FICHE DE RÉVISION

Module : Organisation et Coordination des Réponses à Incidents

Formation : Pilotage et Animation de la Cybersécurité

1. Introduction à la Gestion de Crise Cyber

> **Objectif :** Comprendre les enjeux et les principes d'une réponse coordonnée à incident

Définitions fondamentales

Concept	Définition
Événement de sécurité	Occurrence identifiée d'un état d'un système, service ou réseau indiquant une possible violation de la politique de sécurité (ISO 27035)
Incident de sécurité	Un ou plusieurs événements indésirables ou inattendus ayant une probabilité significative de compromettre les activités métier et de menacer la sécurité de l'information
Crise cyber	Incident de sécurité d'ampleur majeure dépassant les capacités de réponse opérationnelle normale, nécessitant l'activation de la cellule de crise et une communication de crise
RETEX (Retour d'Expérience)	Analyse post-incident permettant d'identifier les causes racines, l'efficacité de la réponse et les actions correctives pour éviter la récurrence
MTTD — Mean Time To Detect	Délai moyen entre la survenance d'un incident et sa détection par les équipes de sécurité — objectif < 24h
MTTR — Mean Time To Respond/Recover	Délai moyen entre la détection d'un incident et sa résolution complète — objectif < 4h pour les incidents critiques

Classification des incidents de sécurité

Niveau	Criticité	Critères de classification	Délai de réponse	Exemple
P1	🔴 Critique	Impact sur la continuité d'activité, données sensibles exposées, systèmes critiques compromis	Immédiat — cellule de crise activée	Ransomware chiffrant le SI, compromission de l'Active Directory
P2	🟠 Majeur	Impact opérationnel significatif, périmètre limité, données internes exposées	< 4 heures	DDoS sur un service critique, accès non autorisé à des données RH
P3	🟡 Modéré	Impact limité, service dégradé, pas de fuite de données confirmée	< 24 heures	Infection malware isolée sur un poste, tentative d'intrusion bloquée
P4	🟢 Faible	Incident mineur, sans impact visible sur le métier ou les données	< 72 heures	Alerte antivirus sur fichier en quarantaine, scan de ports externe détecté

▸ Les enjeux d'une réponse coordonnée à incident

Enjeu	Explication et conséquences en cas de défaillance
Continuité d'activité	Un incident non maîtrisé rapidement peut paralyser le SI pendant des jours ou des semaines (ex. : NotPetya, 22 jours d'arrêt chez Maersk)
Protection des données	Chaque heure supplémentaire sans confinement augmente le volume de données exfiltrées ou chiffrées
Conformité réglementaire	Notification CNIL (72h RGPD), ANSSI (NIS2/LPM) : le non-respect des délais entraîne des sanctions additionnelles
Réputation et confiance	La communication de crise maîtrisée préserve la confiance des clients, partenaires et actionnaires
Responsabilité juridique	La démonstration d'une réponse diligente limite l'engagement de responsabilité civile et pénale des dirigeants
Préservation des preuves	Une réponse non coordonnée détruit souvent les traces numériques nécessaires à l'investigation et aux poursuites

▸ Le cycle de vie d'un incident — Phases clés (NIST SP 800-61)

Phase	Nom	Activités et objectifs
1	Préparation	Mettre en place les outils, procédures, équipes et entraînements avant tout incident — c'est la phase la plus déterminante
2	Détection & Analyse	Identifier, qualifier et classer l'incident ; collecter les premières preuves ; activer la procédure adaptée au niveau de criticité
3	Confinement	Stopper la propagation sans détruire les preuves : isolation réseau, révocation d'accès, coupure des flux suspects
4	Éradication	Supprimer la cause racine de l'incident : malware, backdoor, compte compromis, vulnérabilité exploitée
5	Reprise d'activité	Restaurer les systèmes et services affectés à partir de sauvegardes saines ; vérifier l'intégrité avant remise en production
6	RETEX & Amélioration	Analyser les causes, évaluer la réponse, mettre à jour les procédures, le PTR et la cartographie des risques

