Mise à jour : 01/03/2026

FORMATION : Référent Cybersécurité PME

PUBLIC	Cette formation est à destination des dirigeants de PME/ETI, DSI, responsables informatiques, futurs référents cybersécurité, chefs de projet IT.
PRÉREQUIS ET MATERIEL RÉQUIS	Prérequis : ▪ Connaissances générales en informatique. ▪ Aucune expertise technique approfondie requise. Matériel requis : ▪ Ordinateur portable avec accès Internet, accès administrateur pour les ateliers. ▪ Accès au système d'information (SI) de l'organisation (optionnel mais recommandé 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 : ▪ Évaluer le niveau de cybersécurité de son organisation et identifier les risques majeurs ▪ Mettre en œuvre les mesures de protection techniques et organisationnelles adaptées aux PME ▪ Gérer les incidents de sécurité, de la détection à la reprise d'activité ▪ Assurer la conformité réglementaire (NIS2, RGPD) et préparer les contrôles ▪ Sensibiliser les collaborateurs et développer une culture de la cybersécurité ▪ Piloter la cybersécurité dans la durée : budget, indicateurs, amélioration continue
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	**Panorama des Menaces et Enjeux pour les PME (2h)** 1. Le paysage cyber 2025 2. Pourquoi les PME sont ciblées 3. Les menaces principales 4. Anatomie d'une cyberattaque 5. Conséquences concrètes Étude de cas : Analyse d'un cas réel de ransomware ayant touché une PME industrielle.
	MODULE 2	**Cadre Réglementaire : NIS2, RGPD et Obligations (1h30)** 1. NIS2 pour les PME 2. RGPD et données personnelles 3. Autres obligations 4. Responsabilité du dirigeant Autodiagnostic : « Mon organisation est-elle concernée par NIS2 ? »
	MODULE 3	**Diagnostic de Sécurité : Évaluer sa PME (2h)** 1. Guide d'hygiène ANSSI 2. Cartographie du SI 3. Grille de diagnostic PME 4. Score de maturité Atelier : Chaque participant réalise le diagnostic complet de son organisation.
	MODULE 4	**Analyse de Risques Simplifiée pour PME (1h30)** 1. Méthodologie adaptée PME 2. Identification des actifs critiques 3. Scénarios de menaces 4. Évaluation et traitement Atelier : Réaliser l'analyse de risques simplifiée de sa propre PME.
	MODULE 5	**Sécurité Technique : les Fondamentaux (2h30)** 1. Sécurité réseau 2. Sécurité des postes 3. Sécurité des serveurs 4. Sécurité de la messagerie 5. Mises à jour et patch management Atelier : Vérification en live : tester SPF/DKIM/DMARC de son domaine, scanner la surface externe avec Shodan, vérifier les mises à jour en attente.
	MODULE 6	**Sécurité du Cloud et de la Mobilité (1h)** 1. Sécurité Microsoft 365 / Google Workspace 2. Sécurité des applications SaaS 3. Sécurité mobile et télétravail Atelier : Vérifier le Secure Score de son tenant M365 & identifier les quick wins.
	MODULE 7	**Gestion des Accès et des Identités (1h30)** 1. Politique de mots de passe 2. Authentification multi-facteurs (MFA) 3. Gestion des comptes 4. Revue des accès Atelier : Audit AD rapide avec PingCastle (ou équivalent cloud) : score, comptes inactifs, comptes admin, MFA coverage.

	MODULE 8	**Protection des Données et Sauvegardes (1h)** 1. Classification des données 2. Stratégie de sauvegarde 3. Tests de restauration 4. Chiffrement Atelier : Vérifier sa stratégie de sauvegarde actuelle vs règle 3-2-1-1-0, identifier les écarts, planifier un test de restauration.
	MODULE 9	**Sécurité des Fournisseurs et Sous-traitants (1h)** 1. Risques liés aux fournisseurs 2. Évaluation des fournisseurs 3. Clauses contractuelles 4. Gestion des accès tiers Atelier : Lister ses 5 fournisseurs les plus critiques, les évaluer et identifier les actions.
	MODULE 10	**Détection et Réponse aux Incidents (2h)** 1. Détection pour les PME 2. Qualification d'un incident 3. Fiches réflexes 4. Premières actions de réponse 5. Post-incident Atelier : Scénario : ransomware sur le serveur de fichiers. Les participants déroulent la fiche réflexe, prennent les décisions, rédigent le journal de bord.
	MODULE 11	**Gestion de Crise et Continuité d'Activité (1h30)** 1. PCA/PRA adapté PME 2. Mode dégradé 3. Cellule de crise PME 4. Communication de crise 5. Contacts d'urgence Atelier : Rédiger sa fiche de contacts d'urgence + son plan de communication de crise.
	MODULE 12	**Sensibilisation et Facteur Humain (1h30)** 1. Le facteur humain 2. Programme de sensibilisation PME 3. Campagnes de phishing simulé 4. Charte informatique 5. Formation des dirigeants Atelier : Concevoir le plan de sensibilisation annuel de sa PME (calendrier 12 mois, canaux, budget, KPI).
	MODULE 13	**Politiques de Sécurité et Documentation (1h)** 1. Documents indispensables pour une PME 2. Modèles prêts à l'emploi 3. Gestion documentaire Atelier : Compléter le template de PSSI PME avec les informations de son organisation.
	MODULE 14	**Notification et Obligations Déclaratives (1h)** 1. Notification NIS2 2. Notification RGPD 3. Dépôt de plainte 4. Assurance cyber Atelier : Remplir le formulaire d'alerte précoce NIS2 sur un scénario fictif.

	MODULE 15	**Budget, Indicateurs et Pilotage de la Cybersécurité (1h30)** 1. Budget cybersécurité PME 2. Indicateurs essentiels 3. Tableau de bord direction 4. Présenter la cybersécurité au dirigeant 5. Amélioration continue Atelier : Construire son tableau de bord cyber trimestriel à partir du diagnostic du Jour 1.
	MODULE 16	**Plan d'Action et Feuille de Route Personnalisée (2h)** 1. Synthèse des écarts 2. Méthodologie du plan d'action 3. Roadmap 12 mois Atelier : Chaque participant construit sa feuille de route personnalisée : 15 actions priorisées, 10 quicks wins, roadmap 12 mois, estimation budget, présentation 1 page pour le dirigeant.
	MODULE 17	**Simulation de Crise et Exercice Immersif (2h)** Scénario – « Opération Vendredi Noir » Les participants jouent le rôle de la cellule de crise d'une PME de 120 salariés (négoce BtoB) victime d'un ransomware un vendredi à 17h.
	MODULE 18	**Évaluation Finale et Clôture (1h30)** 1. Récapitulatif des points clés 2. QCM final 3. Correction et échanges 4. Clôture
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.