MAJ 04/11/2025

Formation « Gestion de crise cyber »

Réf : SECUCRISE

Les méthodes proactives demeurent limitées et tout un chacun est confronté un jour à une crise due à des incidents informatiques ou un problème de sécurité. Il faut donc maîtriser cette réaction d'urgence et savoir y faire face.

Objectifs

- Apprendre à mettre en place une organisation adaptée pour répondre efficacement aux situations de crise
- Apprendre à élaborer une communication cohérente en période de crise
- Apprendre à éviter les pièges induits par les situations de crise
- Tester votre gestion de crise SSI.

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Directeur ou responsable des systèmes d'information
- Responsable de la sécurité des systèmes d'information
- Responsable de la gestion de crise
- Responsable des astreintes
- Responsable de la gestion des incidents

Pré-requis

- Cette formation ne demande pas de pré-requis particuliers.

Méthode pédagogique

- Cours magistral avec des exemples basés sur le retour d'expérience des formateurs.

Supports

- Support de cours en français au format papier en présentiel et au format numérique en distanciel
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration
- Evaluation de pré-formation envoyée avant le début de la formation
- Evaluation de mi-formation effectuée en session par le formateur au moyen d'exercices pratiques

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 2h00 en français. L'examen est constitué d'une partie QCM et d'une partie rédactionnelle sous forme d'étude de cas**

Programme

Module 1 : Gestion de crise d'origine cyber

- Exemples de crises d'origine cyber
- Cas concret détaillé d'une crise « rançongiciel »
- Pourquoi est-ce la principale crainte des organisations ?
- État du SI et de l'organisation après un rançongiciel
- Chronologie classique d'une gestion de crise : attaque, constat, réaction, suivi et sortie de crise

Module 2 : Dispositif de crise et spécificités d'une cyber-attaque

- Spécificités d'une crise cyber
- Qu'est-ce qu'un dispositif de gestion de crise ?
- Organisations types
- Processus obligatoires : montée en crise, lancement, points de situation, sortie de crise
- Outillage et corpus documentaire
- Logistique de crise et cyber-assurance
- Mise en situation

Module 3 : Gestion de crise et enjeux réglementaires

- Enjeux de la gestion de crise dans un contexte réglementaire : DORA, NIS2, LOPMI, etc.
- Obligations : dispositif, entraînement, résilience
- Focus sur la notification : quand, à qui, comment, pourquoi
- Mise en situation

Module 4 : Communication en situation de crise

- Communication interne et externe
- Relation avec les autorités, partenaires et parties prenantes
- Bonnes pratiques de communication en temps de crise
- Gestion de la communication sous pression médiatique
- Étude de cas et mise en situation

Module 5 : Observation & Investigation – Comprendre pour agir

- Plan d'investigation : vecteurs d'intrusion, propagation, persistance
- Responsabilités et posture d'observation (discrète / non discrète)
- Actions clefs et outillage de l'investigation
- Interactions inter et intra cellules de crise
- Mise en situation

Module 6 : Défense & Surveillance – Contenir et remédier

- Composition et responsabilités du plan de défense
- Actions clefs : assainissement, reconstruction, durcissement, surveillance
- Remédiation et reconstruction sécurisée
- Surveillance circonstancielle et long terme
- Mise en situation

Module 7 : Le facteur humain en situation de crise

- Contexte lié à la crise et effets sur les individus
- Comportements adaptés et inadaptés
- Principaux biais cognitifs
- Bonnes pratiques pour réduire le stress et favoriser la coopération

Module 8 : Sortie de crise & post-crise

- Critères de sortie de crise
- Analyse post-mortem et RCA (« root cause analysis »)
- Construction du RETEX et plan d'actions post-crise
- Retour en mode projet et en « RUN »
- Exercices de crise : enjeux, conception, animation, évaluation
- Mise en situation : construction d'un plan post-crise, RETEX

Module 9 : Entraînement & Exercice

- Construire un plan d'entraînement
- S'exercer à la gestion de crise
- Evaluer son dispositif de gestion de crise
- Mise en situation

Module 10 : Mise en situation globale

- Exercice de crise grandeur nature (matinée jour 2) : simulation, décisions stratégiques et opérationnelles, débriefing

Examen de certification

- Examen final (Jour 3 après-midi, 2h) : étude de cas + QCM