



CreativMinds
Empowering change



Objectif : Cyber Safe

Sensibilisation à la cybersécurité

Objectif : Cyber Safe

Sensibilisation à la cybersécurité

Description

Objectif : Cyber Safe est un programme de sensibilisation à la cybersécurité sur 3 ans, conçu pour réduire les risques humains et faire progresser la maturité interne de votre organisation.

De la prise de conscience à l'autonomie, jusqu'à la conformité aux standards d'entreprise, vos équipes suivent des cycles d'apprentissage structurés et mesurables. Chaque phase intègre des contenus ciblés, des activités pratiques et un reporting à destination de la direction.

Résultat : des comportements qui changent, des preuves concrètes pour les audits, et des collaborateurs qui deviennent un véritable atout en matière de sécurité.

Phases

Année 1 Les fondamentaux

Objectifs :

- Sensibiliser aux menaces numériques majeures
- Éliminer les comportements à risque
- Diffuser les bons réflexes à l'échelle de l'organisation

Contenu :

- Modules LMS fondamentaux
- Webinaire de lancement
- 3 QuickCards
- Quiz certifiants
- Évaluation du risque initial & checklist de remédiation
- Certificats de complétion

Année 2 Montée en autonomie

Objectifs :

- Responsabiliser les équipes
- Intégrer la sécurité dans les routines de travail
- Réduire les erreurs récurrentes

Contenu :

- Modules LMS avancés & scénarisés
- Newsletters thématiques + quiz d'équipe
- Sessions Q&A et Deep Dives
- Rapport de maturité intermédiaire
- Simulations pratiques (option)

Année 3 Maturité & conformité

Objectifs :

- Atteindre les standards de conformité
- Prouver le niveau de préparation interne
- Intégrer la cybersécurité dans l'onboarding & la gouvernance

Contenu :

- Modules LMS experts
- Dashboard KPI prêt pour la direction
- Score de maturité final
- Intégration dans l'onboarding RH
- Rapport de synthèse pour le CODIR
- Accompagnement aux audits / certifications (optionnel)

⚠ Le nombre, la fréquence et le niveau de personnalisation des activités ci-dessus dépendent du forfait choisi (Basic, Branding, Bespoke).

Bénéfices

Une solution structurée, peu exigeante en termes d'efforts et à forte valeur stratégique :

- Accès LMS sécurisé avec suivi individuel
- Rapports de progression prêts pour les dirigeants
- Certificats nominatifs pour prouver la conformité
- Checklists de remédiation par thématique
- Support & FAQ centralisé

Objective: Cyber Safe

Formules d'abonnement & modalités de déploiement

Description

Pour vous accompagner tout au long de votre parcours cybersécurité — Fondamentaux, Autonomie, Maturité — nous proposons des formules d'abonnement flexibles, adaptées à la taille, aux ambitions et aux exigences de conformité de votre organisation.

Toutes les formules s'appuient sur le même cadre structuré. La différence ? Le niveau d'engagement, de personnalisation et d'intégration stratégique.

Formules

Plan 1 - Basique

✓ PME ou déploiement pilote
(up to 300 users)

Déploiement rapide avec accès LMS, contenus standards et reporting de base.

Idéal pour démarrer la sensibilisation et réduire les risques critiques.

Objectifs :

- Diffuser les fondamentaux
- Éliminer les comportements à risque
- Obtenir des premiers résultats mesurables

Plan 2 - Branding

@ Déploiement par entité
(300–1000 users)

Intègre la charte graphique, du contenu avancé, des sessions Deep Dive, et un suivi de maturité.

Renforce l'engagement des équipes et favorise l'adoption à plus grande échelle.

Objectifs :

- Renforcer les bons réflexes
- Responsabiliser les collaborateurs
- Suivre l'évolution des KPIs de sécurité

Plan 3 - Sur-mesure

🧠 Déploiement global
(1000+ users)

Contenus personnalisés, cas d'usage spécifiques, coaching ciblé.

Dashboards exécutifs, onboarding RH et préparation aux audits inclus. Pour les organisations à forte exigence de conformité.

