

LIVRE BLANC

Réponse à incident cyber : le guide

Détecter, décider, notifier, remédier : le manuel de survie des PME et ETI françaises face à une cyberattaque, des 24 premières heures au retour à la normale.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~55 min Édition 2026 sedona-ai.com

Sommaire

-
- 01** Incident, crise, violation : de quoi parle-t-on vraiment ?
 - 02** Panorama chiffré de la menace 2025 : ce que disent les chiffres officiels
 - 03** Anatomie des grandes familles d'incidents
 - 04** Le coût réel d'un incident et pourquoi les PME sont des cibles de choix
 - 05** RGPD : notifier la CNIL sous 72 heures (art. 33 et 34)
 - 06** NIS2 : le signalement en trois temps (et son statut incertain en France)
 - 07** Les obligations sectorielles et l'assurance : d'autres délais à ne pas rater
 - 08** Notifier n'est pas porter plainte : les démarches cumulatives
 - 09** NIST SP 800-61 : du cycle en 4 phases (Rev.2) aux 6 fonctions (Rev.3)
 - 10** SANS PICERL et ISO/IEC 27035 : les alternatives opérationnelles
 - 11** La doctrine ANSSI : réponse à incident technique vs gestion de crise
 - 12** Lire l'attaque : IOC, TTP, kill chain et MITRE ATT&CK
 - 13** Les 24 premières heures : détecter, qualifier, alerter
 - 14** Confiner, éradiquer, remédier, reconstruire
 - 15** Piloter la crise : cellule, rôles et communication
 - 16** Rançongiciel : payer ou ne pas payer ?
 - 17** Vos modèles prêts à l'emploi : check-lists et documents types
 - 18** Spécificités PME/ETI : faire face avec des moyens limités
 - 19** À qui s'adresser : 17Cyber, PRIS, CERT-FR et CSIRT territoriaux
 - 20** L'assurance cyber : conditions, réflexes et pièges
 - 21** Anticiper : plan de réponse, sauvegardes et exercices de crise
 - 22** Retour d'expérience : transformer l'incident en résilience
-

Une cyberattaque n'est plus une question de « si » mais de « quand » : l'ANSSI a été informée de 1 366 incidents en 2025 et le rançongiciel est présent dans 88 % des violations touchant les PME (Verizon DBIR 2025). Or 65 % des TPE-PME n'ont aucune procédure de réaction formalisée. Ce guide comble ce vide. Il explique, sans jargon, ce qu'est un incident, ce que la loi impose (notification CNIL sous 72 h), ce que prévoit NIS2 (directive non transposée en droit français au 14/10/2026), quel framework suivre (NIST, ANSSI, ISO 27035), puis déroule un playbook heure par heure des 24 et 72 premières heures : qui appeler, quoi isoler, quoi notifier, quoi conserver comme preuve. Modèles, check-lists et plan de préparation inclus. Chaque chiffre est sourcé ; les incertitudes (transposition NIS2) sont signalées.

À retenir

- Le rançongiciel est impliqué dans 88 % des violations chez les PME contre 39 % chez les grandes entreprises (Verizon DBIR 2025) : la petite taille n'est pas une protection, c'est un facteur de risque.
- Deux horloges de 72 h à ne jamais confondre : notification CNIL de la violation de données (RGPD art. 33) et dépôt de plainte pénale pour être indemnisé par l'assurance cyber (LOPMI, art. L12-10-1 du Code des assurances).
- Le délai RGPD de 72 h court dès la PRISE DE CONNAISSANCE de la violation, week-ends et jours fériés compris, pas à la fin de l'investigation : une notification initiale incomplète est explicitement autorisée.
- La directive NIS2 impose un signalement en trois temps (24 h / 72 h / 1 mois), mais elle N'EST PAS transposée en droit français à ce jour (loi « Résilience » non promulguée, France poursuivie devant la CJUE) : à vérifier au moment de la lecture.
- La menace se déplace du chiffrement pur vers l'exfiltration de données comme levier d'extorsion : l'ANSSI recense une forte hausse des exfiltrations en 2025 alors que les rançongiciels « classiques » reculent légèrement.
- La position officielle ANSSI/Cybermalveillance est de NE PAS payer la rançon : environ la moitié seulement des victimes récupèrent correctement leurs données après paiement, avec risque de double extorsion.
- L'anticipation est décisive : un plan écrit, des sauvegardes testées et au moins un exercice de crise par an transforment une catastrophe en incident gérable — 17Cyber (24/7) et les prestataires PRIS qualifiés ANSSI sont les bons interlocuteurs.
- Réduire la surface d'attaque exposée en amont diminue mécaniquement la probabilité et la gravité de l'incident : c'est le seul levier réellement sous votre contrôle avant l'attaque.

01 Incident, crise, violation : de quoi parle-t-on vraiment ?

Avant de savoir réagir, il faut savoir nommer. La confusion des mots est la première faille : un dirigeant qui appelle « crise » un simple e-mail suspect surréagit, celui qui appelle « incident mineur » une exfiltration de fichiers clients sous-réagit — et rate le délai légal. L'ANSSI donne la définition socle dans son glossaire officiel (CyberDico) : un incident de sécurité est « tout événement ayant ou pouvant avoir un impact négatif sur la sécurité du système d'information ». Deux mots comptent : « pouvant » (le risque suffit, l'impact avéré n'est pas requis) et « événement » (un incident n'est pas forcément une attaque — une erreur de configuration ou une panne peut en être un).

Quand un incident devient une crise cyber

Tout incident n'est pas une crise. Selon la doctrine ANSSI (« Anticiper et gérer une crise cyber »), on bascule en crise cyber lorsque l'incident met en péril les objectifs prioritaires de l'organisation. Trois marqueurs la caractérisent : la fulgurance des impacts, le manque de temps pour y répondre et sa forte technicité. Concrètement, la crise sort du périmètre de la DSI : elle engage la gouvernance, la continuité d'activité, le juridique et la communication. L'ANSSI structure sa gestion en 4 phases — anticipation, alerte/qualification, gestion, sortie de crise — cette dernière (remédiation complète) pouvant s'étaler sur plusieurs mois.

Notion	Définition de référence	Ce qui la déclenche	Enjeu pour le dirigeant
Incident de sécurité	« Tout événement ayant ou pouvant avoir un impact négatif sur la sécurité du SI » (CyberDico ANSSI)	Un événement avéré ou seulement potentiel	Qualifier vite : anodin ou structurant ?
Crise cyber	Incident qui met en péril les objectifs prioritaires de l'organisation (doctrine ANSSI)	Fulgurance, manque de temps, forte technicité	Mobiliser la gouvernance, pas seulement l'informatique
Violation de données personnelles	Atteinte entraînant destruction, perte, altération, divulgation ou accès non autorisé à des données personnelles (RGPD)	Une atteinte touchant des données personnelles	Horloge légale : 72 h pour notifier la CNIL (art. 33 RGPD)

- IOC (indicateur de compromission) — selon le CyberDico ANSSI, « combinaison d'informations techniques et contextuelles représentatives d'une manifestation ou d'une tentative de compromission ». Exemples : une adresse IP malveillante, une empreinte de fichier, un nom de domaine de commande. Volatile : un attaquant change ses IOC en quelques minutes.
- TTP (tactiques, techniques et procédures) — la façon d'opérer de l'attaquant : comment il entre, se déplace, exfiltre. Bien plus stable : un adversaire ne change ses TTP qu'en quelques mois ou années.

- Pourquoi ça compte pour un dirigeant : bloquer une IP (IOC) arrête une attaque précise ; comprendre une TTP permet d'anticiper toute une famille d'attaques. Le renseignement fondé sur les TTP a donc une valeur défensive durable, là où la chasse aux seuls IOC est un jeu de ratissage permanent.

Pour cartographier ces TTP, la référence mondiale est MITRE ATT&CK (attack.mitre.org), base de connaissances des comportements adverses réellement observés, organisée en tactiques (les objectifs) et techniques (les méthodes). Elle complète — sans le remplacer — le modèle de « kill chain » de Lockheed Martin, vision linéaire de la progression d'une attaque, de la reconnaissance à l'atteinte de l'objectif. Aucune de ces grilles n'exige d'être experte : elles servent surtout à mettre dirigeant, DSI et prestataire au même niveau de langage le jour où tout s'accélère.

02 Panorama chiffré de la menace 2025 : ce que disent les chiffres officiels

1 366

incidents de cybersécurité portés à la connaissance de l'ANSSI en 2025 (contre 1 361 en 2024), sur 2 209 signalements reçus

ANSSI, Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002, publié le 11 mars 2026)

≈ 60 %

des intrusions initiales passent par le phishing, vecteur dominant en 2025

ENISA, Threat Landscape 2025 (octobre 2025)

> 500 000

victimes assistées par [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en 2025 (+20 %) ; les demandes d'entreprises progressent de +73 %

[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), Rapport d'activité 2025

La photographie 2025 dessine un basculement tactique net. Le rançongiciel chiffrant « classique » recule légèrement (128 compromissions signalées à l'ANSSI, contre 141 en 2024), tandis que les incidents d'exfiltration de données explosent : 196 cas déclarés contre 130 en 2024, soit +51 %. Autrement dit, voler pour faire chanter devient un levier de pression autonome, sans même avoir besoin de chiffrer. Côté européen, l'ENISA confirme la prééminence du phishing (~60 % des vecteurs d'intrusion initiale) et une forte part de rançongiciel dans les incidents cybercriminels visant les organisations de l'UE.

