DAWAN

Plan de la formation

www.dawan.fr

Formation Réponse à incident et analyse forensique – Niveau expert opérationnel

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 975,00 CHF HT (standard) 3 180,00 CHF HT (remisé)
Public :	Consultants en sécurité, membres de SOC ou d'équipes "blue team" - Administrateurs systèmes / réseaux impliqués dans la gestion d'incidents-- RSSI, responsables sécurité opérationnelle, responsables CERT / CSIRT
Pré-requis :	Bonne compréhension générale des architectures systèmes et réseaux - Première expérience de la sécurité opérationnelle (gestion d'incident, supervision, journaux) souhaitable
Objectifs :	Comprendre les principes, enjeux et étapes de la réponse à incident de sécurité - Acquérir les bases méthodologiques de l'analyse forensique sur systèmes et journaux (dans un cadre légal et maîtrisé) - Savoir organiser la collecte, la préservation et l'analyse des preuves numériques lors d'un incident - Être en mesure de contribuer efficacement à la gestion d'un incident majeur et au retour d'expérience
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 :	CYB102750-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 cadre et les enjeux de la réponse à incident

Définir ce qu’est un incident de sécurité, une alerte, un faux positif, un incident majeur
Comprendre les enjeux techniques, organisationnels, juridiques et d’image liés à la gestion d’incidents
Positionner la réponse à incident dans la démarche globale de cybersécurité (SOC, gouvernance, PCA/PRA, gestion de crise)
Identifier les acteurs clés : SOC, équipes techniques, RSSI, direction, juridique, communication, prestataires
Atelier fil rouge : analyser un exemple d’incident médiatisé et reconstituer rapidement les grandes étapes de la réponse

Structurer un processus de réponse à incident

Découvrir les principales étapes : préparation, détection, analyse, confinement, éradication, reprise, retour d’expérience
Définir les critères de criticité et les niveaux d’escalade
Articuler les procédures de réponse à incident avec les outils existants (tickets,

supervision, logs, communication)
Documenter le processus pour qu'il soit utilisable par les équipes opérationnelles
Atelier fil rouge : construire un schéma simple de processus de réponse à incident adapté à son organisation

Collecter et préserver les preuves numériques

Comprendre la notion de preuve numérique et d'intégrité des éléments collectés
Identifier les sources de preuves : journaux systèmes, réseaux, applicatifs, sauvegardes, configurations, artefacts sur postes et serveurs
Mettre en place des pratiques de collecte structurées pour limiter la dégradation des preuves
Préparer les éléments nécessaires à une éventuelle enquête interne, assurance ou action en justice
Atelier fil rouge : élaborer une checklist de collecte d'éléments pour différents types d'incidents

Analyser les journaux et artefacts pour comprendre l'incident

Découvrir les principes de base de l'analyse forensique sur systèmes et journaux, dans un contexte pédagogique
Identifier les traces typiques d'attaques : connexions suspectes, élévation de privilèges, modifications de comptes, exécutions inhabituelles
Relier les observations à une chronologie des événements pour reconstituer le déroulé de l'incident
Articuler cette analyse avec les informations provenant des outils de sécurité (EDR, SIEM, IDS/IPS)
Atelier fil rouge : à partir d'un jeu de journaux simplifiés, reconstituer une timeline résumant l'incident

Contribuer au confinement, à l'éradication et à la reprise

Identifier les options de confinement : isolement de machines, restrictions d'accès, désactivation de comptes
Comprendre les risques liés à un confinement mal maîtrisé (perte de traces, réactions de l'attaquant, impacts métiers)
Participer à l'éradication : suppression de composants malveillants, corrections, durcissement, restaurations ciblées
Préparer et accompagner les phases de reprise en service en limitant les risques de rechute
Atelier fil rouge : travailler sur un scénario d'incident et proposer des

mesures de confinement et d’éradication réalistes

Documenter l’incident et contribuer au retour d’expérience

Structurer le compte rendu d’incident : contexte, détection, chronologie, impacts, actions menées, décisions, preuves disponibles
Adapter les rapports aux différents publics : technique, RSSI, direction, assurance, autorités si nécessaire
Organiser le retour d’expérience (RETEX) pour tirer des enseignements concrets et prioriser les améliorations
Relier ces enseignements à la mise à jour des procédures, des configurations et de la sensibilisation
Atelier fil rouge : rédiger un modèle de compte rendu d’incident et un modèle de synthèse pour la direction

Mettre en place une capacité de réponse à incident opérationnelle

Identifier les prérequis organisationnels et techniques : référentiels, outils, compétences, astreintes, partenaires externes
Définir les rôles au sein d’une équipe de réponse à incident (CSIRT/CERT interne ou externe)
Articuler cette capacité avec la gestion de crise de l’organisation et les assureurs cybersécurité
Prévoir des exercices réguliers de simulation d’incidents pour tester et améliorer le dispositif
Atelier fil rouge : définir une feuille de route pour renforcer la capacité de réponse à incident de son organisation

Construire son plan de progression en forensique et réponse à incident

Identifier les domaines techniques à approfondir : systèmes, réseaux, applicatifs, outils forensiques, EDR, SIEM
Repérer les ressources, formations et communautés pertinentes pour continuer à progresser
Définir un plan d’action individuel et/ou d’équipe sur 6 à 12 mois (outils à mettre en place, pratiques à standardiser, exercices à mener)
Ancrer la réponse à incident et la forensique dans une démarche d’amélioration continue de la sécurité globale
Atelier fil rouge final : formaliser un plan de progression personnel autour de la réponse à incident et de l’analyse forensique