Mise à jour : 01/03/2026

FORMATION : Fondamentaux de la Cybersécurité

PUBLIC	Cette formation est à destination de toute personne souhaitant acquérir une culture cybersécurité : IT, RH, managers, dirigeants, non-techniciens.
PRÉREQUIS ET MATERIEL RÉQUIS	Prérequis : ▪ Aucun prérequis technique. ▪ Utilisation courante d'un ordinateur et d'internet. Matériel requis : ▪ Ordinateur portable avec accès Internet, accès administrateur pour les ateliers.
MODALITÉS ET DÉLAIS D'ACCÈS	En présentiel : ⇨ Formation en présentiel : lieu de formation communiqué en amont de la formation. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation. En distanciel : ⇨ Formation individuelle ou collective à distance sous la forme de visioconférence participative. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation.
DURÉE	28H pour une période de 4 jours
DATES	À définir avec l'organisme de formation
HORAIRES	▪ Les horaires de formation sont : 9H à 12H et de 13H à 17H ▪ Le monitoring et l'assistance pédagogique sont disponibles du lundi au vendredi de 9H à 18H.
LIEU	En présentiel : ⇨ Sur site ⇨ Au siège de Tricolor Expertise ⇨ Autre adresse En distanciel : ⇨ Formation à distance – visioconférence **Pour les personnes en situation de handicap : Nous adaptons nos formations en fonction de votre handicap et nous mettrons tout en œuvre pour vous accueillir ou pour vous réorienter si besoin.** **Vous pouvez nous contacter au 06 34 31 28 65**
TARIF	3 250€ par personne
NOMBRE DE PARTICIPANTS	En présentiel : Jusqu'à 12 personnes En distanciel : Jusqu'à 5 personnes
OBJECTIF DE LA FORMATION ET COMPÉTENCES VISÉES	À l'issue de la formation, le participant sera capable de mettre en œuvre les compétences suivantes : ▪ Comprendre les concepts fondamentaux de la cybersécurité et le paysage des menaces actuelles ▪ Identifier les vecteurs d'attaques courants (phishing, ransomware, ingénierie sociale…) ▪ Appliquer les bonnes pratiques de protection des systèmes, des données et des accès ▪ Contribuer à la mise en œuvre d'une politique de sécurité dans son organisation ▪ Réagir de manière appropriée en cas d'incident de sécurité ▪ Sensibiliser son entourage professionnel aux enjeux de la cybersécurité
MODALITÉS D'ÉVALUATION D'ATTEINTE DES OBJECTIFS DE LA FORMATION	⇨ Évaluation individuelle du profil, des attentes et des besoins du participant avant le démarrage de la formation ⇨ Évaluation des connaissances & compétences en début et en fin de formation via un QCM ⇨ Tests de contrôle de connaissances et validation des acquis à chaque étape ⇨ Travaux pratiques et mises en situation ⇨ Echange avec le formateur ou la formatrice par visioconférence (webinar), téléphone et mail ⇨ Questionnaire d'évaluation de la satisfaction en fin de formation

CONTENU	Dans cette formation, le participant aura accès au programme suivant :

MODULE 1	**Paysage de la Cybersécurité (4h)** 1. Introduction à la cybersécurité 2. Acteurs et motivations 3. Cadre réglementaire et normatif 4. Stratégie de défense en profondeur 5. QCM intermédiaire + discussion
MODULE 2	**Menaces et Attaques Informatiques (6h)** 1. Ingénierie sociale et phishing 2. Malwares 3. Attaques réseau 4. Attaques applicatives 5. Autres vecteurs d'attaque Atelier : Simulation d'une campagne d'attaque, restitution collective et bonnes pratiques.
MODULE 3	**Protection des Systèmes et des Réseaux (6h)** 1. Sécurité des systèmes d'exploitation 2. Sécurité des réseaux 3. Protection des postes de travail (endpoint) 4. Sécurité du cloud Atelier : Mise en place d'une architecture réseau sécurisée simplifiée sur Packet Tracer
MODULE 4	**Gestion des Identités et des Accès (IAM) (4h)** 1. Concepts fondamentaux de l'IAM 2. Authentification et MFA 3. Gestion des accès et des rôles 4. Active Directory et annuaires Atelier et QCM : Audit des droits d'accès — scénario fictif avec matrice RBAC et Quiz sur l'IAM.
MODULE 5	**Protection des Données et Conformité (4h)** 1. Classification et cycle de vie des données 2. Chiffrement des données 3. RGPD et réglementation 4. Sauvegarde et continuité Synthèse et discussion : Retour sur les obligations légales applicables aux participants et cartographie des données de chaque organisation (exercice collectif).
MODULE 6	**Réponse aux Incidents et Bonnes Pratiques (4h)** 1. Détection et surveillance 2. Processus de réponse aux incidents 3. Bonnes pratiques au quotidien Atelier final : Simulation d'incident et debriefing.

MOYENS PERMETTANT LE SUIVI ET L'APPRÉCIATION DES RÉSULTATS	Suivi de l'exécution : ⇨ Feuilles de présences signées par les participants et le formateur ou la formatrice par demi-journée ⇨ Attestation de fin de formation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation.

	Appréciation des résultats : ▪ Recueil individuel des attentes du stagiaire ▪ Questionnaire d'auto-évaluation des acquis en début et en fin de formation ▪ Évaluation continue durant la session ▪ Remise d'une attestation de fin de formation ▪ Questionnaire d'évaluation de la satisfaction en fin de formation
MOYENS PÉDAGOGIQUES ET TECHNIQUES D'ENCADREMENT DES FORMATIONS	Modalités pédagogiques : ▪ Évaluation des besoins et du profil du participant ▪ Apport théorique et méthodologique : séquences pédagogiques regroupées en différents modules ▪ Contenus des programmes adaptés en fonction des besoins identifiés pendant la formation ▪ Réflexion et échanges sur cas pratiques ▪ Questionnaires, exercices, ateliers et étude de cas ▪ Tests de contrôle de connaissances et validation des acquis à chaque étape ▪ Retours d'expériences Éléments matériels : ▪ Mise à disposition de tout le matériel pédagogique nécessaire (pour les formations en présentiel) ▪ Support de cours au format numérique projeté sur écran et transmis au participant par mail à la fin de la formation Référent pédagogique et formateur/formatrice : Chaque formation est sous la responsabilité de la directrice pédagogique de l'organisme de formation ; le bon déroulement est assuré par le formateur ou la formatrice désigné(e) par l'organisme de formation.