PROGRAMME DE BASE

DIGITAL ET INTELLIGENCE ARTIFICIELLE

Cybersécurité : protéger son entreprise et ses données

Formation 100 % sur mesure · Intra, dans vos locaux · 2 jours (14 h)

Un mail qui ressemble à celui d'un fournisseur, un mot de passe partagé par habitude, un poste qui se bloque un lundi matin. Cette formation vous aide à adopter les bons réflexes face aux menaces et à savoir réagir en cas d'incident.

Objectifs de la formation

- Comprendre les principales menaces
- Adopter les bons réflexes au quotidien
- Protéger ses données et ses accès
- Savoir réagir en cas d'incident

PUBLIC CONCERNÉ
Tout public.

PRÉREQUIS
Aucun.

Parlons de votre besoin
Sophie Gendre · 06 42 73 39 61
Laetitia David · 06 42 73 40 54
contact@2cforma.fr
Devis gratuit sous 48 heures

Financement. Finançable par votre OPCO ou votre plan de développement des compétences. En cas de subrogation, nous déposons directement les éléments de fin de formation sur l'espace de votre OPCO.

Organisme certifié Qualiopi au titre de la catégorie Actions de formation. N° de déclaration d'activité : 53351040635

L'essentiel

DURÉE
2 jours — 14 heures

FORMAT
Groupe — 8 stagiaires maximum

LIEU
Intra, dans vos locaux
Bretagne et Île-de-France. Ailleurs en France, sur demande.

PUBLIC
Tout public

PRÉREQUIS
Aucun

TARIF
À partir de 1 350 € HT / jour
Pour un groupe de 8 personnes maximum. Selon la durée, le lieu et l'adaptation du programme à votre besoin. Devis gratuit sous 48 heures.

DÉLAI D'ACCÈS
3 semaines minimum après validation du devis, ou à la date de votre choix

ACCESSIBILITÉ
Situation de handicap ? Notre référent handicap étudie avec vous les adaptations possibles.
Laetitia DAVID, référente handicap
06 42 73 40 54 ·
laetitia.david@2cforma.fr

Programme

2 jours · 14 heures | Groupe, 8 stagiaires maximum | Théorie 40 % · pratique 60 %

Un programme de base, adapté à votre contexte. Les modules ci-dessous sont un point de départ. Nous les ajustons avec vous, selon les situations que vos équipes rencontrent au quotidien et le contexte de votre entreprise. Un seul module vous concerne ? Un sujet manque ? Contactez-nous, nous construisons le programme avec vous.

JOUR 1 Comprendre les menaces — 7 h

01 Les principales menaces : hameçonnage, rançongiciels, fraudes

02 Repérer un message ou un comportement suspect

03 Protéger ses accès et ses mots de passe

JOUR 2 Se protéger et réagir — 7 h

01 Protéger ses données et ses équipements

02 Adopter les bons réflexes en déplacement et en télétravail

03 Réagir en cas d'incident

04 Construire son plan d'action

Méthodes et évaluation

Méthodes et moyens pédagogiques

Support pédagogique remis à chaque participant, échanges interactifs, travail en sous-groupes. Méthode participative et active, avec des exercices ludiques permettant à chaque participant de s'impliquer, d'apprendre et d'expérimenter sur ses propres projets : techniques de pédagogie active, outils de créativité, visual mapping et jeux.

Modalités d'évaluation

- Avant : recueil des attentes et des situations à traiter
- Pendant : exercices et mises en situation
- En fin de formation : questionnaire d'acquisition des compétences (quiz et cas pratiques)
- À chaud : évaluation de la satisfaction par chaque stagiaire

Ce que vous recevez

PENDANT LA FORMATION
Un support pédagogique remis à chaque participant, et les outils utilisés en séance.

À L'ISSUE DE LA SESSION
Le résultat de l'évaluation des acquis, avec les points forts et les axes de progrès de chacun.

EN FIN DE FORMATION
L'attestation de fin de formation pour chaque participant.