Rôle du RSSI pendant une crise de Cyberattaque

CYBERSÉCURITÉ

Objectifs	Renforcer les compétences du RSSI dans la gestion de crise cyber - Apprendre à piloter la réponse technique et organisationnelle tout en assurant un reporting structuré vers la direction et les parties prenantes - Développer des réflexes de leadership, de coordination inter-équipes, et de communication stratégique pendant et après un incident.
Participants	RSSI - responsables sécurité - responsables IT - DSI - gestionnaires de crise cyber - coordinateurs SOC/CSIRT - chefs de projet cyber - consultants SSI - futurs RSSI
Prérequis	Compétences en gouvernance SSI - gestion des incidents - leadership - coordination interservices - compréhension technique des attaques - stratégie de communication interne/externe.
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_PIQPXQ24

Mis à jour le : 25 mars 2026

Programme :

Préparer le RSSI à la gestion de crise

Rôle et posture du RSSI avant, pendant et après la crise

Cartographie des acteurs clés (DSI, COMEX, CERT, métiers, juridique, communication)

Organisation type d'une cellule de crise SSI

Principes de gestion de crise cyber (ISO 27035, ITIL, NIST CSF)

Cas pratique

Cartographie des responsabilités du RSSI dans un incident simulé

Constitution d'une cellule de crise avec répartition des rôles

Rédaction de fiches réflexes pour activation du RSSI en cas d'alerte

Pilotage opérationnel de la réponse

Coordination des équipes techniques (SOC, IR, infra, dev, cloud)

Gestion des priorités : containment, sauvegardes, analyses

Suivi des alertes, validation des IOC, pilotage de la remédiation

Communication interne avec des canaux résilients (hors IT compromis)

Cas pratique

Scénario de compromission : analyse de logs + pilotage des actions IR

Création d'un journal de crise temps réel (synthèse décisionnelle, actions, incidents)

Outil : tableau de bord RSSI (indicateurs clés, statut par domaine)

Leadership et prise de décision sous pression

Posture du RSSI en situation de stress : arbitrages, communication, autorité

Gestion des conflits de priorité entre IT, métiers, juridique

Interface avec le COMEX, reporting tactique et stratégique

Gestion psychologique d'équipe et fatigue décisionnelle

Cas pratique

Jeu de rôle : simulation d'une cellule de crise avec choix difficiles

Production d'un rapport de situation synthétique pour le COMEX

Débrief collectif : qualité du leadership, gestion du temps, posture

Reporting, obligations légales et communication sensible

Rédaction de rapports techniques (timeline, IOCs, MITRE ATT&CK)

Obligations réglementaires : CNIL, ANSSI, autorités judiciaires

Collaboration avec la cellule communication de crise

Documentation post-incident pour l'audit

Cas pratique

Rédaction d'un rapport d'incident technique complet

Préparation d'une communication consolidée (technique + métier)

Simulation de restitution devant un auditeur externe / DPO / COMEX

Atelier complet de gestion de crise pour RSSI

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

Rôle du RSSI pendant une crise de Cyberattaque

CYBERSÉCURITÉ

Scénario global : attaque complexe en environnement hybride (on-prem + cloud)

Compromission AD, ransomware, fuite de données client

Perturbation des services métiers essentiels

Objectifs de l'atelier :

Prise en main immédiate par le RSSI

Coordination de la cellule de crise interservices

Pilotage des mesures de confinement et remédiation

Reporting en temps réel et production de rapports intermédiaires

Communication stratégique avec direction, juridique, partenaires

Restitution finale avec évaluation collective

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