan d'actions de remédiation priorisé



SOLUTION



Prévenir les risques humains et maîtriser l'exposition cyber professionnelle en continu sur l'ensemble des collaborateurs

Identifier les dirigeants et collaborateurs les plus exposés du point de vue d'un attaquant pour prioriser les actions de remédiation

Détecter les usages non conformes à la charte informatique via la supervision des emails professionnels

MENACES ADRESSÉES

Ingénierie sociale

Fraude, arnaque financière

Fuite de données
RansomwareSpear-phishing,
smishing, vishingCompromission
de comptesContournement MFA
SIM-swappingEspionnage,
vol de PIWhaling
Usurpation d'identité

FONCTIONNALITÉS

Évaluation & analyse des risques

Scan et scoring de l'exposition cyber humaine de l'entreprise et détails par menace : Spear-phishing, vol de credentials et compromission de comptes dont « BEC », contournement de l'authentification MFA, SIM-swapping...

Identification des collaborateurs les plus à risque, du point de vue d'un attaquant

Détectez également les usages illicites à la charte informatique liés aux emails professionnels (création de comptes à usages personnels, mots de passe compromis, etc.)

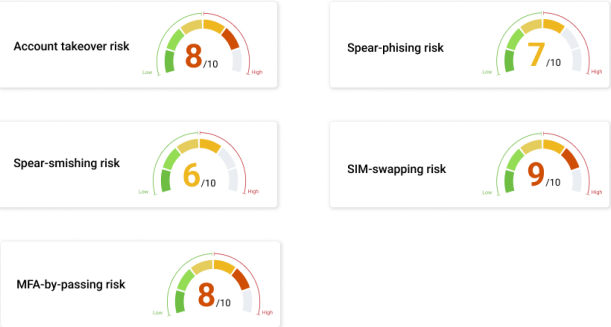
Monitoring

Alertes dès nouvelles fuites de données et compromissions de comptes liées aux emails professionnels des collaborateurs.

Remédiation

Pour une chaîne complète de remédiation et en conformité avec le RGPD, les collaborateurs sont équipés d'une application pour corriger leurs propres vulnérabilités « pro » et « perso ».

Threats



People risks

USERS		GLOBAL RISK	ACCOUNT TAKEOVER	PHISHING	SMISHING
	Louis Ondrejcek	9	7	3	
	Arnaud Leimane	8	8	9	
	Claude Leborgne	8	6	6	
	Clarisse Gueroi	7	5	4	
	Louis Flis	7	5	4	
	Lucie Platine	7	6	4	
	Philippe Murin	7	6	4	
	Mathieu Litus	7	6	6	
	Maelle Dumortier	7	6	3	
	Alam Naïpe	7	6	6	

Persons protected by AY App

1-2-3...200

TECHNOLOGIE AUTOMATISÉE 100% PROPRIÉTAIRE & SOUVERAINE

À partir du domaine email de l'entreprise comme donnée d'entrée, la technologie ANOZR WAY reconstitue la surface d'attaque humaine de l'organisation automatiquement, jusqu'à des milliers de collaborateurs.

Exemple : pour 2 000 collaborateurs, 35 000 recherches de données par pivot sont réalisées automatiquement sur les différentes strates d'internet (réseaux sociaux, deep et darkweb) équivalent à 182 jours-hommes !

A PROPOS

ANOZR WAY est une startup française editrice de logiciels dédiés à la gestion des **vulnérabilités humaines** pour **réduire les risques cyber** et de **fraudes**. Nous aidons les PME, ETI, Grands Groupes de tous secteurs ainsi que le Public et le Régalien, à protéger leurs VIP/dirigeants, collaborateurs et clients/utilisateurs. Nos solutions logicielles sont basées sur une **technologie automatisée 100% propriétaire, souveraine et conforme RGPD**. Notre plateforme est disponible en SaaS, On-Premise et API.

Pour contacter l'équipe commerciale : demo@anozrway.com