▸ Les 5 principes fondamentaux d'une réponse efficace

Principe	Description
1. Anticipation	Les procédures, les rôles et les outils sont définis AVANT l'incident — pas pendant la crise
2. Rapidité	Chaque minute compte : un confinement rapide limite drastiquement l'étendue des dommages
3. Coordination	La réponse implique plusieurs équipes et acteurs externes : une gouvernance claire évite le chaos
4. Préservation des preuves	Toutes les actions sont documentées et horodatées ; les logs et artefacts sont préservés pour l'investigation
5. Communication maîtrisée	Une communication interne et externe structurée évite la rumeur, les erreurs et la panique — un porte-parole unique est désigné

2. Organisation de la Réponse à Incident

> **Objectif :** Identifier les acteurs clés — CERT, RSSI, DSI, prestataires — et leurs rôles

Les acteurs internes et leurs rôles

Acteur interne	Rôle dans la réponse à incident	Actions clés pendant la crise
RSSI	Pilote de la réponse à incident — responsable de la coordination globale et de l'interface avec la direction	Qualification de l'incident, activation de la cellule de crise, pilotage du confinement, reporting à la DG, décision de notification aux autorités
Direction Générale (DG)	Décideur ultime — valide les arbitrages stratégiques et la communication de crise	Activation du PCA/PRA, validation de la communication externe, arbitrage sur la continuité des activités, engagement des ressources (budget, RH)
DSI / Équipes IT	Exécution technique de la réponse — isolation, investigation, restauration	Isolation des systèmes compromis, collecte des logs, restauration depuis les sauvegardes, remise en production sécurisée
Équipe SOC / Analystes sécurité	Détection, analyse et investigation technique de l'incident	Corrélation des alertes SIEM, analyse des IoC, investigation forensique initiale, suivi de la propagation
DPO	Évaluation de l'impact sur les données personnelles et coordination des obligations RGPD	Qualification violation de données, préparation de la notification CNIL, information des personnes concernées si risque élevé
Direction Juridique	Conseil juridique, qualification des infractions, gestion des preuves et des responsabilités	Conseil sur le dépôt de plainte, gestion des relations avec les assurances, clauses contractuelles avec les prestataires impactés
Communication / Relations Presse	Gestion de la communication externe et de la réputation	Rédaction des communiqués, coordination avec le porte-parole, gestion des réseaux sociaux, réponse aux médias
Directions métier	Porteurs des processus critiques — décideurs sur la continuité et les arbitrages métier	Activation des modes dégradés, information des équipes, validation des priorités de reprise, gestion des impacts clients

Les acteurs externes et leurs rôles

Acteur externe	Nature et mission	Quand et comment les solliciter
ANSSI	Agence nationale — autorité compétente pour les OIV/OSE et incidents NIS2 majeurs	Notification obligatoire sous 24h (NIS2 alerte précoce) pour les entités essentielles ; demande d'assistance possible pour les incidents critiques nationaux
CERT-FR	Centre gouvernemental de veille et réponse aux incidents — dépend de l'ANSSI	Signalement d'incidents via cert.ssi.gouv.fr ; source d'IoC et de bulletins d'alerte ; assistance technique pour les entités publiques
CNIL	Autorité de contrôle RGPD — notification des	Notification obligatoire sous 72h en cas de violation de données personnelles ; formulaire en ligne sur le portail CNIL

	violations de données personnelles	
Prestataire PRIS (Prestataire de Réponse à Incidents de Sécurité)	Expert qualifié ANSSI en investigation et réponse à incident	Sollicitation dès le début d'un incident critique P1/P2 ; recommandé d'avoir un contrat cadre pré-établi avant tout incident
Assureur cyber	Couverture des pertes financières liées à l'incident cyber	Notification dans les délais contractuels (souvent 48 à 72h) ; l'assureur peut imposer des prestataires agréés pour la réponse
Forces de l'ordre (BL-ANSSI / C3N)	Investigation judiciaire, dépôt de plainte, préservation des preuves	Dépôt de plainte dès constatation de l'infraction ; gendarmerie (C3N) ou BEFTI (Police) selon le type d'attaque
Hébergeur / Fournisseur Cloud	Support technique, accès aux logs infrastructure, isolation de VM	Contacter le support sécurité en urgence ; demander la préservation des logs cloud (durée limitée) ; vérifier les clauses contractuelles de notification

▸ La cellule de crise cyber — Composition et organisation

Rôle dans la cellule de crise	Titulaire (exemple)	Responsabilités spécifiques en cellule de crise
Directeur de crise (Crisis Manager)	Directeur Général ou DG délégué	Décision finale sur tous les arbitrages stratégiques ; approbation de la communication externe ; engagement des ressources
Coordinateur technique (RSSI)	RSSI	Pilotage de l'investigation et du confinement ; interface entre équipes techniques et direction ; suivi du journal de crise
Cellule technique (War Room)	DSI + Analystes SOC + PRIS	Exécution des actions techniques : isolation, forensique, restauration, surveillance ; reporting horaire au coordinateur
Cellule juridique et conformité	Directeur Juridique + DPO	Qualification des violations RGPD, préparation des notifications, gestion des preuves, relations assurances
Cellule communication	Directeur Communication + porte-parole	Rédaction et diffusion des messages internes et externes, gestion des médias, veille réputationnelle
Cellule métier	Directeurs des entités impactées	Activation des modes dégradés, information des équipes, gestion des impacts clients et fournisseurs

▸ Le journal de crise — Document clé

Le journal de crise est le registre chronologique de toutes les actions, décisions et communications pendant l'incident. Il est tenu en continu par le RSSI ou son adjoint désigné.

Horodatage	Auteur	Action / Décision / Observation	Justification et suite
JJ/MM HH:MM	RSSI	Qualification de l'incident — niveau P1 confirmé	Ransomware détecté sur 3 serveurs, propagation active via SMB

JJ/MM HH:MM	DSI	Isolation réseau du VLAN Serveurs	Coupure des flux est-ouest pour stopper la propagation
JJ/MM HH:MM	RSSI	Notification DG et activation cellule de crise	Seuil P1 atteint — procédure de crise activée
JJ/MM HH:MM	DPO	Qualification violation RGPD — données clients exposées	Notification CNIL à préparer — délai 72h déclenché

📡 3. Coordination des Équipes et Procédures d'Escalade

> **Objectif :** Mettre en place un processus clair de communication et d'alerte

▸ Le processus de gestion d'incident — Étape par étape

#	Étape	Actions détaillées et responsables
1	Détection de l'événement	Alerte SIEM, antivirus, utilisateur, prestataire ou CERT-FR → Enregistrement dans le système de ticketing — Responsable : SOC / DSI
2	Qualification initiale	L'analyste évalue : type d'incident, périmètre impacté, données concernées, criticité → Attribution d'un niveau P1 à P4 — Responsable : RSSI ou analyste senior
3	Notification et escalade	Selon le niveau de criticité : notification du RSSI (P3/P4), du DSI (P2), de la DG et activation cellule de crise (P1) — délais définis dans la procédure
4	Confinement immédiat	Isolation des systèmes compromis, révocation des accès suspects, blocage des flux malveillants — sans attendre l'investigation complète — Responsable : DSI + SOC
5	Investigation et analyse	Collecte et préservation des preuves (logs, dumps mémoire, images disques), analyse forensique, identification des IoC, reconstruction de la chronologie de l'attaque
6	Communication de crise	Information des équipes internes (points de situation réguliers), communication externe maîtrisée (porte-parole unique), notifications réglementaires (CNIL, ANSSI)
7	Éradication	Suppression du malware, fermeture des backdoors, changement des credentials compromis, patch des vulnérabilités exploitées — validation par le RSSI avant reprise
8	Reprise et surveillance renforcée	Restauration progressive des services, vérification d'intégrité, surveillance accrue pendant 30 à 90 jours post-incident
9	RETEX et clôture	Analyse des causes racines, bilan de la réponse, mise à jour des procédures, présentation à la direction, clôture formelle du ticket d'incident

