

Formation CYBERDISE

Contenu 2025

Une approche unique, modulaire et personnalisable de la formation en cybersécurité pour les organisations aux besoins complexes

Principaux avantages

- Basé sur un concept didactique bien défini pour une cohérence maximale du portefeuille.
- Modules entièrement personnalisables : modifiez, ajustez ou ajoutez du contenu personnalisé selon les besoins et les politiques de votre organisation.
- Marque blanche : ajoutez votre CI/CD et votre contenu en marque blanche pour correspondre à l'identité visuelle de votre organisation.
- Formats de formation flexibles : choisissez entre texte, vidéo ou un mélange selon les préférences de votre équipe.
- Parcours d'apprentissage structuré : Théorie → Jeu → Examen pour une formation engageante et mesurable.
- Toujours à jour : accédez au contenu 2025 le plus récent pour anticiper les menaces émergentes.
- Intégration de contenu personnalisé : formez les employés avec vos propres politiques et supports.
- Leçons courtes et ciblées : modules brefs de 5 à 15 minutes pour minimiser les interruptions.
- Portée mondiale : contenu traduit et localisé professionnellement en plus de 12 langues.
- Conception adaptée aux mobiles : formez-vous à tout moment, n'importe où, sur n'importe quel appareil.
- 20+ sujets essentiels couvrant les niveaux de base à avancé – conçus pour soutenir l'intégration des employés, la reformation régulière, et la conformité, avec des parcours personnalisables pour chaque organisation.

Le portefeuille de formation à la sensibilisation à la sécurité CYBERDISE repose sur une structure didactique et pédagogique solide, garantissant que le contenu d'apprentissage soit à la fois engageant et efficace pour favoriser un changement de comportement. Les modules permettent aux organisations ayant des exigences de sécurité complexes d'adapter la formation à leurs défis spécifiques, politiques et profils de risque. Cela vous aide à transmettre le « pourquoi » des politiques de sécurité et à les responsabiliser pour devenir une ligne de défense proactive contre les cybermenaces.

Voici la liste de nos sujets de formation, conçus pour sensibiliser, instaurer une culture de la sécurité et donner à votre équipe les moyens de prendre des décisions éclairées et sécurisées :

Programme complet de cybersécurité (CCC) avec plus de 20 sujets du niveau basique à avancé

Sensibilisation à la cybersécurité

- Impact des cyberattaques sur les entreprises, les employés et les individus
- Rôle des employés dans la prévention des violations

Mentalité et comportement en cybersécurité

- Réflexe de sécurité, détection d'anomalies et sensibilisation à la sécurité physique
- Processus de signalement et habitudes de réaction

Concepts fondamentaux de la cybersécurité

- Intégrité, disponibilité, authentification, autorisation, risques, chi rement, vulnérabilités, réponse aux incidents



Next Gen Security
Awareness Training



Gold Winner-
Company of the Year



Cybersecurity Learning
Management System

«La solution moderne répond à tous nos besoins. C'est un élément essentiel de notre protection contre les cybermenaces, elle contribue fortement à la sensibilisation et réduit les risques. Nous recommandons vivement CYBERDISE.» **Ismael Aemisegger, Responsable de l'équipe support IT chez GLB**

« En tant qu'ingénieur système, j'ai pu lancer ma première campagne de phishing en 30 minutes, y compris l'installation. J'ai configuré le système, ajouté des domaines, généré des certificats SSL, créé une simulation de phishing à partir d'un modèle, ajouté des utilisateurs, et j'étais prêt. Ce que j'ai particulièrement apprécié, ce sont les vérifications de campagne ! » **Norman Umbach, Consultant Senior chez DSS-CONNECT**

Types de menaces cyber courantes

- Malware, phishing, ransomware, DDoS, menaces internes, deepfakes, exploits zero-day

Gestion des risques cyber

- Évaluation des risques, renseignement sur les menaces, gestion des vulnérabilités, analyse d'impact métier, conformité

Notions de base en cybersécurité

- Définitions, menaces, risques et mesures de protection

Vecteurs d'attaque

- Phishing, smishing, appels vidéo deepfake, QR codes non sécurisés, clés USB, outils de messagerie

Sécurité des mots de passe

- Création et gestion de mots de passe sécurisés, authentification à deux facteurs

Protection contre les malwares

- Détection et prévention des virus, chevaux de Troie et autres programmes malveillants

Navigation sécurisée sur Internet

- Éviter les sites dangereux et les téléchargements à risque

Protection des données et confidentialité

- Traitement des données personnelles, principes de confidentialité, attentes réglementaires
- Données soumises à des exigences de protection accrues

Informations personnelles

- Types de données personnelles et stratégies de protection

Sécurité physique et visiteurs

- Contrôle d'accès, présence non autorisée, procédures de signalement
- Bureau rangé

Sécurité réseau

- Utilisation sécurisée du Wi-Fi, VPN, pare-feu

Sécurité en déplacement & en télétravail

- Protection des appareils et sécurité des données lors des déplacements professionnels
- Risques du travail à distance et comportements sûrs en dehors du bureau

Appareils mobiles

- Mesures de sécurité pour smartphones et tablettes, BYOD (Bring Your Own Device)

Réponse aux incidents

- Détection, signalement, confinement et procédures d'escalade

Compliance and legal regulations

- RGPD, CCPA, nDSG et autres cadres juridiques

Politiques de sécurité et documents internes

- Politiques internes, directives obligatoires et gestion documentaire

Sécurité IA

- Risques de manipulation par IA, détection des deepfakes, sécurisation des outils d'IA

Vidéos de sensibilisation à la sécurité

Nous proposons un large éventail de vidéos de sensibilisation à la sécurité pour compléter vos initiatives de formation. Ces vidéos sont conçues pour offrir un contenu supplémentaire et marquant qui reste en mémoire bien après la fin de la formation. En gardant la sécurité au premier plan, vous pouvez instaurer une culture de vigilance et réduire le risque de cybermenaces au sein de votre organisation.

- Vidéo de sensibilisation à la sécurité IA
- Vidéo de sensibilisation aux deepfakes
- Vidéo de sensibilisation à la sécurité des e-mails
- Vidéo de sensibilisation aux malwares
- Vidéo de sensibilisation à la sécurité mobile
- Vidéo de sensibilisation à la sécurité des mots de passe
- Vidéo de sensibilisation au phishing
- Vidéo de sensibilisation aux réseaux sociaux
- Vidéo de sensibilisation au télétravail
- Et bien d'autres

EN SAVOIR PLUS

Pour plus d'informations, visitez : www.cyberdise-awareness.com/

À PROPOS DE CYBERDISE

CYBERDISE AG est une entreprise de sensibilisation à la cybersécurité alimentée par l'intelligence artificielle, qui protège les plus grands atouts — et les plus grandes vulnérabilités — des organisations : leurs employés. Grâce à des solutions hautement personnalisables, CYBERDISE aide les entreprises du monde entier à renforcer la culture de vigilance face aux cybermenaces et à la protection des données, afin de rendre les personnes plus intelligentes et les entreprises plus sûres. Des organisations de toutes tailles font confiance à CYBERDISE pour des solutions de sensibilisation à la sécurité centrées sur l'humain et adaptées aux besoins les plus complexes. Plus d'informations sont disponibles sur <https://cyberdise-awareness.com/>

© cyberdise AG. cyberdise AG est une marque déposée de CYBERDISE en Suisse et dans d'autres pays. Toutes les autres marques mentionnées sont la propriété de leurs détenteurs respectifs.