Déclaré n'est pas confirmé : se méfier du volume brut

Les compteurs officiels agrègent des événements DÉCLARÉS ou revendiqués, pas des faits systématiquement avérés. Sur les 196 exfiltrations « déclarées » en 2025, l'ANSSI n'en aurait confirmé qu'une minorité — de l'ordre de 80 (source secondaire : L'Usine Digitale reprenant l'ANSSI, à recouper). Les attaquants gonflent leurs revendications pour maximiser la pression. Ne jamais présenter un volume brut de signalements comme un nombre de compromissions prouvées : c'est le piège du « recall brut trompeur ». De même, le chiffre souvent cité « PME = 48 % des victimes de rançongiciel » provient d'une source secondaire (shattered.io) et n'a pas été confirmé mot pour mot dans le PDF officiel — à traiter avec une confiance basse.

Indicateur 2025	Chiffre	Source	Confiance
Incidents traités par l'ANSSI	1 366 (vs 1 361 en 2024)	ANSSI, Panorama cybermenace 2025	Élevée
Signalements reçus	2 209	ANSSI, Panorama cybermenace 2025	Élevée
Événements de sécurité traités	3 586 (-18 %)	ANSSI, Panorama cybermenace 2025	Moyenne
Compromissions par rançongiciel	128 (vs 141 en 2024)	ANSSI, Panorama cybermenace 2025	Moyenne
Exfiltrations de données déclarées	196 (vs 130), soit +51 %	ANSSI, Panorama cybermenace 2025	Moyenne
Exfiltrations effectivement confirmées	~80 sur 196 revendiquées	ANSSI / L'Usine Digitale (secondaire)	Basse
Part PME/TPE/ETI parmi les victimes rançongiciel	~48 % (à vérifier)	Source secondaire (shattered.io)	Basse

03 Anatomie des grandes familles d'incidents

Famille	Mécanisme	Signaux d'alerte	Impact type PME
Rançongiciel	Chiffrement des données, précédé d'une exfiltration pour double extorsion	Fichiers renommés/chiffrés, note de rançon, pics d'activité nocturne, antivirus désactivé	Arrêt d'activité, perte de données, extorsion, atteinte à l'image
Intrusion / compromission de système	Accès non autorisé via faille, identifiants volés ou service exposé	Connexions inhabituelles, comptes créés, mouvements latéraux, alertes EDR	Point d'entrée vers vol de données ou rançongiciel ; persistance discrète
Compromission de compte & fraude au président (BEC)	Détournement de messagerie, usurpation de dirigeant ou de fournisseur	E-mails de virement « urgents et confidentiels », règle de transfert cachée, IBAN modifié	Fraude financière directe, souvent sans aucun logiciel malveillant
Violation de données personnelles	Accès ou divulgation non autorisée de données personnelles	Fuite constatée, revendication sur un forum, alerte d'un tiers	Notification CNIL sous 72 h, sanctions, perte de confiance clients
Déni de service (DoS/DDoS)	Saturation de la bande passante ou des ressources serveur	Indisponibilité soudaine du site/service, latence extrême	Perte de chiffre d'affaires en ligne, parfois diversion d'une autre attaque
Chaîne d'approvisionnement (supply chain)	Compromission d'un prestataire ou d'un éditeur logiciel de confiance	Comportement anormal après une mise à jour, alerte de l'éditeur	Contamination par un tiers de confiance, très difficile à anticiper

La lecture des chiffres 2025 impose de souligner un glissement tactique majeur : le rançongiciel chiffant recule (128 cas ANSSI, -9 %) au profit de l'exfiltration pure (196 cas, +51 %). La logique de l'attaquant change : il n'a plus besoin de paralyser un système pour extorquer, il lui suffit de voler des données et de menacer de les publier. Pour une PME, cela veut dire qu'une attaque « sans écran bloqué et sans rançon visible » peut être tout aussi grave — et que l'absence de chiffrement ne signifie jamais l'absence de vol.

- Connexions hors horaires ouvrés ou depuis des géographies inhabituelles
- Comptes créés, ou privilèges élevés attribués, sans demande légitime
- Volumes de données sortants anormaux — indice direct d'une exfiltration en cours
- Désactivation d'outils de sécurité (antivirus, journalisation, sauvegardes)

- E-mails internes de paiement présentés comme « urgents et confidentiels »
- Alerte émanant d'un tiers : client, banque, CERT-FR ou chercheur en sécurité

04 Le coût réel d'un incident et pourquoi les PME sont des cibles de choix

4,44 M\$

coût moyen MONDIAL d'une violation de données en 2025 (-9 % vs 4,88 M\$ en 2024, première baisse en 5 ans)

IBM, Cost of a Data Breach Report 2025

241 jours

délai moyen MONDIAL pour identifier puis contenir une brèche (181 j + 60 j) — le plus bas en 9 ans

IBM, Cost of a Data Breach Report 2025

88 %

des violations touchant les PME impliquent un rançongiciel, contre 39 % pour les grandes entreprises

Verizon, 2025 Data Breach Investigations Report

Deux enseignements structurent le calcul du risque. D'abord, la vitesse paie : selon IBM, une brèche contenue en moins de 200 jours coûte en moyenne 3,87 M\$, contre 5,01 M\$ au-delà, soit +29 %. Le délai de détection est donc un levier financier direct, pas un simple indicateur technique. Ensuite, l'asymétrie PME/grandes entreprises est frappante. Le Verizon DBIR 2025 montre que le rançongiciel frappe 88 % des violations en PME contre 39 % chez les grands comptes — et 43 % des PME n'ont aucun collaborateur dédié à la cybersécurité. Moins outillées, moins surveillées, souvent maillon d'une chaîne d'approvisionnement plus vaste : les PME concentrent l'exposition et le manque de moyens, ce qui en fait des cibles rationnelles pour un attaquant.

Attention aux moyennes : mondial ≠ France ≠ PME

Le coût moyen de 4,44 M\$ et le délai de 241 jours sont des moyennes MONDIALES, toutes tailles et tous secteurs confondus — ni un chiffre France, ni un chiffre PME. Il serait trompeur de les appliquer tels quels à une PME française. Les estimations France diffusées via IBM (~3,59 M€ pour l'édition 2025, ou ~3,8 M€ ≈ 4,8 M\$ pour 2024) proviennent de synthèses secondaires, mélangeant parfois les devises et reposent sur de petits échantillons : à manier avec réserve, jamais comme un tarif garanti.

Où Sedona agit — et où elle n'agit pas

Sedona.AI n'est pas prestataire de réponse à incident ni de forensic. Face à un incident avéré, mobilisez un prestataire qualifié PRIS par l'ANSSI, votre assureur cyber et le guichet public 17Cyber (17cyber.gouv.fr, 24/7). Là où Sedona intervient, c'est en amont : voir ce que votre organisation expose sur Internet (Sedona Radar l'analyse ; il ne certifie rien) et sensibiliser vos équipes. Anticiper coûte toujours moins cher que subir les 241 jours de la moyenne mondiale.

05 RGPD : notifier la CNIL sous 72 heures (art. 33 et 34)

Dès qu'un incident touche des données à caractère personnel, une horloge démarre. L'article 33 du RGPD impose au responsable de traitement de notifier la violation à l'autorité de contrôle — la CNIL en France — « dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance ». Ce délai ne se déclenche pas à la survenance technique de l'incident, ni à la fin de l'investigation forensic : il court à partir de la PRISE DE CONNAISSANCE, avec un degré raisonnable de certitude qu'une violation s'est produite. Seule exception : la violation qui n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

1 JO — Prise de connaissance

Le compteur de 72 h démarre au moment où vous acquérez la certitude raisonnable qu'une violation a eu lieu — pas au moment de l'attaque, pas à la fin du forensic. Horodatez ce moment : c'est lui qui fait foi. Le délai court en heures calendaires, week-ends et jours fériés compris, sans suspension.

2 Évaluer le risque pour les personnes

S'il n'existe aucun risque pour les droits et libertés des personnes, la notification CNIL n'est pas obligatoire (mais la violation doit être documentée en interne). Dès qu'un risque existe, la notification devient obligatoire.

3 Notifier la CNIL (même incomplet)

La notification se fait via le téléservice officiel notifications.cnil.fr. Le texte autorise **EXPLICITEMENT** une notification initiale incomplète dans les 72 h : nature de la violation, catégories et volume approximatif de personnes/enregistrements, conséquences probables, mesures prises. Mieux vaut une notification partielle dans les délais qu'une notification complète hors délais.

4 Compléter par phases

Les informations manquantes sont transmises ultérieurement, au fur et à mesure de l'investigation, via des notifications complémentaires rattachées au dossier initial.

5 Informer les personnes si le risque est ÉLEVÉ (art. 34)

Si — et seulement si — la violation est susceptible d'engendrer un risque ÉLEVÉ pour les personnes, vous devez en informer directement les personnes concernées, dans les meilleurs délais, en clair et sans jargon (nature de la violation, conséquences, mesures, point de contact).

Le piège du point de départ

Beaucoup de PME croient disposer de 72 h à partir de la fin de l'enquête technique. C'est faux. Le délai court dès la prise de connaissance de la violation, week-ends et jours fériés inclus. Un incident détecté un vendredi soir n'attend pas le lundi. Si vous dépassez les 72 h, la loi vous oblige à accompagner la notification des MOTIFS DU RETARD — l'absence de justification est en soi un manquement.

Critère	Art. 33 — Notification CNIL	Art. 34 — Information des personnes
Destinataire	La CNIL (autorité de contrôle)	Les personnes concernées elles-mêmes
Seuil de déclenchement	Risque pour les droits et libertés	Risque ÉLEVÉ pour les droits et libertés
Délai	72 h après prise de connaissance	Dans les meilleurs délais (pas de durée chiffrée)
Caractère	Systématique dès qu'il y a risque	Seulement si le risque est qualifié d'élevé
Notification incomplète	Admise puis complétée	Doit être claire et compréhensible

jusqu'à 10 M€ ou 2 % du CA mondial

Sanction maximale pour manquement à l'obligation de notification (RGPD art. 83(4)(a), le montant le plus élevé étant retenu)

RGPD, article 83 — règlement (UE) 2016/679, texte officiel sur EUR-Lex

Ce que la CNIL a sanctionné en 2025

En 2025, la CNIL a prononcé 83 sanctions pour un montant cumulé record de 486 839 500 €. La sécurité des données figure parmi les principaux motifs (mots de passe faibles, comptes partagés...), aux côtés des cookies et de la surveillance des salariés. Exemple marquant : France Travail, 5 M€ (sanction rendue publique début 2026) pour défaut de sécurité des données de demandeurs d'emploi. Source : CNIL, Bilan des sanctions 2025 (cnil.fr/fr/bilan-sanctions-2025). Le défaut de notification relève de la catégorie de sanction la plus lourde du RGPD.

06 NIS2 : le signalement en trois temps (et son statut incertain en France)

DRAPEAU — à vérifier à la date de votre lecture (état au 14/10/2026)

La directive NIS2 n'est PAS, à ce jour, transposée en droit français. L'échéance européenne de transposition (17 octobre 2024) est dépassée. Le projet de « loi Résilience » (transposant NIS2 + directive REC + directive (UE) 2022/2556, volet DORA) a été adopté en 1re lecture par le Sénat le 12 mars 2025, puis retiré de l'ordre du jour des séances des 7 et 9 octobre 2026 de l'Assemblée nationale, sans nouvelle date : le texte n'est ni voté ni promulgué. La Commission européenne a saisi la Cour de justice de l'UE contre la France le 8 juillet 2026 pour défaut de transposition. Les délais ci-dessous sont ceux de la DIRECTIVE EUROPÉENNE ; ils ne constituent pas encore une obligation légale française opposable aux PME/ETI. Vérifiez le statut à jour sur cyber.gouv.fr.

L'article 23 de la directive (UE) 2022/2555 (NIS2) organise, pour les entités « essentielles » et « importantes », un signalement chronométré en trois temps vers l'autorité compétente ou le CSIRT national, déclenché par un incident « significatif » — notion distincte de la « violation de données » du RGPD. Un incident est significatif s'il cause (ou peut causer) une perturbation opérationnelle sévère ou une perte financière pour l'entité, ou s'il affecte des tiers en causant un préjudice matériel/immatériel considérable. Un même événement peut donc relever simultanément du RGPD et de NIS2, avec des horloges différentes.

Étape	Délai	Contenu attendu
Alerte précoce	Sans retard injustifié, au plus tard 24 h après connaissance de l'incident significatif	Signaler l'existence de l'incident, soupçon d'acte malveillant, impact transfrontière éventuel
Notification d'incident	Au plus tard 72 h après connaissance	Évaluation initiale : gravité, impact, indicateurs de compromission ; mise à jour de l'alerte
Rapport intermédiaire	Sur demande du CSIRT / autorité	État d'avancement si l'incident est toujours en cours
Rapport final	Au plus tard 1 mois après la notification d'incident	Analyse détaillée, cause racine, mesures d'atténuation appliquées

La transposition française doit élargir massivement le périmètre : d'environ 300 à 500 opérateurs sous l'ancien régime OIV/OSE (issu de NIS1 / LPM) à environ 15 000 entités « essentielles » ou « importantes » (estimation de l'étude d'impact du projet de loi, octobre 2024), dont environ 1 500 collectivités territoriales. Les deux catégories partagent les mêmes obligations de gestion des risques (art. 21) et de notification (art. 23) ; elles se distinguent surtout par le régime de supervision (a priori pour les essentielles, a posteriori pour les importantes) et par le barème de sanctions. Attention : ces délais ne s'appliqueront qu'aux entités effectivement désignées dans le périmètre — pas à toute PME.

ReCyF : une préfiguration, pas une obligation

En amont de la loi, l'ANSSI a publié (en 2026, selon les sources spécialisées à recouper sur cyber.gouv.fr) le Référentiel Cyber France (ReCyF), qui traduit les exigences NIS2 en objectifs concrets : environ 20 objectifs de sécurité pour les entités essentielles, 15 pour les importantes. Tant que la loi n'est pas promulguée, ReCyF est une préfiguration utile pour se préparer, sans valeur contraignante formelle. L'ANSSI devrait rester l'autorité nationale désignée.

07 Les obligations sectorielles et l'assurance : d'autres délais à ne pas rater

Au-delà du RGPD et de NIS2, certains secteurs ajoutent leurs propres horloges, et l'assurance cyber en crée une supplémentaire, souvent ignorée. Ces régimes sont CUMULABLES : un même incident peut les déclencher en parallèle, chacun avec son texte, son destinataire et son délai propres.

Régime	Qui est concerné	Destinataire	Délai	Fondement
Santé	Établissements de santé, laboratoires de biologie médicale, radiothérapie, médico-social	Agence régionale de santé (ARS)	Sans délai (pas de durée chiffrée)	Art. L.1111-8-2 CSP + décret n°2022-715 du 27/04/2022 (Légifrance)
Finance (DORA)	Entités financières (banque, assurance, etc.)	ACPR (autorité désignée en France)	Notif. initiale 4 h après classification « majeur », au plus tard 24 h après détection ; rapport intermédiaire 72 h ; rapport final 1 mois	Règlement (UE) 2022/2554 (DORA) — à confirmer sur EUR-Lex
Assurance cyber (LOPMI)	Personnes morales et professionnels assurés	Autorités compétentes (dépôt de plainte pénale)	72 h après connaissance de l'atteinte	Art. L.12-10-1 Code des assurances, loi LOPMI (en vigueur depuis le 24/04/2023) — Légifrance

Deux horloges de 72 h qu'il ne faut JAMAIS confondre

Il existe en France deux délais de 72 h déclenchés par le même incident, mais totalement distincts. (1) RGPD art. 33 : NOTIFICATION à la CNIL d'une violation de données personnelles. (2) LOPMI art. L.12-10-1 : DÉPÔT DE PLAINTE PÉNALE auprès des autorités, condition sine qua non pour être indemnisé par votre assurance cyber. Textes différents, destinataires différents, finalités différentes. Dire « vous avez 72 h » sans préciser laquelle est juridiquement inexact — et peut coûter votre indemnisation.

- S'applique aux personnes morales et aux professionnels (pas aux particuliers).
- Le versement de l'indemnité pour une atteinte à un système de traitement automatisé de données (art. 323-1 à 323-3-1 du Code pénal) est subordonné au dépôt d'une plainte.
- Délai : au plus tard 72 h après la connaissance de l'atteinte par la victime.
- Conséquence pratique : intégrez le dépôt de plainte dans votre procédure d'incident dès la première heure — pas après la remédiation. Le portail 17Cyber (17cyber.gouv.fr) oriente vers le dépôt de plainte.

Note de prudence : les délais DORA et les montants NIS2 cités ici proviennent en partie de sources secondaires et doivent être recoupés avec les textes officiels (EUR-Lex, Légifrance) avant toute décision engageante. Vérifiez systématiquement le texte applicable à votre secteur et la date d'entrée en vigueur.

08 Notifier n'est pas porter plainte : les démarches cumulatives

L'idée fausse qui coûte cher : « j'ai signalé à l'ANSSI, donc c'est réglé »

Signaler un incident à l'ANSSI (ou à un CSIRT) ne vous dispense NI de la notification CNIL, NI du dépôt de plainte pénale, NI de la déclaration à votre ARS ou à votre assureur. Ce sont des démarches DISTINCTES et CUMULATIVES : chacune a sa logique, son destinataire, son délai et sa sanction en cas d'omission. En accomplir une ne libère d'aucune autre.

La confusion est d'autant plus dangereuse dans la santé : un établissement de santé victime d'un rançongiciel touchant des données patients peut devoir accomplir jusqu'à TROIS notifications parallèles — à l'ARS (incident grave de SI de santé, sans délai), à la CNIL (violation de données personnelles, 72 h) et, s'il entre dans le périmètre une fois NIS2 transposée, à l'ANSSI/CSIRT (24 h / 72 h / 1 mois) — auxquelles s'ajoutent le dépôt de plainte pénale (72 h, condition LOPMI) et la déclaration à l'assureur. Cinq logiques, cinq destinataires, plusieurs horloges qui tournent en même temps.

Événement déclencheur	Démarche	Destinataire	Délai
Violation de données personnelles avec risque pour les personnes	Notification (RGPD art. 33)	CNIL	72 h après prise de connaissance
Violation à risque ÉLEVÉ pour les personnes	Information (RGPD art. 34)	Personnes concernées	Dans les meilleurs délais
Incident significatif chez une entité NIS2 (si/quand transposée)	Alerte + notification + rapport	ANSSI / CSIRT national	24 h / 72 h / 1 mois
Incident grave de SI de santé	Signalement	ARS	Sans délai
Incident TIC majeur (secteur financier)	Notification DORA	ACPR	4 h / 24 h / 72 h / 1 mois
Infraction pénale (intrusion, extorsion...)	Dépôt de plainte	Autorités (police/gendarmerie, procureur) — via 17Cyber	72 h (condition d'indemnisation LOPMI)
Sinistre couvert par une police cyber	Déclaration de sinistre	Assureur	Délai contractuel (souvent 24-72 h)

Le réflexe opérationnel

Préparez à l'avance une checklist « qui prévenir » et attribuez chaque démarche à un responsable nommé (DPO pour la CNIL, direction/juridique pour la plainte et l'assureur, RSSI pour l'ANSSI/CSIRT). En pleine crise, personne n'a le temps de découvrir ces obligations. Cette cartographie se prépare avant l'incident, avec vos équipes ; Sedona.AI intervient en amont (ce que vous exposez sur Internet, la sensibilisation de vos équipes), et la réponse forensique elle-même relève de prestataires PRIS qualifiés par l'ANSSI et de votre assureur.

09 NIST SP 800-61 : du cycle en 4 phases (Rev.2) aux 6 fonctions (Rev.3)

Publié par le National Institute of Standards and Technology américain, le SP 800-61 (« Computer Security Incident Handling Guide ») est le référentiel technique de réponse à incident le plus cité au monde, y compris dans la littérature francophone. Point de vigilance immédiat : deux versions coexistent aujourd'hui, et elles ne décrivent pas la même structure. Confondre les deux — ou présenter « les 4 phases NIST » comme la doctrine en vigueur — est une erreur fréquente qu'un livre blanc sérieux se doit d'éviter.

Phase (Rev.2)	Ce qu'elle recouvre concrètement
1. Préparation	Politique et procédures, constitution du CSIRT/équipe de réponse, outillage (journalisation, EDR, sauvegardes), formation et exercices — tout ce qui se met en place AVANT l'incident.
2. Détection & analyse	Repérage des indicateurs, qualification et priorisation de l'incident, documentation des faits et de la chronologie.
3. Confinement, éradication & rétablissement	Isolement des systèmes touchés, suppression de la cause racine (comptes, persistance, malwares), puis restauration et remise en service contrôlée. Les trois activités sont regroupées dans UNE seule phase.
4. Activité post-incident	Retour d'expérience (REX), leçons apprises, mise à jour des procédures et des défenses.

La Rev.3, publiée en version finale en avril 2025, rompt explicitement avec ce découpage. Elle n'est plus structurée en « 4 phases » mais devient un profil communautaire (« CSF 2.0 Community Profile ») entièrement aligné sur les six fonctions du NIST Cybersecurity Framework 2.0 : Govern (gouverner), Identify (identifier), Protect (protéger), Detect (détecter), Respond (répondre), Recover (rétablir). Concrètement, le texte réorganise la réponse à incident autour de deux blocs : un premier couvrant la préparation et l'amélioration continue (Govern, Identify, Protect), un second couvrant l'incident proprement dit (Detect, Respond, Recover). Il n'existe donc plus de « quatre phases » au sens strict dans le document de référence actuel.

Honnêteté : ne pas confondre les deux versions

Parler des « 4 phases NIST » aujourd'hui décrit la Rev.2 (2012), toujours largement enseignée et reprise par les guides pratiques francophones — mais ce n'est plus le texte de référence en vigueur. La Rev.3 (finale, avril 2025) a abandonné ce cycle au profit des 6 fonctions du CSF 2.0. Les deux modèles restent utiles : la Rev.2 pour sa lisibilité opérationnelle, la Rev.3 pour son ancrage dans une gouvernance globale des risques. Mais il faut les distinguer, pas les fusionner. Source : NIST, SP 800-61 Rev.3 — csrc.nist.gov/pubs/sp/800/61/r3/final.

10 SANS PICERL et ISO/IEC 27035 : les alternatives opérationnelles

NIST n'est pas le seul cadre. Deux alternatives dominant en pratique : le modèle SANS PICERL, très prisé des équipes techniques pour sa granularité, et la norme ISO/IEC 27035, référence internationale qui s'articule naturellement avec un système de management de la sécurité ISO/IEC 27001. Ni l'un ni l'autre ne contredit NIST : ce sont des dialectes du même processus, avec des nuances de nomenclature qu'il faut connaître pour ne pas se tromper de vocabulaire en pleine crise.

1. Préparation (préparation) — équipe, procédures, outils et jeux d'entraînement en amont.
2. Identification — détecter et confirmer qu'un incident a bien lieu, en déterminer la portée initiale.

3. Containment (confinement) — endiguer la propagation, isoler ce qui doit l'être (à court puis à long terme).
4. Eradication (éradication) — supprimer la cause racine : malwares, comptes compromis, mécanismes de persistance.
5. Recovery (rétablissement) — restaurer les systèmes, revenir en production sous surveillance renforcée.
6. Lessons Learned (leçons apprises) — retour d'expérience formalisé pour renforcer la posture.

Cadre	Découpage	Nuance clé vs NIST
NIST SP 800-61 Rev.2	4 phases	Regroupe confinement + éradication + rétablissement dans UNE seule phase.
SANS PICERL	6 étapes	Sépare l'« Identification » de l'analyse, et scinde confinement / éradication / rétablissement en 3 étapes distinctes — d'où une granularité opérationnelle plus fine.
ISO/IEC 27035-1:2023	5 phases (Plan & Prepare, Detect, Assess, Respond, Learn Lessons)	Norme internationale générique, adaptable à toute taille d'organisation, complémentaire d'ISO/IEC 27001 ; remplace l'édition 2016. Ajoute une phase « Assess » (évaluation) explicite entre détection et réponse.

Le bon réflexe PME/ETI : choisir un cadre et s'y tenir

Le pire scénario, c'est l'improvisation en pleine attaque. Le choix du cadre importe moins que la discipline de s'y tenir. Une PME déjà engagée dans une démarche ISO 27001 gagnera à adopter ISO/IEC 27035 (continuité normative). Une équipe technique orientée SOC/CSIRT préférera souvent la granularité de SANS PICERL. NIST reste l'esperanto qui permet de dialoguer avec un prestataire ou un assureur. Fixez le vocabulaire commun AVANT l'incident, dans votre plan de réponse — pas pendant. Sources : SANS Institute (Incident Handler's Handbook) ; ISO/IEC 27035-1:2023, iso.org/standard/78973.html.

11 La doctrine ANSSI : réponse à incident technique vs gestion de crise

Pour une PME ou une ETI française, la référence utile n'est pas seulement technique : elle est aussi doctrinale, portée par l'ANSSI. La distinction structurante à intégrer est celle de deux échelles différentes. D'un côté, la réponse technique à un incident sur le système d'information — c'est le terrain des cadres NIST, SANS ou ISO. De l'autre, la gestion de crise cyber, qui se déclenche quand l'incident dépasse la DSI et engage la gouvernance, la continuité d'activité et la communication. Selon le CyberDico de l'ANSSI, un incident devient une « crise cyber » lorsqu'il met en péril les objectifs prioritaires de l'organisation, et se caractérise par la fulgurance des impacts, le manque de temps pour réagir et sa forte technicité.

Critère	Réponse technique à incident	Gestion de crise cyber (doctrine ANSSI)
Cadres de référence	NIST 800-61, SANS PICERL, ISO/IEC 27035	Guide ANSSI « Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique » (déc. 2021, MàJ mars 2023)
Périmètre	Le SI : endiguer, éradiquer, restaurer	L'organisation entière : décision, continuité, juridique, communication, RH
Déclencheur	Un incident détecté et qualifié	L'incident menace les objectifs prioritaires de l'entité
Pilotage	Équipe technique / CSIRT / PRIS	Cellule de crise décisionnelle mobilisant direction et métiers, distincte du niveau technique

- 1. Anticipation**
 Se préparer avant l'incident : constituer la cellule de crise, écrire les procédures, s'entraîner par des exercices. C'est la phase que l'ANSSI place au cœur du dispositif.
- 2. Alerte & qualification**
 Détecter, qualifier la gravité et décider — ou non — d'activer la cellule de crise et de basculer du mode « incident » au mode « crise ».
- 3. Gestion**
 Piloter la crise sur les plans opérationnel ET stratégique : maintien de la continuité d'activité, coordination technique, décisions de direction, communication interne et externe.
- 4. Sortie de crise**
 Remédiation, reconstruction durable du SI et retour d'expérience. Cette phase peut s'étendre sur plusieurs mois — la fin de la crise médiatique ne signifie pas la fin de la remédiation technique.

Le poids de l'anticipation : une position ANSSI, pas une statistique

L'ANSSI insiste sur le fait que la préparation en amont conditionne largement la réussite de la gestion de crise — certaines de ses synthèses avancent que « l'anticipation représente 70 % du succès ». À lire comme une position qualitative de l'ANSSI destinée à convaincre les dirigeants d'investir dans la préparation, et non comme une donnée mesurée par une étude indépendante. À retenir aussi : ne pas prêter à l'ANSSI une échelle de gravité type « P1-P4 » ou un RACI figé — ces éléments relèvent des pratiques ITSM/ITIL, pas de la doctrine ANSSI. Source : ANSSI, « Anticiper et gérer une crise cyber », cyber.gouv.fr/securisation/gestion-de-crise.

12 Lire l'attaque : IOC, TTP, kill chain et MITRE ATT&CK

Répondre efficacement suppose de savoir lire l'attaque, et pas seulement d'en ramasser les débris. Deux niveaux de lecture coexistent. Les IOC (indicateurs de compromission) sont, selon le CyberDico de l'ANSSI, « une combinaison d'informations techniques et contextuelles représentatives d'une manifestation ou d'une tentative de compromission » : adresses IP, hachages de fichiers, noms de domaine. Les TTP (tactiques, techniques et procédures) décrivent, elles, le comportement de l'attaquant — sa façon de faire. La différence est décisive pour l'anticipation.

- IOC — volatils. Un attaquant peut changer ses adresses IP, ses domaines ou ses hachages en quelques minutes. Précieux pour la détection immédiate, mais périmés vite.
- TTP — stables. Modifier sa manière d'opérer (outils, enchaînements, techniques) demande des mois, voire des années à un adversaire. C'est donc un signal bien plus significatif et durable.
- Conséquence : le renseignement fondé sur les TTP anticipe mieux les menaces émergentes que la simple chasse aux IOC, qui reste réactive.

Critère	Cyber Kill Chain (Lockheed Martin)	MITRE ATT&CK
Nature	Modèle linéaire, vision haut niveau	Base de connaissances des comportements adverses observés en conditions réelles
Structure	Étapes séquentielles, de la reconnaissance à l'atteinte de l'objectif	Tactiques (les objectifs de l'attaquant) × techniques et sous-techniques (les méthodes)
Usage	Comprendre la progression globale d'une attaque, communiquer avec la direction	Cartographier précisément CE que l'attaquant a fait, à chaque étape
Granularité	Faible (macro)	Élevée (technique par technique)

L'usage concret : cartographier l'intrusion pour bien éradiquer

En réponse à incident, projeter les faits observés sur la kill chain donne la vue d'ensemble ; les rattacher aux techniques MITRE ATT&CK révèle l'étendue réelle de l'intrusion — points d'entrée, déplacements latéraux, persistance installées, exfiltration. Cette cartographie est ce qui distingue une éradication complète d'un nettoyage partiel : tant que toutes les techniques employées ne sont pas identifiées et neutralisées, l'attaquant peut revenir. ATT&CK complète la kill chain, il ne la remplace pas. Sources : MITRE ATT&CK (attack.mitre.org) ; CyberDico ANSSI (cyber.gouv.fr/cyberdico).

Comment Sedona AI intervient — en amont, honnêtement

Sedona AI n'est pas prestataire de réponse à incident ni de forensic. En cas d'attaque avérée, orientez-vous vers un prestataire qualifié PRIS par l'ANSSI et vers votre assureur cyber. Là où Sedona agit, c'est en amont : voir ce que votre organisation expose sur Internet (Sedona Radar l'analyse, sans certifier), sensibiliser vos équipes et simuler du phishing. La préparation de crise elle-même — plan de réponse, exercices — se construit avec vos équipes et les guides publics de l'ANSSI.

13 Les 24 premières heures : détecter, qualifier, alerter

La fenêtre des premières heures est celle où l'on perd — ou l'on sauve — le plus. Chaque geste réflexe, chaque trace préservée, chaque appel passé au bon moment pèse sur le coût final et sur la capacité à reconstruire proprement. L'objectif de cette phase n'est pas de « réparer » : c'est de reconnaître, qualifier, contenir la panique et enclencher les bons circuits — techniques, humains et légaux — sans détruire ce qui permettra demain de comprendre et de prouver.

3,87 M\$ vs 5,01 M\$

Coût moyen d'une brèche selon qu'elle est contenue en moins de 200 jours ou au-delà (+29 %) — la vitesse de réaction est un levier de coût direct

IBM, Cost of a Data Breach Report 2025

1 Reconnaître les signaux

Fichiers chiffrés ou renommés, message de rançon, comptes verrouillés, alertes EDR/antivirus en rafale, connexions ou transferts de données inhabituels, ralentissements anormaux, e-mails sortants suspects. Ne jamais minimiser un signal faible : le premier réflexe humain est de chercher une explication banale — c'est précisément ce que l'attaquant exploite.

2 Qualifier la gravité

Distinguer l'incident (événement ayant ou pouvant avoir un impact négatif sur la sécurité du SI, définition ANSSI/CyberDico) de la crise cyber, qui met en péril les objectifs prioritaires de l'organisation et se caractérise par la fulgurance des impacts, le manque de temps et la forte technicité (guide ANSSI « Crise d'origine cyber »). Cartographier ce qui est touché, ce qui est encore sain, ce qui est vital.

3 Journaliser dès la première minute

Ouvrir une main courante horodatée : qui a fait quoi, quand, sur quel système, sur quelle décision. Chaque action datée à la minute. Ce journal est à la fois l'outil de pilotage de la cellule et le socle de la valeur probante ultérieure.

4 Activer la cellule de crise

Mobiliser en parallèle la cellule décisionnelle (direction, métiers) et la cellule technique (RSSI/DSI, prestataire). Désigner un pilote unique et un point de collecte d'information. Basculer sur des canaux de communication de secours si la messagerie est potentiellement compromise.

5 Préserver les traces

Isoler les systèmes du réseau sans les éteindre (voir réflexes CERT-FR ci-dessous). Sauvegarder les journaux avant qu'ils ne tournent ou soient effacés. Ne rien « nettoyer » avant d'avoir figé une image de l'état compromis.

6 Passer les premiers appels

17Cyber (17cyber.gouv.fr, guichet unique public 24/7) pour faire le point et vous orienter ; un prestataire de réponse aux incidents qualifié PRIS par l'ANSSI ; l'assureur cyber (activation de la garantie et de l'assistance) ; le DPO si des données personnelles sont concernées.

7 Déclencher les horloges légales

Noter l'heure exacte de la prise de connaissance : elle fait courir le compteur de 72 h de notification CNIL (RGPD art. 33) si des données personnelles sont en jeu, et le compteur de 72 h de dépôt de plainte conditionnant l'indemnisation assurantielle (LOPMI). Deux horloges distinctes, même point de départ.

Les réflexes CERT-FR en cas d'intrusion

Ne pas éteindre brutalement les machines : couper l'alimentation détruit la mémoire vive et des traces volatiles précieuses. Débrancher du réseau (câble/Wi-Fi) plutôt qu'éteindre, pour contenir sans détruire. Ne pas alerter l'attaquant : éviter de réinitialiser massivement les mots de passe ou de communiquer sur les canaux potentiellement compromis avant d'avoir préparé la remédiation — un adversaire qui se sait repéré accélère, verrouille ou détruit. Préserver et sauvegarder les journaux (systèmes, pare-feu, proxy, AD) avant toute manipulation. Source : CERT-FR, « Les bons réflexes en cas d'intrusion sur un système d'information ».

☐ Heure exacte de prise de connaissance notée et figée (départ des compteurs légaux)

☐ Main courante horodatée ouverte, un responsable désigné pour la tenir

☐ Systèmes touchés isolés du réseau sans extinction brutale

☐ Journaux (AD, pare-feu, proxy, EDR, messagerie) sauvegardés hors ligne

☐ Cellule de crise activée (décisionnelle + technique), pilote unique désigné

☐ Canal de communication de secours établi (hors SI potentiellement compromis)

☐ 17Cyber contacté et analyse de la situation lancée

☐ Prestataire PRIS et assureur cyber alertés

☐ DPO informé, pré-évaluation du risque pour les personnes engagée

- ☐ Décision explicite : ne pas payer, ne pas négocier seul, ne pas improviser sur les réseaux sociaux

Deux compteurs de 72 h à ne pas confondre

Le RGPD (art. 33) impose de notifier la CNIL dans les 72 h suivant la prise de connaissance d'une violation de données personnelles à risque. La LOPMI (art. L.12-10-1 du Code des assurances) subordonne l'indemnisation d'un sinistre cyber au dépôt d'une plainte pénale dans les 72 h suivant la connaissance de l'atteinte. Même durée, même déclencheur — mais destinataires, textes et finalités différents. Traiter les deux en parallèle, ne jamais dire « on a 72 h » sans préciser laquelle.

14 Confiner, éradiquer, remédier, reconstruire

Le cœur technique de la réponse suit une progression que l'on retrouve dans tous les référentiels (NIST SP 800-61, SANS PICERL, ISO/IEC 27035) : contenir la propagation, supprimer la cause racine, remettre sur une base saine, reconstruire durablement. La tentation permanente est d'aller trop vite — restaurer pour « rouvrir la boutique » — au risque de réinfecter des systèmes propres à partir de sauvegardes elles-mêmes compromises, ou de détruire les preuves nécessaires à l'enquête et à l'assurance.

1 Confiner

Isoler chirurgicalement : segmenter le réseau, couper sélectivement les accès des machines compromises, désactiver les comptes suspects, bloquer les flux vers les adresses de commande-et-contrôle. Objectif : arrêter la propagation sans tout paralyser inutilement, et sans détruire les traces (débrancher, pas effacer).

2 Éradiquer

Identifier et supprimer la cause racine : porte d'entrée initiale, comptes détournés, persistances (tâches planifiées, services, clés de registre, webshells), portes dérobées. Éradiquer un symptôme sans traiter la voie d'accès garantit une réinfection. C'est l'étape qui exige le plus souvent un prestataire spécialisé.

3 Remédier

Corriger durablement : appliquer les correctifs, renforcer l'authentification (MFA), rotation complète des secrets et mots de passe, durcissement des configurations, réduction de la surface d'attaque exposée. La remédiation vise à ce que la même attaque ne fonctionne plus.

4 Reconstruire sur base saine

Restaurer depuis des sauvegardes vérifiées et non compromises, idéalement hors ligne ou immuables. Reconstruire les systèmes critiques plutôt que « nettoyer » l'existant douteux. Réintégrer progressivement au réseau sous surveillance renforcée, en validant l'absence de persistance avant chaque remise en service.

Vos sauvegardes sont peut-être déjà compromises

Les attaquants ciblent délibérément les sauvegardes avant de déclencher le chiffrement, pour couper l'échappatoire. Avant toute restauration : vérifier l'intégrité et la date des sauvegardes, s'assurer qu'elles sont antérieures à la compromission initiale (souvent bien plus ancienne que la détection), et restaurer sur un environnement isolé avant réintégration. Une restauration hâtive depuis une sauvegarde infectée relance l'incident à zéro.

Préserver la valeur probante (bonne pratique à faire valider par un juriste)

Conserver les journaux horodatés, tracer chaque manipulation, figer des copies de l'état compromis, et — selon les enjeux — envisager un constat d'huissier sont des pratiques généralement admises pour renforcer la valeur probante en cas de plainte, de contentieux ou de discussion avec l'assureur. Ce ne sont PAS des obligations légales chiffrées : leur pertinence et leurs modalités exactes doivent être arbitrées avec votre conseil juridique et, le cas échéant, votre prestataire PRIS.

241 jours (181 + 60)

Délai moyen MONDIAL pour identifier puis contenir une violation en 2025 (le plus bas en 9 ans) — moyenne toutes tailles/secteurs, pas un chiffre France ni PME

IBM, Cost of a Data Breach Report 2025

Dernier point à intégrer dans la communication et le pilotage : la remédiation complète ne se compte pas en heures mais en semaines, voire en mois. La sortie de crise (au sens du guide ANSSI de gestion de crise) englobe la reconstruction durable, le retour d'expérience et le suivi des mesures — bien au-delà du simple redémarrage des services. Annoncer un « retour à la normale » prématuré est l'une des erreurs les plus coûteuses en crédibilité.

15 Piloter la crise : cellule, rôles et communication

Une crise cyber n'est pas qu'un problème technique : c'est un problème de décision sous pression, d'information incomplète et de temps compté. La doctrine ANSSI de gestion de crise recommande de distinguer nettement deux niveaux : une cellule décisionnelle (stratégique), qui arbitre et engage l'organisation, et une cellule opérationnelle/technique, qui investigate et remédie. Les mélanger, c'est paralyser les techniciens par des demandes de reporting permanent, et priver la direction d'une vision claire.

Fonction	Rôle type dans la crise
Direction générale	Arbitrages stratégiques, engagement de l'organisation, décision de non-paiement, validation de la communication externe, relations avec les parties prenantes majeures
RSSI / DSI	Pilotage de la cellule technique, coordination de l'investigation et de la remédiation, interface avec le prestataire PRIS, reporting synthétique à la direction
DPO	Évaluation du risque pour les personnes concernées, préparation et dépôt de la notification CNIL (art. 33) et, si risque élevé, information des personnes (art. 34)
Juridique	Dépôt de plainte, gestion des obligations contractuelles et réglementaires, relation avec l'assureur, sécurisation de la valeur probante
Communication	Messages internes et externes, relation médias, cohérence et cadencement, prévention des rumeurs et des fuites
RH	Information et soutien des salariés, gestion des astreintes et de la fatigue, dimension sociale et managériale de la crise

- **Factuel** : ne communiquer que ce qui est établi, distinguer clairement le confirmé de l'hypothétique
- **Cadencé** : rythmer les points d'information (interne, clients, partenaires, régulateurs, médias) plutôt que de subir l'événement
- **Ne pas sur-promettre** : éviter d'annoncer un « retour à la normale » ou une « absence de fuite » avant confirmation — un démenti forcé détruit la confiance
- **Cohérent** : une seule voix, des messages alignés entre les canaux et les publics
- **Anticipé** : les personnes concernées et les régulateurs doivent l'apprendre de vous, pas de la presse ou de l'attaquant

Séparer le stratégique de l'opérationnel

L'ANSSI insiste sur la distinction entre la cellule de crise décisionnelle (direction, métiers, juridique, communication) et le niveau technique (réponse à incident, investigation numérique). Le pilote de crise fait le pont : il protège les techniciens des sollicitations permanentes et alimente la direction en information synthétisée. Attention à ne pas attribuer à l'ANSSI un RACI détaillé ou une échelle de gravité « P1-P4 » : ces classifications relèvent des pratiques ITSM courantes, pas d'un standard réglementaire français vérifié.

Gérer la pression temporelle et la fatigue est une responsabilité de pilotage à part entière. Une crise structurante s'étale sur des jours ; les mêmes personnes ne peuvent pas tenir 72 h d'affilée sans dégrader leur jugement. Organiser des relais et des astreintes, imposer des pauses, prévoir un back-up pour chaque rôle clé, et tenir un journal partagé pour que la relève reprenne sans perte d'information : ce sont des conditions de la qualité des décisions, pas du confort. L'anticipation — plans testés, exercices annuels, contacts pré-établis — est, selon l'ANSSI, le principal facteur de réussite d'une gestion de crise.

16 Rançongiciel : payer ou ne pas payer ?

Position officielle : ne pas payer

L'ANSSI et Cybermalveillance.gouv.fr recommandent de ne pas payer la rançon. Payer ne garantit ni la récupération des données, ni l'absence de publication, ni l'immunité contre une nouvelle attaque — et alimente directement l'écosystème criminel. La décision, si elle est malgré tout posée, relève de la direction générale, jamais d'un arbitrage technique isolé, et doit se prendre avec le prestataire, l'assureur et le conseil juridique.

~50 %

Ordre de grandeur du taux de récupération effective des données après paiement ; à l'inverse, une part importante des victimes ayant payé ne récupèrent pas correctement leurs données (ordres de grandeur convergents, études distinctes, confiance moyenne)

ANSSI / Cybermalveillance.gouv.fr ; sources secondaires (Solutions Numériques, Le Monde Informatique) — à recouper

64 %

Part des victimes qui refusent désormais de payer la rançon (contre 50 % deux ans plus tôt) ; paiement médian tombé à 115 000 \$

Verizon, 2025 Data Breach Investigations Report

- Aucune garantie de récupération : une part importante des paiements n'aboutit pas à une restauration effective, outils de déchiffrement souvent défaillants
- Risque de double extorsion : les données exfiltrées peuvent être publiées ou revendues malgré le paiement
- Financement de l'écosystème criminel : chaque rançon payée finance et professionnalise les groupes d'attaquants
- Re-ciblage : les victimes qui paient sont identifiées comme solvables et parfois attaquées de nouveau
- Tendance de fond : le refus de payer devient majoritaire (64 % selon Verizon), signe que la non-négociation est une posture viable

Le glissement tactique observé par l'ANSSI en 2025 renforce ce raisonnement : le rançongiciel « classique » avec chiffrement recule (128 compromissions signalées, contre 141 en 2024) tandis que l'exfiltration de données pure explose (196 incidents, +51 %). Autrement dit, payer pour « récupérer une clé de déchiffrement » ne règle en rien le vol de données déjà parti. Enfin, la LOPMI conditionne l'indemnisation assurantielle d'un sinistre cyber au dépôt d'une plainte pénale dans les 72 h suivant la connaissance de l'atteinte (art. L.12-10-1 du Code des assurances) : la décision sur la rançon doit donc s'articuler étroitement avec la plainte et avec l'assureur, jamais en vase clos.

17 Vos modèles prêts à l'emploi : check-lists et documents types

☐ Date et heure exactes de l'événement ou de l'action (à la minute)

☐ Auteur de l'action (nom, fonction)

☐ Système / périmètre concerné

☐ Nature de l'action ou de la constatation (fait, décision, communication)

☐ Décision prise et par qui (traçabilité des arbitrages)

☐ Preuve ou pièce rattachée (capture, export de log, référence)

☐ Impact observé et suites à donner

Contact	Coordonnées / accès
17Cyber (guichet unique 24/7)	17cyber.gouv.fr — orientation et mise en relation
Prestataire de réponse à incident (PRIS ANSSI)	Liste à jour sur cyber.gouv.fr — contractualiser en amont si possible
Assureur cyber	N° de police + ligne d'assistance 24/7 (activer la garantie ; dépôt de plainte sous 72 h côté LOPMI)
DPO	Nom + contact direct (pilote de la notification CNIL)
CNIL	notifications.cnil.fr (violation de données personnelles, art. 33)
Dépôt de plainte	Police / gendarmerie / procureur — plainte pénale sous 72 h (LOPMI)
Direction générale + cellule de crise	Coordonnées personnelles + canal de secours hors SI

Champ	Contenu attendu
Nature de la violation	Type d'incident (confidentialité, intégrité, disponibilité) et circonstances
Catégories et volume	Catégories de personnes et de données concernées, nombre approximatif
Conséquences probables	Risques pour les droits et libertés des personnes
Mesures prises	Mesures de remédiation et d'atténuation engagées ou prévues
Coordonnées DPO	Point de contact pour l'autorité
Motif du retard (si > 72 h)	Justification obligatoire en cas de dépassement du délai

- Alerte précoce — sous 24 h après connaissance de l'incident significatif : signalement initial minimal (nature, soupçon d'origine malveillante, impact transfrontalier éventuel)
- Notification d'incident — sous 72 h : évaluation initiale de gravité et d'impact, indicateurs de compromission connus
- Rapport intermédiaire — si l'incident est toujours en cours, sur demande de l'autorité/CSIRT
- Rapport final — sous 1 mois : cause racine, mesures d'atténuation, impact constaté

☐ Des données personnelles sont-elles concernées ? → Si oui et s'il existe un risque pour les personnes : notifier la CNIL sous 72 h (RGPD art. 33)

☐ Le risque pour les personnes est-il ÉLEVÉ ? → Si oui : informer aussi directement les personnes concernées (RGPD art. 34)

☐ L'entité entre-t-elle dans le périmètre NIS2 (essentielle/importante) ET l'incident est-il significatif ? → Anticiper le triptyque 24 h / 72 h / 1 mois (sous réserve de la transposition française, voir ci-dessous)

☐ Établissement de santé ? → Signalement « sans délai » à l'ARS pour incident grave de SI de santé

☐ Dans tous les cas : plainte pénale (condition d'indemnisation assurantielle sous 72 h, LOPMI)

☐ Rappel : ces démarches sont cumulatives — signaler à l'ANSSI n'exonère ni de la plainte, ni de la notification CNIL

NIS2 en France : statut non finalisé au 14/10/2026

Les délais 24 h / 72 h / 1 mois sont ceux de la directive européenne (UE) 2022/2555, art. 23. Mais la loi française de transposition (« loi Résilience », transposant NIS2, REC et la directive (UE) 2022/2556, volet DORA) n'est PAS promulguée à la date de rédaction : adoptée en 1re lecture au Sénat le 12 mars 2025, elle n'a pas été votée par l'Assemblée nationale, et la Commission européenne a saisi la CJUE contre la France le 8 juillet 2026 pour défaut de transposition. Ne présentez pas ces obligations comme du droit français en vigueur : elles ne s'appliqueront qu'aux ~15 000 entités désignées essentielles/importantes une fois la loi votée et les décrets publiés. Vérifiez le statut à jour sur cyber.gouv.fr au moment de votre lecture.

Des points de départ, pas des documents prêts à signer

Ces trames sont des modèles à adapter à votre contexte et à faire relire par un juriste avant tout usage engageant. Pour les procédures pas-à-pas selon le type d'incident (rançongiciel, piratage de compte, violation de données...), appuyez-vous sur les fiches officielles « Que faire en cas de... » de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), mises à jour et pensées pour les TPE/PME. Sedona.AI n'est pas prestataire de réponse à incident ni forensic : son rôle se limite à l'amont (voir ce que vous exposez sur Internet, sensibiliser vos équipes) ; le moment venu, orientez-vous vers un prestataire PRIS qualifié et votre assureur.

18 Spécificités PME/ETI : faire face avec des moyens limités

Tout ce qui précède — qualification, confinement, éradication, communication de crise — suppose implicitement une organisation outillée. La réalité d'une PME ou d'une ETI est différente : pas d'équipe SOC, pas de CERT interne, un budget cyber contraint, et une dépendance forte à un ou deux prestataires IT externes qui gèrent aussi l'infrastructure attaquée. Ce n'est pas une excuse pour renoncer : c'est une invitation à concentrer l'effort sur un socle réduit mais réellement tenu, plutôt que sur un dispositif ambitieux jamais testé. L'écart de vulnérabilité est documenté : chez les PME, un rançongiciel est présent dans 88 % des violations analysées, contre 39 % pour les grandes entreprises, et 43 % des PME n'ont aucun collaborateur dédié à la cybersécurité (Verizon, 2025 Data Breach Investigations Report).

65 %

des TPE-PME concernées n'ont aucune procédure de réaction à incident formalisée
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), Rapport d'activité 2025

44 %

des dirigeants de PME se disent conscients d'être très exposés à la menace numérique (vs 38 % un an plus tôt)

Baromètre maturité cyber TPE-PME ([Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)) — à recouper

6 sur 10

dirigeants déclarent ne pas savoir évaluer les conséquences d'une cyberattaque, et 80 % ne se sentent pas suffisamment préparés

Cybermalveillance.gouv.fr, Rapport d'activité 2025

Trois choses à ne pas confondre

Se sentir « équipé » (antivirus, pare-feu, sauvegardes) n'est pas être « préparé » (plan écrit, rôles désignés, sauvegardes testées), et être « préparé » n'est pas la même chose qu'avoir « vécu » un incident. La prise de conscience progresse (44 % en 2025 contre 38 % en 2024) mais reste très en avance sur la préparation réelle : 65 % n'ont toujours aucune procédure de réaction et 6 dirigeants sur 10 s'avouent incapables d'évaluer les conséquences d'une attaque. C'est précisément dans cet écart que l'incident fait le plus de dégâts.

- Sauvegardes 3-2-1 réellement testées : 3 copies, sur 2 supports différents, dont 1 hors ligne / hors site (déconnectée du réseau pour survivre à un rançongiciel) — et une restauration d'essai vérifiée, pas seulement une sauvegarde qui « tourne ».
- MFA (double authentification) sur les accès critiques : messagerie, VPN, accès administrateur, outils cloud — le vecteur d'intrusion initial dominant reste le phishing, dans environ 60 % des attaques (ENISA, Threat Landscape 2025).
- Un plan de réaction minimal écrit : qui fait quoi dans les premières heures, comment isoler une machine, qui décide de couper le réseau — une page suffit pour commencer.
- Un annuaire de crise pré-établi et accessible hors du SI : prestataire IT, assureur cyber (numéro d'astreinte), 17Cyber, CNIL, un contact PRIS identifié à l'avance.
- La formalisation de ce que fait — et ne fait pas — le prestataire IT externe en cas d'incident : est-il joignable 24/7 ? sait-il faire de la réponse à incident ou seulement de l'exploitation ?

19 À qui s'adresser : 17Cyber, PRIS, CERT-FR et CSIRT territoriaux

L'écosystème de secours français est gradué selon la taille de la structure et la gravité de l'incident. Une PME sans compétence interne commence par le guichet unique public ; une ETI avec un SI complexe et un incident avéré s'oriente vers un prestataire qualifié ; les incidents majeurs et les entités critiques relèvent du CERT-FR national. Ces recours ne s'excluent pas : 17Cyber sert souvent de premier aiguillage vers les autres.

Interlocuteur	Pour qui / quand	Ce qu'il apporte
17Cyber (17cyber.gouv.fr)	Particuliers, TPE/PME, associations, collectivités — premier réflexe, 24h/24 et 7j/7	Questionnaire interactif de qualification (une cinquantaine de cas types, dont le rançongiciel), orientation, mise en relation avec des prestataires, aide au dépôt de plainte. Guichet unique lancé le 17 décembre 2024.
Prestataires PRIS qualifiés ANSSI	PME/ETI avec SI complexe, incident avéré nécessitant une réponse professionnelle	5 activités qualifiables : recherche d'indicateurs de compromission (IOC), investigation numérique (forensic), analyse de codes malveillants, pilotage/coordination des investigations, gestion de crise d'origine cyber (référentiel v3.0, déc. 2024, niveaux substantiel et élevé).
CSIRT territoriaux	Structures de taille moyenne, collectivités et ETI à l'échelle régionale	Appui de proximité et coordination régionale, relais entre la victime et le niveau national.
CERT-FR	Incidents majeurs, entités critiques / d'importance vitale	Coordination nationale, alerte, appui aux incidents structurants.

La liste PRIS publique n'est pas exhaustive

Seuls les prestataires ayant accepté d'être publiés figurent sur la liste officielle ANSSI ; c'est donc un sous-ensemble, et elle évolue. Vérifiez toujours la liste à jour sur cyber.gouv.fr avant de contractualiser. À titre indicatif seulement (liste non exhaustive et évolutive, à reconfirmer) : Almond, Capgemini, Intrinsec, Lexfo, Mandiant France, Orange Cyberdefense, Synacktiv, Thales, Wavestone.

La position de Sedona, en toute transparence

Sedona n'est pas prestataire de réponse à incident ni de forensic. En cas d'incident avéré, le bon réflexe est d'activer votre assureur cyber et un prestataire PRIS qualifié par l'ANSSI (et 17Cyber comme premier aiguillage). Ce que Sedona apporte se situe en amont : réduire la surface d'attaque exposée et sensibiliser les équipes — ce sur quoi porte la dernière partie de ce guide.

20 L'assurance cyber : conditions, réflexes et pièges

L'assurance cyber ne remplace pas la sécurité, mais elle finance la réponse au moment où la trésorerie est sous tension. Encore faut-il connaître son contrat avant l'incident, et non le découvrir pendant. Un point de droit français est décisif et souvent ignoré : depuis la loi LOPMI, l'indemnisation d'un sinistre cyber est conditionnée à un dépôt de plainte rapide.

- Les frais d'expertise et d'investigation numérique (forensic) et l'assistance à la gestion de crise.
- Les frais de notification (CNIL, personnes concernées) et l'accompagnement juridique associé.
- Les pertes d'exploitation liées à l'interruption d'activité.
- Selon les contrats, la prise en charge d'une éventuelle rançon — clause à examiner de près, la position officielle ANSSI/Cybermalveillance restant de ne pas payer.

Deux délais de 72 h à ne surtout pas confondre

Un même incident peut déclencher deux obligations distinctes de 72 heures, avec des destinataires et des textes différents. Les confondre — ou n'en respecter qu'une — peut coûter à la fois une sanction et l'indemnisation.

Obligation	Délai exact	Auprès de qui	Base légale
Notifier une violation de données personnelles (si risque pour les personnes)	72 h après en avoir pris connaissance (week-ends et jours fériés compris ; notification initiale incomplète admise, à compléter ensuite)	CNIL	RGPD, article 33
Déposer plainte — condition de la prise en charge assurantielle du sinistre cyber	au plus tard 72 h après la connaissance de l'atteinte (personnes morales et professionnels)	Services de police / gendarmerie (autorités compétentes)	LOPMI, article L.12-10-1 du Code des assurances (en vigueur depuis le 24 avril 2023)

- Déclarer vite : la plupart des contrats imposent une déclaration sans délai et prévoient un numéro d'astreinte 24/7 — repérez-le et affichez-le dans l'annuaire de crise avant l'incident.
- Conserver les preuves : ne pas éteindre ni reformater précipitamment les machines touchées ; préserver logs et traces conditionne à la fois l'investigation, la plainte et l'indemnisation.
- Vérifier les prestataires imposés : de nombreux contrats obligent à passer par un panel d'experts désignés par l'assureur — appeler « son » informaticien avant l'assureur peut faire tomber la garantie.
- Lire les exclusions fréquentes : défaut de mesures de sécurité de base (MFA, sauvegardes, correctifs), négligence, actes étatiques/« guerre », rançon selon les juridictions.
- Faire l'exercice à froid : sortir le contrat une fois par an et vérifier que le numéro d'astreinte, le périmètre et les plafonds correspondent toujours à l'entreprise réelle.

21 Anticiper : plan de réponse, sauvegardes et exercices de crise

C'est le cœur du message de ce guide : on ne gère bien que ce qu'on a préparé. L'ANSSI le formule sans détour — l'anticipation représente l'essentiel du succès d'une gestion de crise (position qualitative de l'ANSSI, et non une mesure statistique). Pour une PME, préparer ne veut pas dire

produire un classeur de 200 pages : cela veut dire écrire l'essentiel, désigner les responsables et l'avoir répété au moins une fois.

1 Écrire un plan de réponse à incident

Un document court et opérationnel : critères de déclenchement, premiers gestes (isoler, ne pas éteindre, préserver les preuves), arbre de décision (qui décide de couper le réseau), et les obligations de notification (CNIL sous 72 h, plainte LOPMI sous 72 h).

2 Désigner les rôles à l'avance

Qui pilote la crise, qui parle aux clients et aux médias, qui gère le juridique et le RGPD, qui coordonne avec le prestataire IT et l'assureur. Nommer des personnes et leurs suppléants, pas des fonctions abstraites.

3 Tester les sauvegardes, pas seulement les faire

Vérifier régulièrement qu'une restauration fonctionne réellement, à partir d'une copie hors ligne/hors site (3-2-1). Une sauvegarde jamais restaurée est une hypothèse, pas une garantie.

4 Pré-établir l'annuaire de crise

Prestataire IT, PRIS, assureur (astreinte), 17Cyber, CNIL, direction, communication — sur un support accessible hors du SI (papier, téléphone personnel), car la messagerie peut être la première victime.

5 S'exercer au moins une fois par an

L'ANSSI recommande a minima un exercice de gestion de crise cyber par an. Pour débiter, privilégier un exercice sur table planifié — de l'ordre de 2 à 3 heures de jeu pour environ 6 semaines de préparation — plutôt qu'une simulation impromptue plus lourde (jusqu'à 2 jours).

☐ Critères de déclenchement et premier point de contact interne

☐ Gestes réflexes des 60 premières minutes (isoler, préserver, ne pas payer dans la précipitation)

☐ Rôles nommés + suppléants

☐ Annuaire de crise hors ligne

☐ Rappel des délais légaux : plainte 72 h (LOPMI) et notification CNIL 72 h (RGPD art. 33)

☐ Procédure et test de restauration des sauvegardes 3-2-1

☐ Date du dernier exercice réalisé

Sur le coût d'un exercice

Des sources secondaires spécialisées évoquent une fourchette indicative de l'ordre de 3 000 à 8 000 € pour un exercice sur table animé par un prestataire, pour une PME. À prendre comme un ordre de grandeur de confiance basse : ce n'est pas un chiffre officiel de l'ANSSI, et le coût réel dépend du périmètre et de l'animation.

Là où Sedona aide, honnêtement

L'amont est précisément le terrain de Sedona : sensibiliser vos équipes (des formations, des simulations de phishing) et voir ce que votre organisation expose sur Internet pour le réduire durablement. Pas de plan de réponse ni d'exercice de crise, pas de réponse à incident ni de forensic — mais ce qui diminue la probabilité et l'ampleur du prochain incident.

22 Retour d'expérience : transformer l'incident en résilience

Un incident se termine mal quand on se contente de « remettre en service ». Il devient utile quand on en tire, à froid, les enseignements qui empêcheront le suivant. Cette phase de retour d'expérience (REX) porte des noms selon les référentiels — Post-Incident Activity chez NIST (SP 800-61 Rev.2 ; la Rev.3 finalisée en avril 2025 l'intègre désormais aux fonctions du CSF 2.0), Lessons Learned dans le modèle SANS PICERL, Learn Lessons dans l'ISO/IEC 27035-1:2023 — mais l'idée est constante : boucler le cycle.

1 Réunir un REX à froid

Quelques jours à quelques semaines après la sortie de crise, une fois la pression retombée, réunir les acteurs internes et externes pour reconstituer la chronologie factuelle des événements et des décisions.

2 Analyser la cause racine

Remonter au-delà du symptôme (« un poste chiffré ») jusqu'à la cause première (accès sans MFA, correctif manquant, compte prestataire compromis) — le vecteur d'intrusion initial dominant restant le phishing, dans environ 60 % des attaques (ENISA, Threat Landscape 2025).

3 Corriger les vulnérabilités exploitées

Refermer concrètement la porte d'entrée : correctifs, MFA généralisé, révocation des accès inutiles, durcissement des services exposés — et vérifier que la correction tient dans le temps.

4 Mettre à jour le plan et les procédures

Reporter dans le plan de réponse ce qui a manqué (un contact absent, une décision floue, une sauvegarde non restaurable) et affiner les playbooks à partir du cas réellement vécu.

Un REX sans culture du blâme

Le retour d'expérience ne sert à rien s'il devient un tribunal. On cherche les causes systémiques, pas un coupable : c'est la seule manière d'obtenir des acteurs qu'ils racontent honnêtement ce qui s'est passé — condition d'une analyse de cause racine juste, et donc d'une correction efficace.

- Des playbooks affinés, testés contre un cas réel plutôt que théorique.
- Des indicateurs concrets : les brèches contenues en moins de 200 jours coûtent en moyenne 3,87 M\$ contre 5,01 M\$ au-delà (IBM, Cost of a Data Breach Report 2025, moyenne mondiale) — la vitesse de réaction, améliorée par le REX, a une valeur mesurable.
- Une décision de rançon documentée : 64 % des victimes refusent désormais de payer (Verizon, 2025 Data Breach Investigations Report), conformément à la position officielle ANSSI/Cybermalveillance.
- Un exercice de crise reprogrammé, intégrant le scénario réellement subi.

Reste une évidence stratégique : entre deux attaques, on ne contrôle ni la motivation de l'attaquant, ni le prochain jour zéro. Le seul levier réellement sous votre main, c'est la surface d'attaque que vous exposez — les services publiés, les accès oubliés, les fuites de données, les erreurs de configuration visibles de l'extérieur. La réduire de façon régulière, c'est diminuer à la fois la probabilité et l'ampleur du prochain incident. C'est exactement l'objet de ce guide, et le terrain sur lequel Sedona intervient.

§ Sources

1. ANSSI / CERT-FR — Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002) — <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf>
2. ANSSI — CyberDico (glossaire officiel : incident, IOC, crise) — <https://cyber.gouv.fr/cyberdico/>
3. ANSSI — Anticiper et gérer une crise cyber (doctrine gestion de crise) — <https://cyber.gouv.fr/securisation/gestion-de-crise/anticiper-gerer-une-crise-cyber/>
4. ANSSI — Prestataires de réponse aux incidents de sécurité (PRIS) — <https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/services-de-securite-evalue/solutions-en-cours-de-qualification/pris/>
5. ANSSI — Organiser un exercice de gestion de crise cyber — <https://messervices.cyber.gouv.fr/guides/organiser-un-exercice-de-gestion-de-crise-cyber>
6. CNIL — Notifier une violation de données personnelles (art. 33/34 RGPD) — <https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles>
7. CNIL — Quand faut-il notifier une violation de données (FAQ 72h) — <https://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-quand-faut-il-notifier-une-violation-de-donnees-la-cnil>
8. CNIL — Bilan des sanctions 2025 (83 sanctions, 486,8 M€) — <https://www.cnil.fr/fr/bilan-sanctions-2025>
9. EUR-Lex — Directive (UE) 2022/2555 (NIS2), art. 23 — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
10. Sénat — Projet de loi Résilience (transposition de NIS2, de REC et de la directive (UE) 2022/2556, volet DORA) — <https://www.senat.fr/dossier-legislatif/pjl24-033.html>
11. Légifrance — Code des assurances, art. L.12-10-1 (LOPMI, plainte 72h) — https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047048152
12. Légifrance — Code de la santé publique, art. L.1111-8-2 — https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036515017/
13. NIST — SP 800-61 Rev.3, final (Incident Response, avril 2025) — <https://csrc.nist.gov/pubs/sp/800/61/r3/final>

14. ISO — ISO/IEC 27035-1:2023 (gestion des incidents) — <https://www.iso.org/standard/78973.html>
15. MITRE ATT&CK — base de connaissances des comportements adverses — <https://attack.mitre.org/>
16. ENISA — Threat Landscape 2025 (octobre 2025) — <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
17. Verizon — 2025 Data Breach Investigations Report (DBIR) — <https://www.verizon.com/business/resources/reports/dbir/>
18. IBM — Cost of a Data Breach Report 2025 — <https://www.ibm.com/reports/data-breach>
19. Cybermalveillance.gouv.fr — Rapport d'activité 2025 & plateforme 17Cyber — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2025>

Voyez ce que vous exposez avant qu'un attaquant ne le trouve

Sedona n'est pas prestataire de réponse à incident — en cas d'attaque, appuyez-vous sur 17Cyber, un prestataire PRIS qualifié ANSSI et votre assureur. Mais avant l'attaque, Sedona Radar analyse ce que votre domaine expose sur Internet et remet un rapport en français, avec un plan de correction. Le premier scan est gratuit.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit