

MODÈLE

Plan de réponse à incident cyber

Modèle prêt à remplir : cellule de crise, délais légaux, procédures et REX

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~12 min Édition 2026 sedona-ai.com

Le pire moment pour improviser une réponse à une cyberattaque, c'est pendant la cyberattaque. Un plan de réponse à incident écrit, connu et testé fait gagner les heures qui séparent un incident maîtrisé d'une crise incontrôlée — et il conditionne le respect de délais légaux stricts. Ce modèle reprend les référentiels de référence (NIST, SANS, ANSSI) et les obligations de notification (RGPD, NIS2) sous une forme prête à personnaliser : remplissez les zones [entre crochets] avec vos coordonnées et vos règles internes.

À retenir

- Deux horloges se déclenchent dès la détection : 72 h pour notifier la CNIL en cas de violation de données personnelles, et jusqu'à 24 h / 72 h vis-à-vis de l'ANSSI pour les entités concernées par NIS2 (délais de la directive, non transposée en droit français au 14/10/2026).
- Un plan repose sur une cellule de crise aux rôles définis à l'avance et un annuaire d'urgence tenu à jour hors ligne.
- La réponse suit un cycle éprouvé : préparation, détection/analyse, endiguement, éradication, rétablissement, retour d'expérience.
- Préservez les preuves : n'éteignez pas les machines, isolez-les du réseau, conservez les journaux.
- Un plan non testé est un document mort : exercez-le au moins une fois par an.

01 Comment utiliser ce modèle

Ce document est une trame. Chaque zone [entre crochets] est à compléter avec vos informations propres (noms, coordonnées, seuils). Diffusez la version finale à votre cellule de crise, imprimez-en une copie conservée hors ligne (une attaque peut rendre vos systèmes — et donc ce fichier — inaccessibles), et révisez-la après chaque exercice ou incident.

4,44 M\$

Coût moyen mondial d'une violation de données en 2025 ; il grimpe à 5,08 M\$ pour un incident d'extorsion / rançongiciel.

IBM, Cost of a Data Breach Report 2025

48 %

Part des PME, TPE et ETI parmi les victimes de rançongiciel signalées à l'ANSSI en 2025 — la catégorie la plus ciblée.

ANSSI/CERT-FR, Panorama de la cybermenace 2025

02 Délais de notification à ne pas rater

Obligation	Délai	Auprès de qui
Violation de données personnelles (risque pour les personnes)	72 h après en avoir pris connaissance	CNIL — art. 33 du RGPD
Information des personnes concernées	Dans les meilleurs délais si risque élevé	Personnes concernées — art. 34 du RGPD
Incident important — alerte précoce (entités NIS2)	24 h	ANSSI / CSIRT — art. 23 de la directive NIS2
Incident important — notification (entités NIS2)	72 h	ANSSI / CSIRT — art. 23 de la directive NIS2
Incident important — rapport final (entités NIS2)	1 mois après la notification	ANSSI / CSIRT — art. 23 de la directive NIS2

À vérifier pour votre entité

Les délais RGPD (72 h) s'appliquent dès aujourd'hui à toute organisation traitant des données personnelles. Les délais 24 h / 72 h / 1 mois sont ceux fixés par la directive NIS2 ; leur application en France dépend de la loi de transposition, non promulguée au 14/10/2026, et de ses décrets. Confirmez si votre organisation est une entité « essentielle » ou « importante » au sens de NIS2.

Réflexes complémentaires en France : déposer plainte (police/gendarmerie), utiliser le guichet unique 17Cyber (assistance 24/7), et prévenir votre assureur cyber sans délai (les polices imposent souvent une déclaration rapide).

03 [À remplir] Cellule de crise & annuaire d'urgence

Rôle	Responsable (titulaire / suppléant)	Contact 24/7
Décideur (direction générale)	[Nom / suppléant]	[Téléphone / e-mail]
Pilote technique (RSSI / DSI)	[Nom / suppléant]	[Téléphone / e-mail]
Référent données personnelles (DPO)	[Nom]	[Téléphone / e-mail]
Communication	[Nom]	[Téléphone / e-mail]
Juridique	[Nom]	[Téléphone / e-mail]
Prestataire réponse à incident	[Société]	[Hotline]
Assureur cyber	[Compagnie / n° de police]	[Hotline sinistre]
Autorités (CNIL, ANSSI/CSIRT, 17Cyber, forces de l'ordre)	—	notifications.cnil.fr · 17cyber.gouv.fr

04 [À remplir] Classification de la gravité

Niveau	Critères	Déclenchement
P1 — Critique	Arrêt d'activité, données personnelles massives, rançongiciel actif	Cellule de crise complète + direction
P2 — Majeur	Compromission confirmée, impact limité, propagation possible	Cellule technique + décideur
P3 — Modéré	Tentative avérée sans compromission, périmètre restreint	Pilote technique
P4 — Mineur	Événement suspect à investiguer	Astreinte / support

05 Les 6 étapes de la réponse

Ce cycle synthétise les référentiels de référence : le guide du NIST (SP 800-61) et le modèle SANS. Adaptez-le à votre organisation, sans en sauter d'étape.

1 Préparation

Avant tout incident : plan à jour, sauvegardes hors ligne testées, journalisation activée, rôles connus, exercices réalisés. C'est ici que se gagne 80 % de la réponse.

2 Identification & analyse

Détecter, qualifier et classer l'incident (niveau P1-P4). Déterminer si des données personnelles sont concernées (horloge CNIL) et si vous êtes une entité NIS2 (horloge ANSSI).

3 Endiguement

Isoler les systèmes touchés du réseau SANS les éteindre, préserver les preuves (images disque, journaux), suspendre les comptes compromis, protéger les sauvegardes.

4 Éradication

Identifier la cause racine, supprimer le point d'entrée et les persistances, corriger les vulnérabilités exploitées.

5 Rétablissement

Restaurer depuis des sauvegardes saines, remettre en service progressivement sous surveillance renforcée, vérifier l'absence de réinfection.

6 Retour d'expérience (REX)

Reconstituer la chronologie, mesurer les impacts (coûts, durée d'arrêt), en tirer un plan d'action correctif et mettre à jour le plan.

06 Arbre de décision & endiguement

1. Incident confirmé ? Sinon, poursuivre l'investigation (P4).
2. Des données personnelles sont-elles concernées ? Si oui → démarrer l'horloge des 72 h (CNIL).
3. Êtes-vous une entité NIS2 ? Si oui → démarrer l'horloge des 24 h (alerte précoce ANSSI).
4. Le système peut-il être isolé sans aggraver la situation ? Isoler sans éteindre, préserver les preuves.
5. Rançongiciel : ne pas payer (paiement déconseillé par l'ANSSI, sans garantie et finançant la menace) ; contacter prestataire + assureur + autorités.

N'éteignez pas, ne réinstallez pas dans la précipitation

Éteindre une machine ou réinstaller trop tôt détruit les preuves nécessaires à l'analyse et à d'éventuelles poursuites. Isolez du réseau, conservez les journaux, et laissez le prestataire de réponse à incident travailler sur des copies.

07 [À remplir] Communication & check-list post-incident

Désignez un porte-parole unique et préparez à l'avance des modèles de messages : information interne des collaborateurs, communication aux clients et partenaires, réponse aux régulateurs et à la presse. Le silence et l'improvisation aggravent l'atteinte à l'image.

☐ Chronologie complète de l'incident reconstituée et horodatée.

☐ Notifications légales effectuées dans les délais (CNIL / ANSSI) et tracées.

- ☐ Cause racine identifiée et corrigée ; vulnérabilité fermée.
- ☐ Sauvegardes vérifiées saines avant toute restauration.
- ☐ Coûts et durée d'indisponibilité (MTTD / MTTR) mesurés.
- ☐ Plan d'action correctif défini, avec responsables et échéances.
- ☐ Plan de réponse à incident mis à jour ; prochain exercice planifié.

§ Sources

1. RGPD — art. 33 et 34 (notification des violations) — <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
2. CNIL — Notifier une violation de données personnelles — <https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles>
3. Directive (UE) 2022/2555 (NIS2) — art. 23 (notification d'incident) — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
4. NIST — SP 800-61, Computer Security Incident Handling Guide — <https://csrc.nist.gov/pubs/sp/800/61/r3/final>
5. ANSSI — Anticiper et gérer une crise d'origine cyber — <https://cyber.gouv.fr/securisation/gestion-de-crise/anticiper-gerer-une-crise-cyber/>
6. 17Cyber — guichet unique d'assistance cyber — <https://17cyber.gouv.fr>
7. IBM — Cost of a Data Breach Report 2025 — <https://www.ibm.com/reports/data-breach>
8. ANSSI/CERT-FR — Panorama de la cybermenace 2025 — <https://www.cert.ssi.gouv.fr/>

Avant l'incident, voyez ce que vous exposez

Un plan de réponse se prépare avant l'incident. Sedona Radar analyse ce que votre domaine expose sur Internet et classe les constats par gravité : de quoi nourrir vos scénarios avec des faits. Sedona n'est pas un prestataire de réponse à incident. Lancez un scan gratuit pour objectiver votre point de départ.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit