

FORMATION : Risques Psychosociaux en Cybersécurité : Prévenir, Identifier et Agir

PUBLIC	Cette formation est à destination des : ▪ Professionnels de la cybersécurité ▪ Analystes SOC ▪ Administrateurs systèmes et réseaux ▪ RSSI ▪ Responsables informatiques ▪ Managers d'équipes IT et cybersécurité ▪ Responsables RH impliqués dans la prévention des RPS
PRÉREQUIS	<u>Prérequis :</u> ▪ Aucun prérequis technique spécifique. ▪ Une connaissance générale de l'environnement informatique et des métiers du numérique est recommandée.
MODALITÉS ET DÉLAIS D'ACCÈS	<u>En présentiel :</u> ⇒ Formation en présentiel : lieu de formation communiqué en amont de la formation. ⇒ Inscription à réaliser 1 mois avant le démarrage de la formation. <u>En distanciel :</u> ⇒ Formation individuelle ou collective à distance sous la forme de visioconférence participative. ⇒ Inscription à réaliser 1 mois avant le démarrage de la formation.
DURÉE	14H pour une période de 2 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	<u>En présentiel :</u> ⇒ Sur site ⇒ Au siège de Tricolor Expertise ⇒ Autre adresse <u>En distanciel :</u> ⇒ Formation à distance – visioconférence Pour les personnes en situation de handicap : Nous adaptons nos formations en fonction de votre handicap et nous mettons tout en œuvre pour vous accueillir ou pour vous réorienter si besoin. Vous pouvez nous contacter au 06 34 31 28 65
TARIF	1650€ par personne
NOMBRE DE PARTICIPANTS	<u>En présentiel :</u> Jusqu'à 12 personnes <u>En distanciel :</u> 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 : ▪ Définir les risques psychosociaux et leurs conséquences. ▪ Identifier les facteurs de risques spécifiques aux métiers de la cybersécurité. ▪ Repérer les signaux faibles de stress chronique, de surcharge mentale et d'épuisement professionnel. ▪ Comprendre les mécanismes psychologiques liés à la gestion des incidents et des crises cyber. ▪ Mettre en œuvre des actions de prévention individuelles et collectives. ▪ Participer à la construction d'un environnement de travail favorisant la résilience et la performance durable.

**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	Comprendre les risques psychosociaux en cybersécurité <u>Objectifs</u> ▪ Définir les RPS. ▪ Identifier les enjeux humains de la cybersécurité. <u>Contenus</u> ▪ Définition des risques psychosociaux. ▪ Cadre réglementaire et responsabilité de l'employeur. ▪ Les différentes formes de RPS : ○ stress professionnel ; ○ surcharge mentale ; ○ épuisement professionnel ; ○ conflits de valeurs ; ○ isolement professionnel. ▪ Les spécificités du secteur cyber : ○ vigilance permanente ; ○ gestion de l'urgence ; ○ pression liée aux incidents ; ○ responsabilité organisationnelle. <u>Activité pédagogique</u> Étude de situations réelles issues du secteur numérique.
MODULE 2	Les mécanismes psychologiques <u>Objectifs</u> ▪ Comprendre les réactions du cerveau face au stress. <u>Contenus</u> ▪ Fonctionnement du stress aigu et chronique. ▪ Hypervigilance et fatigue cognitive. ▪ Fatigue décisionnelle. ▪ Syndrome de l'imposteur dans les métiers techniques. ▪ Problèmes éthiques ▪ Impacts physiologiques et psychologiques de la pression continue. <u>Activité pédagogique</u> Analyse collective de cas pratiques.
MODULE 3	Détecter les signaux d'alerte <u>Objectifs</u> ▪ Repérer les indicateurs individuels et collectifs. <u>Contenus</u> ▪ Signaux physiques : ○ fatigue ; ○ troubles du sommeil ; ○ tensions corporelles. ▪ Signaux émotionnels : ○ irritabilité ; ○ anxiété ; ○ perte de motivation. ▪ Signaux organisationnels : ○ absentéisme ; ○ turnover ;

		○ erreurs récurrentes ; ○ baisse de performance. <u>Activité pédagogique</u> Autodiagnostic et échanges d'expériences.
	MODULE 4	Prévenir les risques psychosociaux <u>Objectifs</u> ▪ Développer des pratiques favorisant la santé mentale au travail. <u>Contenus</u> ▪ Gestion de la charge mentale. ▪ Priorisation et organisation du travail. ▪ Gestion de l'attention et des interruptions. ▪ Importance de la récupération et de la déconnexion. ▪ Prévention collective : ○ rotation des missions ; ○ débriefing post-incident ; ○ coopération au sein des équipes. <u>Activité pédagogique</u> Construction d'un plan d'action individuel.
	MODULE 5	Gestion de crise et facteurs humains <u>Objectifs</u> ▪ Comprendre l'impact psychologique des incidents de sécurité. <u>Contenus</u> ▪ Fonctionnement des équipes en situation de crise. ▪ Gestion émotionnelle lors d'un incident cyber. ▪ Communication sous pression. ▪ Retour d'expérience et apprentissage organisationnel. <u>Activité pédagogique</u> Simulation d'incident cyber avec prise de décision collective.
	MODULE 6	Développer la résilience individuelle et collective <u>Objectifs</u> ▪ Renforcer les capacités d'adaptation des professionnels. <u>Contenus</u> ▪ Définition de la résilience. ▪ Facteurs de protection psychologique. ▪ Ressources individuelles et collectives. ▪ Intelligence émotionnelle et gestion des émotions. ▪ Préservation de la performance durable. <u>Activité pédagogique</u> Élaboration d'un plan de résilience professionnelle.
	MODULE 7	Construire une culture de prévention <u>Objectifs</u> ▪ Favoriser une démarche durable de prévention. <u>Contenus</u> ▪ Rôle des managers. ▪ Rôle des équipes RH. ▪ Culture du feedback et du droit à l'erreur. ▪ Mise en place d'indicateurs de suivi. ▪ Bonnes pratiques organisationnelles. <u>Activité pédagogique</u> Atelier collaboratif de construction d'actions de prévention.
MOYENS PERMETTANT LE SUIVI ET L'APPRÉCIATION DES RÉSULTATS		<u>Suivi de l'exécution :</u> ⇒ 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.

	<u>Appréciation des résultats :</u> ▪ 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	<u>Modalités pédagogiques :</u> ▪ 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 <u>Éléments matériels :</u> ▪ 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 <u>Référent pédagogique et formateur/formatrice :</u> 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.