▸ Procédure d'escalade — Matrice décisionnelle

Niveau	Criticité	Escalade vers	Délai max d'escalade	Actions d'escalade
P4	🟢 Faible	Analyste SOC senior	4 heures	Traitement standard, documentation dans le ticketing, information hebdomadaire du RSSI

P3	🟡 Modéré	RSSI	2 heures	Notification RSSI, plan d'action sous 24h, suivi quotidien jusqu'à résolution
P2	🟠 Majeur	RSSI + DSI + DG	30 minutes	Notification DG, mobilisation DSI, point de situation toutes les 2h, préparation communication interne
P1	🔴 Critique	DG + Cellule de crise complète	15 minutes	Activation cellule de crise, war room ouverte, point horaire, notifications réglementaires, PRIS sollicité

▸ Délais réglementaires de notification — À ne pas manquer

Réglementation	Autorité destinataire	Délai de notification	Contenu de la notification
RGPD Art. 33	CNIL	72h après constatation de la violation	Nature de la violation, catégories et volume de données, conséquences probables, mesures prises ou envisagées
RGPD Art. 34	Personnes concernées	Sans délai si risque élevé pour leurs droits	Description claire de la violation, coordonnées du DPO, conséquences probables, mesures de remédiation
NIS2 — Alerte précoce	ANSSI / autorité compétente	< 24h après détection	Notification initiale : type d'incident, périmètre touché, impact estimé — pas besoin d'analyse complète
NIS2 — Notification d'incident	ANSSI / autorité compétente	72h après détection	Rapport d'incident intermédiaire : analyse préliminaire, indicateurs de compromission, mesures de confinement
NIS2 — Rapport final	ANSSI / autorité compétente	1 mois après détection	Rapport complet : causes racines, impact réel, mesures correctives mises en oeuvre, plan de prévention
DORA (secteur financier)	Autorité nationale compétente	< 4h (incidents majeurs TIC)	Notification initiale puis rapport intermédiaire (72h) et rapport final (1 mois)
Assureur cyber	Assureur désigné au contrat	Délai contractuel : souvent 48-72h	Description de l'incident, systèmes impactés, premières estimations des pertes, mesures de confinement

▸ Communication de crise — Principes et canaux

Cible	Message clé à adapter	Canaux et fréquence

Équipes internes (tous)	Situation, consignes de sécurité immédiates, point de contact unique — ne pas spéculer	Email de crise depuis un canal de secours (si messagerie compromise), intranet, réunion flash — toutes les 2h minimum
Direction Générale / COMEX	Niveau d'impact, progression du confinement, risques résiduels, décisions à valider, coûts estimés	Points de situation structurés toutes les heures (P1) ou toutes les 2h (P2) — format 1 page synthèse
Clients et partenaires impactés	Impact sur leurs services, mesures prises, délai de rétablissement estimé — sans minimiser	Email personnalisé ou appel direct du directeur commercial — dès que l'impact est confirmé
Médias / Grand public	Faits confirmés uniquement, mesures prises, engagement de transparence — porte-parole unique	Communiqué de presse officiel validé par la DG et le juridique — pas de communication improvisée
Autorités (CNIL, ANSSI, police)	Faits documentés, chronologie, périmètre impacté, mesures de remédiation — langage précis et factuel	Formulaires officiels + email de confirmation + éventuellement appel au référent — dans les délais réglementaires

▸ Les 6 erreurs à éviter pendant une crise cyber

- Minimiser ou nier l'incident publiquement avant d'en connaître l'étendue réelle
- Laisser plusieurs porte-paroles communiquer des messages contradictoires
- Remettre en production des systèmes avant d'avoir éradiqué la menace (risque de ré-infection)
- Supprimer des logs ou des preuves dans la précipitation — compromet l'investigation et les poursuites judiciaires
- Payer la rançon sans consulter l'ANSSI et le juridique — ne garantit pas la récupération et finance les attaquants
- Négliger la communication interne — la rumeur et l'inquiétude des équipes désorganisent la réponse

