Mise à jour : 01/06/2026

FORMATION : Gestion de crise cybersécurité

PUBLIC	Cette formation est à destination des RSSI, responsable informatique, manager IT, membre des cellules de crise, chef de projet cybersécurité, dirigeant de PME/ETI impliqué dans la gestion d'incidents.
PRÉREQUIS	Prérequis : ▪ Connaissances générales en cybersécurité et en gestion des risques informatiques.
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	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	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	1650€ 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 mécanismes humains et organisationnels en situation de crise cyber. ▪ Prioriser les actions critiques lors d'un incident majeur. ▪ Coordonner efficacement les différents acteurs internes et externes. ▪ Communiquer de manière claire et adaptée sous pression. ▪ Prendre des décisions dans un contexte d'incertitude. ▪ Préparer et animer une cellule de crise. ▪ Construire un dispositif de gestion de crise adapté à leur organisation. ▪ Capitaliser sur les retours d'expérience afin d'améliorer la résilience de l'entreprise.
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 la crise cyber et ses impacts** Objectifs spécifiques • Identifier les caractéristiques d'une crise cyber. • Comprendre les conséquences techniques, humaines, financières et réputationnelles. Contenu **Qu'est-ce qu'une crise cyber ?** • Incident de sécurité versus situation de crise. • Critères de bascule vers une crise. • Typologie des incidents majeurs : o ransomware ; o fuite de données ; o compromission de comptes ; o attaque par déni de service ; o indisponibilité des systèmes critiques. **Les effets d'une crise sur l'organisation** • Stress et surcharge cognitive. • Désorganisation des équipes. • Pression médiatique et managériale. • Impacts juridiques et réglementaires. • Atteinte à l'image de marque. Atelier • Analyse collective d'un cas réel de crise cyber.
	MODULE 2	**Prioriser et décider en situation dégradée** Objectifs spécifiques • Développer sa capacité de décision sous pression. • Identifier les priorités opérationnelles. Contenu **Les mécanismes psychologiques sous stress** • Fonctionnement du cerveau en situation d'urgence. • Biais cognitifs fréquents. • Risques de précipitation ou d'inaction. **Les principes de priorisation** • Évaluer rapidement la situation. • Distinguer urgence et importance. • Déterminer les actifs critiques. **Les premières mesures de protection** • Isolement des systèmes compromis. • Protection des sauvegardes. • Maintien des activités essentielles. • Mise en place des mesures conservatoires. **Les décisions à différer** • Éviter les actions irréversibles. • Gérer l'incertitude. • Conserver des éléments de preuve. Exercices • Mises en situation chronométrées de prise de décision.
	MODULE 3	**Piloter et coordonner une cellule de crise** Objectifs spécifiques • Structurer la gouvernance de crise. • Organiser la coordination entre les parties prenantes. Contenu **Organisation d'une cellule de crise** • Composition et rôles. • Répartition des responsabilités. • Circuit de validation des décisions.

		Coordination des acteurs internes • Équipes systèmes et réseaux. • Équipes applicatives. • Direction générale. • Ressources humaines. • Communication interne et externe. • Services juridiques. **Coordination des acteurs externes** • Prestataires techniques. • Experts en réponse à incident. • Assureurs cyber. • Autorités compétentes. • Forces de l'ordre si nécessaire. **Outils de pilotage** • Main courante. • Journal des décisions. • Tableau de suivi des actions. • Indicateurs de situation. Atelier • Construction d'une organisation de crise adaptée à son entreprise.
	MODULE 4	**Communiquer efficacement pendant une crise** Objectifs spécifiques • Adapter sa communication aux différents publics. • Maintenir la confiance malgré l'incertitude. Contenu **Principes fondamentaux de la communication de crise** • Transparence maîtrisée. • Communication factuelle. • Gestion des rumeurs. • Cohérence des messages. **Communication interne** • Informer les collaborateurs. • Prévenir la panique. • Donner des consignes claires. **Communication externe** • Clients. • Fournisseurs. • Partenaires. • Médias. **Les erreurs à éviter** • Minimiser ou dramatiser la situation. • Faire des promesses irréalistes. • Communiquer sans validation. Jeux de rôle • Simulation de conférence de crise et points de situation.
	MODULE 5	**Leadership et posture du responsable cybersécurité** Objectifs spécifiques • Développer une posture rassurante et efficace. • Renforcer ses compétences relationnelles en contexte de tension. Contenu **Le rôle du leader en situation de crise** • Garder une vision globale. • Maintenir le cap stratégique. • Faciliter la coopération. **Intelligence émotionnelle** • Gestion du stress. • Régulation émotionnelle. • Gestion des conflits.

		Posture managériale • Rassurer sans masquer les difficultés. • Encourager les équipes. • Préserver la dynamique collective. Exercices • Auto-évaluation et entraînement aux situations difficiles.
	MODULE 6	**Préparer la gestion de crise avant qu'elle n'arrive** Objectifs spécifiques • Construire un dispositif de préparation efficace. • Renforcer la résilience organisationnelle. Contenu **Élaboration d'un plan de gestion de crise** • Gouvernance. • Procédures. • Escalade. • Continuité d'activité. **Les fiches réflexes** • Structure. • Utilisation. • Mise à jour. **Les scénarios de crise** • Construction des scénarios. • Niveau de gravité. • Exercices progressifs. **Les exercices de simulation** • Simulation immersive. • Retour d'expérience. Atelier • Création d'une fiche réflexe de gestion de crise cyber.
	MODULE 7	**Retour d'expérience et amélioration continue** Objectifs spécifiques • Capitaliser sur les enseignements d'une crise. • Mettre en place une démarche d'amélioration continue. Contenu **Organiser un RETEX efficace** • Collecte des faits. • Analyse des décisions. • Identification des points forts et axes d'amélioration. **Transformation des enseignements en actions** • Mise à jour des procédures. • Renforcement des compétences. • Ajustement des outils. **Développer une culture de résilience** • Sensibilisation continue. • Exercices réguliers. • Partage d'expérience. Cas pratique final • Simulation complète d'une attaque par ransomware impliquant direction, communication, juridique et équipes techniques.
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	<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>Livrables remis aux participants</u> ▪ Support pédagogique complet. ▪ Modèle de plan de gestion de crise. ▪ Modèles de fiches réflexes. ▪ Check-list de communication de crise. ▪ Trame de retour d'expérience (RETEX). ▪ Boîte à outils du responsable cybersécurité en situation de crise. <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.