Objectifs :

- S'aligner sur les exigences de gouvernance
- Fournir des preuves concrètes de maturité
- Intégrer la cybersécurité à la culture d'entreprise

Bénéfices

Des formules d'abonnement flexibles conçues pour répondre à vos besoins :

- Toutes les formules suivent le cadre Cyber Safe sur 3 ans (Fondamentaux → Autonomie → Maturité)
- Choisissez votre niveau de personnalisation, d'accompagnement et de reporting
- Le plan Sur-mesure est recommandé pour les organisations soumises à des audits ou certifications

Choisissez la formule adaptée à votre niveau de maturité cyber

Description

Nos trois formules s'appuient sur la même structure éprouvée Cyber Safe sur 3 ans — seule la profondeur, la personnalisation et l'échelle du programme varient. Toutes incluent des mises à jour continues du LMS avec des livrables définis par formule. Des services additionnels peuvent être ajoutés selon vos besoins.

Comparaison des formules

Fonctionnalités	Plan 1	Plan 2	Plan 3
Quick Cards	3 standard	5 avec branding	5+, adaptées aux cas d'usage interne
Modules eLearning	12 modules standards	12 modules avec identité visuelle	12 modules adaptés au contexte interne
Webinaires	Webinaires trimestriels standards (live or replay)	Webinaires trimestriels personnalisés (live or replay)	Webinaires trimestriels sur mesure (live or replay)
Newsletters	Trimestrielles, génériques	Trimestrielles, adaptées à votre secteur	Trimestrielles, sur mesure avec actualités internes
Reporting	Rapport initial + score de sensibilisation	+ rapport de maturité intermédiaire	+ tableau de bord final (prêt CODIR)
Tarif	29 CHF / pers. / mois*	Sur demande	Sur demande

Engagement minimum de 12 mois – 290 CHF / utilisateur / an (≈ 10 % de remise) ou 2'200 CHF / 10 licences / an (≈ 15 % de remise)
⚠ Les volumes sont fixes par activité. Personnalisations ou sessions supplémentaires disponibles sur demande (facturation séparée).

Bénéfices

- Toutes les formules suivent la structure Cyber Safe sur 3 ans (Fondamentaux → Autonomie → Maturité)
- Offres à prix fixe incluant l'accès LMS et les certifications
- Newsletters et contenus internes personnalisables
- Passage facile d'un plan à un autre selon vos besoins d'évolution ou de conformité

Nos modules de cybersécurité

Sensibilisation à la cybersécurité

- Introduction à la cybersécurité
- Comprendre les bases de la cybersécurité
- Créer des mots de passe robustes
- Sécuriser sa messagerie électronique
- Naviguer sur le web en toute confidentialité
- Se protéger contre l'ingénierie sociale
- Adopter le principe du bureau propre
- Déjouer les tentatives de phishing
- Identifier les logiciels malveillants
- Adopter les bonnes pratiques sur Internet
- Comprendre l'usurpation d'identité
- Sécuriser l'usage des réseaux sociaux
- Travailler à distance en toute sécurité
- Se protéger contre les rançongiciels
- Éviter la compromission des e-mails professionnels
- Reconnaître une menace interne involontaire
- Signaler efficacement un incident
- Identifier les sites frauduleux
- Utiliser les services cloud en toute sécurité
- Renforcer sa posture de sécurité (être Security Aware)
- Se protéger du spear phishing / fraude au président
- Comprendre les techniques de phishing
- Se prémunir contre le smishing
- Gérer les risques liés à l'IA
- Relever les défis actuels en cybersécurité
- Gouverner la sécurité au quotidien
- Montrer l'exemple en matière de cybersécurité

Sécurité des systèmes et des accès

- Sécuriser les accès physiques
- Gérer le contrôle des accès
- Mettre en place une politique BYOD sécurisée
- Sécuriser les appareils mobiles
- Voyager sans compromettre la sécurité
- Protéger son ordinateur personnel à domicile
- Gérer les risques liés aux réseaux Wi-Fi
- Sécuriser l'utilisation des smartphones
- Comprendre l'authentification MFA
- Aperçu de la sécurité réseau
- Identifier les attaques réseau courantes
- Sécuriser l'infrastructure réseau
- Aperçu de la sécurité applicative
- Reconnaître les attaques applicatives courantes
- Adopter un développement sécurisé
- Introduction à la cryptographi

Protection des données

- Classer efficacement les informations
- Comprendre le cycle de vie des données
- Protéger ses données personnelles
- Sécuriser les paiements en ligne
- Réagir face à une fuite de données
- Encadrer la collecte des données personnelles
- Respecter les principes de la vie privée
- Identifier les atteintes à la vie privée
- Sécuriser les référentiels de données

Contactez-nous



+41 21 561 16 01



zoey.faromont@creativminds.ch



Rue de la Gare 1, 1260 Nyon
VD Suisse



www.creativminds.ch



CreativMinds
Empowering change