4. Plan de Continuité et de Reprise d'Activité

> **Objectif :** Intégrer la réponse à incident dans la continuité de service

▸ Définitions et distinctions PCA / PRA / PRIS

Document / Plan	Objectif principal	Périmètre et déclenchement
PCA — Plan de Continuité d'Activité	Maintenir un niveau minimal de service pendant l'incident (mode dégradé)	Dès le début de l'incident — processus critiques priorisés, solutions de contournement activées
PRA — Plan de Reprise d'Activité	Restaurer les systèmes et services à leur état nominal après l'incident	Dès que la menace est éradiquée — restauration depuis sauvegardes saines, remise en production progressive
PRIS — Plan de Réponse aux Incidents de Sécurité	Gérer la réponse technique et organisationnelle à l'incident lui-même	Dès la détection — investigation, confinement, éradication ; complément au PCA/PRA
PGC — Plan de Gestion de Crise	Gérer la dimension stratégique, décisionnelle	Activation lors des incidents P1 et P2 — cellule de crise, communication, arbitrages DG

	et communicationnelle de la crise	

▸ Les indicateurs clés du PCA/PRA

Indicateur	Définition	Objectif type	Exemple concret
RTO — Recovery Time Objective	Durée maximale d'interruption tolérable pour un service ou processus critique	Service de paiement : RTO < 4h SI bureautique : RTO < 24h	Si le RTO est 4h, le PRA doit permettre de restaurer le service en moins de 4h
RPO — Recovery Point Objective	Volume maximal de données pouvant être perdues (exprimé en durée)	Données financières : RPO < 1h Données RH : RPO < 24h	Si le RPO est 1h, les sauvegardes doivent être au maximum toutes les heures
MTPD — Max Tolerable Period of Disruption	Durée maximale au-delà de laquelle l'impact devient irrémédiable pour l'organisation	Varie selon le secteur et le processus — souvent 24h à 72h pour les SI critiques	Au-delà du MTPD, la continuité métier est compromise même si le SI est restauré
MAO — Minimum Acceptable Operation	Niveau minimal de service permettant la poursuite des activités essentielles en mode dégradé	Défini par les métiers pour chaque processus critique	Traiter 20 % des commandes manuellement pendant la restauration du SI de commandes

▸ Structure type d'un PCA/PRA cyber

§	Chapitre	Contenu attendu
1	Contexte et périmètre	Processus et systèmes couverts, classification de criticité (BIA — Business Impact Analysis), liens avec la PSSI et la cartographie des risques
2	Organisation de crise	Cellule de crise, rôles et responsabilités, annuaire de crise (contacts 24/7), suppléances
3	Scénarios d'activation	Conditions déclenchant le PCA (pannes, cyberattaque, sinistre physique), niveaux d'activation, critères de retour à la normale
4	Modes dégradés par processus	Pour chaque processus critique : solution de contournement en mode dégradé, niveau MAO, durée maximale de mode dégradé
5	Procédures de reprise (PRA)	Ordre de priorité de restauration, prérequis techniques, étapes de restauration par système, critères de validation avant remise en production
6	Gestion des sauvegardes	Architecture de sauvegarde (3-2-1), fréquence, localisation, procédure de restauration testée, RTO/RPO garantis
7	Communication de crise	Messages types par cible (interne, clients, médias, autorités), canaux de communication de secours, porte-parole désigné
8	Tests et exercices	Programme annuel de tests : simulation de crise, test de restauration, exercice PCA avec les métiers — documentation des résultats
9	Maintenance et révision	Fréquence de révision (annuel + après incident), responsable de la mise à jour, processus de validation, versionnage

La règle des sauvegardes 3-2-1-(1-0) — Fondement du PRA

Règle	Signification	Mise en oeuvre et justification
3	3 copies des données	1 copie de production + 2 copies de sauvegarde → élimine tout point de défaillance unique
2	2 supports différents	Ex. : NAS local + bande LTO ou cloud → protège contre la défaillance d'un type de support
1	1 copie hors site	Copie déportée géographiquement (datacenter secondaire, cloud) → protège contre le sinistre physique (incendie, inondation)
+1	1 copie hors ligne (air-gap)	Copie déconnectée du réseau (bande, disque déconnecté) → inaccessible au ransomware, protection ultime
=0	0 erreur de restauration	Les sauvegardes doivent être testées régulièrement — une sauvegarde non testée n'est pas une sauvegarde

Programme de tests et d'exercices du PCA/PRA

Type d'exercice	Objectif	Fréquence recommandée	Participants
Test de restauration (technique)	Valider que les sauvegardes sont restaurables dans les délais RTO/RPO définis	Semestriel minimum	DSI, équipes IT, RSSI
Table-top exercise (jeu de rôle)	Tester les procédures d'escalade et les réflexes des équipes sur un scénario fictif sans impact réel	Annuel	RSSI, COPIL, Cellule de crise, métiers
Exercice de crise complet (full-scale)	Simuler une crise cyber réelle : activation cellule de crise, modes dégradés, communication	Annuel ou bisannuel	DG, RSSI, DSI, Communication, Juridique, métiers
Test de basculement (failover)	Vérifier le basculement automatique vers le site de secours ou le cloud DR	Annuel	DSI, RSSI, prestataires hébergement
Exercice de notification réglementaire	Tester le processus de notification CNIL et ANSSI sur un scénario fictif	Annuel	DPO, Juridique, RSSI, Communication

Analyse d'Impact Métier (BIA — Business Impact Analysis)

Le BIA est la base du PCA/PRA : il identifie les processus critiques, leur niveau de priorité et les ressources nécessaires à leur maintien en mode dégradé.

Processus métier	Criticité (1-4)	RTO cible	RPO cible	MAO	Dépendances SI critiques

Traitement des paiements	4 — Critique	< 1h	< 15 min	Manuel partiel	ERP, connexion bancaire, réseau
Gestion des commandes clients	4 — Critique	< 4h	< 1h	Traitement papier	CRM, ERP, messagerie
Production / Opérations	3 — Élevé	< 8h	< 4h	Mode manuel dégradé	SCADA, ERP production, réseau OT
RH / Paye	3 — Élevé	< 24h	< 24h	Saisie manuelle	SIRH, messagerie, VPN
SI bureautique (postes)	2 — Modéré	< 48h	< 24h	Postes de prêt	Active Directory, VPN, messagerie

📌 Mémo Récapitulatif — À Retenir

🚨 Gestion de Crise	🏗️ Acteurs & Organisation	📡 Escalade & Communication	🔄 PCA / PRA
• 4 niveaux : P1 🔴 → P4 🟢 • 6 phases NIST : Prép. → RETEX • 5 principes : Anticip., Rapidité, Coord., Preuves, Comm. • MTTD < 24h | MTTR critique < 4h • Journal de crise : horodaté et continu • Cellule de crise activée dès P1	• RSSI : coordinateur technique central • DG : décideur ultime de la cellule de crise • PRIS (ANSSI) : expert qualifié à contacter en P1 • CERT-FR : signalement + source d'IoC • DPO : notification CNIL sous 72h • Assureur : notification dans le délai contractuel	• P1 : escalade DG en 15 min, war room • P2 : escalade RSSI + DG en 30 min • NIS2 : alerte 24h → notif. 72h → rapport 1 mois • RGPD violation : CNIL sous 72h • Porte-parole unique pour les médias • 6 erreurs à éviter : minimiser, payer rançon, écraser les preuves…	• PCA = maintien service | PRA = restauration • RTO : durée max d'interruption tolérable • RPO : volume max de données perdues tolérable • Règle 3-2-1+1=0 : copies, supports, hors site, air-gap • BIA : identifier les processus critiques et leurs dépendances • Tests annuels : table-top + restauration + full-scale

Le cycle de la réponse à incident

Préparation → Détection → Confinement → Éradication → Reprise (PCA/PRA) → RETEX → Amélioration continue