Rétablir la confiance après une attaque

CYBERSÉCURITÉ

Objectifs	Savoir piloter la reprise d'activité de manière structurée et sécurisée après une cyberattaque - Réinstaurer la confiance auprès des parties prenantes : internes, clients, partenaires, autorités - Mettre en oeuvre un audit post-incident rigoureux pour corriger les failles et documenter les actions - Préparer les futures crises par une boucle d'amélioration continue.
Participants	RSSI - DSI - responsables communication - gestionnaires de crise - consultants cybersécurité - responsables qualité / conformité - administrateurs systèmes - juristes SSI - chefs de projet cyber - étudiants en sécurité informatique avancée.
Prérequis	Compétences en gestion de crise - communication de crise - analyse d'impact - restauration technique (systèmes, données) - gestion relationnelle avec clients/partenaires - posture empathique.
Moyens pédagogiques	1 poste par participant - 1 vidéoprojecteur - Support de cours fourni à chaque participant Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et évaluation des acquis tout au long de la formation
Méthodes pédagogiques	Exposés interactifs et démonstrations - Travaux pratiques individuels et en groupe - Échanges d'expériences et de bonnes pratiques
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	4150 € HT
Durée	5 jour(s) - 35 heure(s)
Modalités et délais d'accès	Formations accessibles sous 15 à 20 jours suite à votre demande. Un entretien initial doit être prévu avant votre entrée en formation.

Code : NCI_GX34KEVH

Mis à jour le : 25 mars 2026

Programme :

Stabilisation post-attaque & plan de reprise sécurisé

Phases post-incident : stabilisation, reprise, retour à la normale

Réinstallation des systèmes compromis : principes de confiance zéro

Sécurisation des sauvegardes, validation de l'intégrité, mesures d'urgence

Priorisation des services critiques, approche progressive de la reprise

Cas pratique

Étude d'un environnement compromis (VM sandboxée, logs compromis)

Élaboration d'un plan de reprise technique : étapes, prérequis, priorités

Vérification d'une restauration via hash et validation d'intégrité

Gestion de l'image et communication réparatrice

Communication après crise : posture, transparence, sincérité

Regagner la confiance des clients, collaborateurs et partenaires

Relations publiques post-incident : interviews, publications, communiqués

Cas pratique

Rédaction d'un plan de communication post-attaque (message d'excuse, engagement, plans d'action)

Préparation d'un discours officiel post-crise

Simulation de questions-réponses avec des journalistes / clients

Audit post-incident : technique, organisationnel, réglementaire

Objectifs de l'audit post-incident : compréhension, preuve, amélioration

Récupération et analyse des journaux, horodatages, artefacts

Approche technique (timeline, pivot, persistance)

Aspects réglementaires (CNIL, RGPD, notifications correctives)

Cas pratique

Analyse de logs d'incident (Windows, Linux, SIEM)

Création d'un rapport de timeline technique (TTP adverses, MITRE ATT&CK)

Rédaction d'un rapport d'audit synthétique pour comité exécutif

Plan d'action, durcissement et retour à l'opérationnel

Définition d'un plan d'actions correctives : technique, RH, processus

Renforcement des mesures de sécurité (MFA, EDR, segmentation, supervision)

MCO post-crise : gestion de l'obsolescence, redondance, surveillance accrue

Sensibilisation et formation renforcées post-incident

Cas pratique

Création d'un plan d'action détaillé sur base de l'audit

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon

Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille

www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20

Application d'un durcissement (CIS Benchmarks, Playbooks de réponse)

Simulation de relance d'un environnement sur base d'un environnement sécurisé reconstruit

Atelier final : gestion de post-crise complète

Mise en situation : entreprise fictive ayant subi une attaque majeure (ransomware + fuite de données)

Objectifs :

Reprendre l'activité critique en sécurité

Produire une communication interne/externe restauratrice

Mener un audit post-incident technique et organisationnel

Présenter un plan d'actions correctives crédible

Assurer le suivi avec un tableau de bord de résilience

Livrables attendus :

Plan de reprise (technique et métier)

Kit de communication post-incident

Rapport d'audit

Plan de durcissement et indicateurs de confiance

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20