DAWAN

Plan de la formation

www.dawan.fr

Formation Gérer une cyber-crise : Les fondamentaux

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	1 575,00 € HT (standard) 1 260,00 € HT (remisé)
Public :	Responsable du Plan de Continuité Informatique et de la gestion des crises du SI - Responsable de la Sécurité du Système d'Information (RSSI) - Manager d'équipe en charge de gérer une cybercrise - Gestionnaires d'incidents et de problèmes - Responsable du Plan de Continuité d'Activité (RPCA) et de la gestion de crise - Dirigeant d'un organisme, membres ou non de la cellule de crise - Directeur des risques - Directeur et manager ayant à gérer des crises, y compris cyber
Pré-requis :	Connaître le fonctionnement général du système d'information de l'organisme et avoir une première expérience de gestion de crise, d'incident ou de continuité d'activité
Objectifs :	Présenter l'environnement des cybermenaces et les risques de cyber-crise - Rappeler les bases de la gestion de crise et de la continuité d'activité - Réaliser le lien entre la gestion d'une cyberattaque et la gestion de crise « classique »- Anticiper la cyber-crise par la mise en œuvre d'un dispositif organisationnel et technique efficace - Prendre de la hauteur et se positionner comme gestionnaire d'une crise cyber- Donner les clés de la gestion d'une cyber-crise, de l'alerte jusqu'au bilan - Permettre aux participants de se mettre en situation grâce à un exercice de gestion d'une cyber-crise
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalités d’évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102745-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre le contexte et les enjeux d’une cyber-crise

Situer la cyber-crise parmi les différents types de crises que peut rencontrer une organisation
Identifier les grandes familles de cybermenaces susceptibles de déclencher une crise : ransomware, fuite massive de données, indisponibilité prolongée du SI, fraude
Mesurer les impacts potentiels : indisponibilité des services, pertes financières, enjeux réglementaires, atteinte à l’image et à la confiance
Relier la cyber-crise aux enjeux de gouvernance, de communication et de responsabilité de la direction
Atelier fil rouge : analyser un ou deux exemples de cyber-crises médiatisées et en tirer les principaux enseignements de gouvernance et de gestion

Rappeler les bases de la gestion de crise et de la continuité d’activité

Revenir sur les notions clés : incident majeur, crise, cellule de crise, PCA, PRA, plans de secours
Clarifier les rôles et responsabilités en situation de crise : direction générale, DSI, RSSI,

métiers, communication, juridique, RH
Distinguer gestion opérationnelle de l'incident et pilotage stratégique de la crise
Comprendre l'articulation entre continuité d'activité, reprise informatique et gestion des parties prenantes internes et externes
Atelier fil rouge : cartographier la gestion de crise existante dans son organisation (forces, faiblesses, zones floues)

Relier gestion de cyberattaque et gestion de crise

Identifier ce qui différencie une cyberattaque d'un incident technique « classique » (incertitude, temporalité, adversaire, médiatisation potentielle)
Comprendre comment un incident cyber se transforme en crise (seuils de bascule, critères, déclenchement de la cellule de crise)
Articuler les équipes techniques (SOC, équipes d'exploitation, prestataires) avec la cellule de crise et la direction
Mettre en cohérence les plans techniques (PRA, plans de secours) avec les plans de crise et de communication
Atelier fil rouge : à partir d'un scénario d'attaque, identifier le moment où l'on doit basculer en mode crise et alerter la gouvernance

Anticiper une cyber-crise : préparer les acteurs, les processus et les outils

Définir un dispositif de préparation à la cyber-crise : rôles, circuits d'alerte, documentation, outils
Identifier les prérequis techniques et organisationnels : inventaires, cartographies, plans, contacts clés, procédures succinctes
Préparer les supports pour le pilotage de crise : fiches réflexes, grilles de décision, tableaux de bord, modèles de messages
Prévoir la coordination avec les prestataires externes, assureurs cyber, autorités, partenaires stratégiques
Atelier fil rouge : élaborer une fiche réflexe « cyber-crise » simple et opérationnelle pour son organisation

Gérer une cyber-crise : de l'alerte à la stabilisation

Structurer les premières heures : détection, qualification, escalade, déclenchement de la cellule de crise
Organiser le travail de la cellule de crise : rythme des réunions, répartition des rôles, prise de décision, traçabilité
Piloter les axes clés : diagnostic technique, continuité des activités, communication interne et externe, relation clients et partenaires

Gérer le temps long : stabilisation, reprise progressive, gestion de la fatigue et du stress des équipes
Atelier fil rouge : simuler les premières heures d'une cyber-crise en définissant les décisions à prendre et les informations à faire remonter

Coordonner gestion des incidents, des problèmes et enquête post-incident

Clarifier la différence entre gestion des incidents, des problèmes et gestion de crise
Organiser la collecte des faits, des preuves et des éléments techniques nécessaires à l'enquête
S'appuyer sur les processus existants ITIL ou internes : gestion d'incidents, problèmes, changements, vulnérabilités
Préparer le retour d'expérience (RETEX) technique, organisationnel et managérial
Atelier fil rouge : construire une trame de compte rendu de crise cyber à l'usage de la direction et des autorités si besoin

Conduire la communication en situation de cyber-crise

Identifier les parties prenantes : collaborateurs, clients, partenaires, autorités, médias, réseaux sociaux
Définir les principes d'une communication de crise efficace : transparence mesurée, cohérence, régularité, maîtrise des messages
Articuler communication de crise et obligations légales (notifications, régulateurs, CNIL, etc.)
Gérer les rumeurs, les fuites d'information et l'exposition médiatique
Atelier fil rouge : rédiger un message interne et un message externe adaptés à un scénario de cyber-crise

Se mettre en situation : exercice de gestion d'une cyber-crise

Participer à un exercice fil rouge de gestion de cyber-crise (type jeu de rôle ou exercice sur table)
Vivre les différentes phases : alerte, montée en charge, décisions clés, communication, stabilisation
Expérimenter la coordination entre cellule de crise, équipes techniques et métiers
Identifier les points forts et les axes d'amélioration de sa posture de gestionnaire de crise
Atelier fil rouge : exercice de gestion de crise cyber, avec débriefing collectif sur les décisions prises et les leviers d'amélioration

Capitaliser et prendre de la hauteur pour mieux se positionner

Synthétiser les bonnes pratiques de préparation et de gestion d’une cyber-crise
Clarifier son propre rôle et ses responsabilités dans une future situation de crise cyber
Identifier les actions prioritaires à mettre en œuvre à l’issue de la formation (documentation, organisation, exercices, sensibilisations)
Construire une première feuille de route « gestion de cyber-crise » adaptée à son contexte

Atelier fil rouge final : formaliser un mini plan d’actions personnel et organisationnel pour renforcer la gestion des cyber-crises