Playbook de réponse à un rançongiciel

Playbook | Français · Modèle à adapter | v3.0 · 2026-10-16

Version du modèle : 3.0. Le scénario de préparation est une PME d'environ 80 personnes, avec informatique et surveillance éventuellement externalisées. Les rôles ci-dessous sont des fonctions pouvant être cumulées avec suppléance. Le décideur interne conserve l'acceptation du risque métier ; les prestataires n'exécutent que les actions autorisées relevant de leur périmètre et de leurs accès réels.

Mode d'emploi. Les sections 1–6 donnent la séquence courte. Appliquer les responsabilités et dépendances des sections 7–8 avant l'isolement, puis les contrôles des sections 10–11 avant la reprise. La section 9 guide la préservation et la section 12 fournit l'exemple. Ces références s'emploient au moment concerné, pas après la clôture. Une protection urgente préautorisée reste possible dans ses limites ; consigner les vérifications ou informations manquantes.

Type : procédure opérationnelle adaptable. Ce playbook accompagne la politique de réponse aux incidents. Il couvre une suspicion de chiffrement malveillant ou d'extorsion de données sur postes, serveurs, services cloud et sauvegardes inclus dans le périmètre autorisé. Il ne contient pas de commande de suppression ni de restauration automatique.

Approbation et préparation

Champ	Valeur à renseigner
Organisation, référence, version	[À RENSEIGNER : organisation, référence, version]
Propriétaire et approbateur	[À RENSEIGNER : responsable sécurité, direction]
Approbation et prochaine révision	[À RENSEIGNER : dates]
Services et systèmes couverts	[À RENSEIGNER : périmètre et exclusions]
Incident et responsable de conduite	[À RENSEIGNER : référence, nom, suppléant]
Canal de crise indépendant	[À RENSEIGNER : moyen testé, annuaire hors ligne]

La direction arbitre les interruptions majeures. Le responsable d'incident coordonne ; le SOC qualifie et suit la propagation. Les équipes systèmes, identité, réseau et sauvegarde exécutent les actions autorisées. Les métiers définissent les priorités de continuité. Communication et conseil juridique valident les messages et obligations avec les interlocuteurs compétents.

Préparez hors incident un inventaire critique, les dépendances de restauration, les accès d'urgence et les coordonnées des prestataires. Vérifiez leur disponibilité sans dépendre uniquement de la messagerie habituelle. Pour les environnements industriels ou de soins, la sécurité physique et les procédures d'exploitation priment sur l'application mécanique de ce document.

1. Déclencher et qualifier

☐ Ouvrir le carnet d'incident et horodater le premier signalement.

☐ Relever symptômes, hôtes concernés, chemins touchés, messages et outils de détection.

☐ Vérifier un échantillon sans ouvrir de fichier suspect sur un poste de travail ordinaire.

☐ Recenser les services indisponibles et impacts métier confirmés.

☐ Activer la coordination selon [À RENSEIGNER : seuils et procédure d'astreinte].

Le chiffrement visible ne décrit pas nécessairement le début de l'intrusion. Recherchez aussi une compromission de comptes, une suppression de sauvegardes, une persistance et une possible exfiltration. L'absence de chiffrement n'exclut pas une extorsion de données.

2. Limiter la propagation

Appliquez un confinement proportionné, documenté et vérifié. La checklist CISA privilégie l'isolement réseau des systèmes touchés ; elle envisage l'arrêt lorsque la déconnexion est impossible pour empêcher la propagation. L'arrêt peut détruire des éléments volatils. Faites arbitrer cette décision selon l'urgence, les dépendances et les consignes du responsable d'incident.

☐ Isoler les hôtes identifiés par les moyens maîtrisés ; confirmer l'effet réel.

☐ Réduire les partages et accès distants à risque après validation de l'impact.

☐ Protéger les dépôts de sauvegarde et leurs comptes d'administration.

☐ Révoquer ou restreindre les comptes compromis avec l'équipe identité.

☐ Vérifier la couverture des mesures sur sites distants et services cloud.

☐ Consigner toute exception nécessaire à la sécurité ou à la continuité.

Ne reconnectez pas un poste pour « vérifier s'il fonctionne ». N'effacez pas massivement les fichiers ou les logs. Ne transmettez pas d'échantillon contenant des données de l'organisation à un service public sans autorisation.

3. Préserver et comprendre

Question	Collecte proposée, sous autorisation	Responsable
Quel périmètre ?	Inventaire, alertes, partages et ressources cloud concernés	[À RENSEIGNER : équipe]
Quel accès initial ?	Logs identité, accès distant, messagerie et services exposés	[À RENSEIGNER : équipe]
Quelle progression ?	Logs réseau, endpoint, administration et changements de comptes	[À RENSEIGNER : équipe]
Quelle perte possible ?	Journaux de lecture/export, transferts, inventaire des données	[À RENSEIGNER : équipe]

Préservez note de rançon, horodatages, échantillons autorisés et traces de modification des sauvegardes. Une acquisition mémoire ou disque demande une méthode et des compétences adaptées. Enregistrez collecte, intégrité, stockage, accès et limites dans le carnet. Séparez preuves d'exfiltration, indices et données indisponibles.

4. Organiser les décisions de crise

Tenez un état partagé des services : indisponible, isolé, en reconstruction, validé. Fixez une cadence de situation [À RENSEIGNER : fréquence] et un décideur pour chaque arbitrage. Le référent compétent identifie les notifications et interlocuteurs selon juridiction, secteur, contrats et données concernés ; aucun délai universel ne convient à toutes les organisations.

Ce modèle ne recommande pas le paiement d'une rançon. Toute décision relative à une demande d'extorsion exige une gouvernance spécifique et des conseils compétents. Une promesse de l'attaquant ne garantit ni récupération ni suppression des données. Conservez les échanges éventuels dans un canal contrôlé, sans engagement improvisé d'un analyste.

5. Reconstruire et restaurer

☐ Examiner les accès initiaux connus ou plausibles et traiter les chemins de persistance identifiés. Documenter les incertitudes restantes et faire accepter le risque résiduel par le responsable d'incident avant la reprise.

☐ Disposer d'un environnement de reconstruction séparé et administré sainement.

☐ Sélectionner les sauvegardes selon leur date, intégrité et risque de contamination.

☐ Corriger les accès et vulnérabilités impliqués avant remise en service.

☐ Restaurer un service pilote, vérifier fonctionnement et contrôles de sécurité.

☐ Faire accepter le résultat par le propriétaire métier avant élargissement.

☐ Maintenir une surveillance renforcée et un retour arrière réalisable.

6. Clôturer et exercer

Documentez pertes connues, période incertaine, services restaurés et risques résiduels. Affectez un propriétaire et une échéance aux corrections. Testez ensuite ce playbook en exercice : messagerie indisponible, sauvegarde douteuse, compte administrateur compromis. Le succès se mesure à des décisions traçables et une restauration vérifiée, pas au seul redémarrage des serveurs.

Limites : les actions doivent respecter les habilitations, les contraintes métier et les procédures spécialisées. Ce modèle ne prouve ni éradication totale ni conformité réglementaire.

Points de passage et décisions attendues

Le responsable d'incident adapte ces points de passage à la gravité et aux contraintes de sûreté. Ils servent à rendre la progression explicite ; ils n'imposent ni un délai identique pour tous les services ni une attente de certitude absolue. Un risque résiduel accepté doit préciser les faits disponibles, les inconnues, le décideur et le prochain contrôle.

Point de passage proposé	Preuve et autorité à compléter
Confinement initial	[À RENSEIGNER : systèmes isolés, exceptions, vérification, décideur]
Reconstruction autorisée	[À RENSEIGNER : périmètre sain, accès traités, inconnues acceptées]
Reprise pilote	[À RENSEIGNER : tests techniques, validation métier, surveillance]
Retour au fonctionnement convenu	[À RENSEIGNER : risques restants, propriétaires, conditions d'arrêt]

En cas de réapparition de signes suspects, suspendre l'élargissement de la reprise et faire réévaluer le périmètre. Une nouvelle alerte ne prouve pas automatiquement une récidive ; conserver son origine et la confronter aux modifications réalisées. Le compte rendu de reprise précise les services réellement testés et les dépendances non vérifiées. Les accès temporaires et environnements de secours reçoivent un responsable et une condition de retrait.

7. Organiser la conduite avec des prestataires

Avant adoption, relier ce playbook aux services effectivement utilisés : postes distants, fichiers, identité, messagerie, applications SaaS, hébergeur et sauvegardes. Pour chaque service, identifier le propriétaire métier, l'exécutant technique, le titulaire du contrat et le moyen d'obtenir une décision hors horaires habituels. Une astreinte non contractualisée ou non financée ne doit pas être supposée disponible.

Décision	Autorité interne proposée	Exécution et preuve
Isoler un poste non critique	Coordinateur dans sa délégation	Prestataire ou opérateur habilité ; état d'isolement contrôlé
Couper un service partagé	Responsable métier ou direction	Exploitant ; dépendances et conséquences consignées
Restreindre identité ou sauvegardes	Autorité désignée avec propriétaires concernés	Administrateur habilité ; accès utiles et risques de verrouillage vérifiés

Décision	Autorité interne proposée	Exécution et preuve
Autoriser reconstruction et reprise	Direction ou propriétaire métier mandaté	Prestataire ; critères techniques et métier satisfaits ou risque accepté

Le coordinateur active un canal indépendant de l'environnement suspect et vérifie l'identité des intervenants par des coordonnées connues. Il attribue un numéro de dossier commun aux demandes IT, MSSP, hébergeur et sauvegarde. Les comptes rendus indiquent demandé, exécuté, vérifié ou impossible. Le MSSP peut manquer de droits d'administration ; une alerte transmise ne constitue pas une action de confinement.

Si le prestataire ne répond pas, utiliser le contact de secours et le circuit contractuel. Consigner les tentatives, leurs effets et les protections disponibles sans privilèges supplémentaires. Le décideur interne arbitre une suspension d'activité ou une attente protégée dans les limites de sûreté. Il ne partage pas un secret d'urgence dans une conversation collective pour contourner l'absence de contact.

8. Vérifier les dépendances avant une coupure

Construire une carte courte : identité nécessaire aux administrateurs, réseau nécessaire aux sauvegardes, services nécessaires aux opérations métier et moyens de communication. La carte doit rester lisible hors du système suspect. Identifier les dépendances circulaires, par exemple un coffre accessible uniquement avec l'identité indisponible qu'il doit permettre de restaurer. Décider avant crise comment les personnes autorisées pourront récupérer les moyens indispensables.

Dépendance	Question avant action	Décision et trace
Identité et administration	L'isolement empêche-t-il les accès de secours ou la collecte ?	[À RENSEIGNER : solution autorisée, responsable]
Sauvegarde et stockage	Le compte ou réseau compromis peut-il modifier les copies ?	[À RENSEIGNER : protection vérifiée, accès conservés]
Métier et sûreté	Une coupure empêche-t-elle une activité dangereuse à interrompre ?	[À RENSEIGNER : arbitrage, fonctionnement dégradé]
Fournisseur et télétravail	Qui peut agir sur les systèmes hors site ?	[À RENSEIGNER : couverture, contact, limite]

L'isolement initial peut devoir précéder une carte complète si la propagation est active. Documenter alors les hypothèses, l'autorité, l'effet attendu et la vérification suivante. Une mesure irréalisable ne doit pas bloquer toute décision : proposer un périmètre plus limité, une interruption métier ou une restriction d'accès réellement disponible. Les mesures compensatoires doivent être contrôlées, pas seulement annoncées.

L'administration des sauvegardes constitue un périmètre à examiner séparément : console, comptes, dépôt, copies distantes et moyens de restauration. Le guide StopRansomware recommande de protéger les sauvegardes ; la présence d'un produit de sauvegarde ne prouve pas que ces éléments sont hors d'atteinte. Demander au responsable de démontrer les protections et conserver les limites, sans détruire une copie douteuse avant arbitrage.

9. Préserver avec une question précise

Demander au prestataire les traces nécessaires pour établir l'accès initial plausible, les modifications d'identité, les systèmes atteints et les changements de sauvegarde. Préciser la période, le fuseau, la source et le format souhaités. Conserver la note de rançon et les identifiants de détection sans reproduire inutilement des données sensibles dans les communications de crise.

Pour une acquisition volatile ou disque, l'exécutant décrit le risque, l'outil, la méthode et les autorisations. Le coordinateur consigne si l'urgence impose de sacrifier une collecte. Il ne tente pas d'improviser une

acquisition spécialisée sur un serveur critique. Si les logs ont expiré ou manquent, élargir les sources autorisées pertinentes ; ne pas combler l'absence par une attribution certaine.

Les prestataires SaaS peuvent appliquer leurs propres procédures et délais contractuels. Demander une référence de demande, le périmètre exportable, l'heure de conservation et le contrôle possible. Une réponse « aucune alerte » ne prouve pas l'absence d'accès : demander ce qui était effectivement surveillé. Relier chaque conclusion à sa période et à ses sources plutôt qu'à une formule générale « environnement sain ».

10. Reconstruire dans un périmètre maîtrisé

La reconstruction commence avec une décision, un inventaire des dépendances et des moyens d'administration autorisés. Choisir les systèmes prioritaires selon le besoin métier ; vérifier identité, réseau, résolution de noms, applications, clés et droits nécessaires. Les documents d'urgence et secrets associés doivent être récupérables par des personnes habilitées sans dépendre exclusivement du domaine suspect.

Étape et entrée	Action attendue	Échec et preuve de sortie
Périmètre de reconstruction approuvé	Préparer réseau et administration séparés selon l'analyse	Si isolation ou accès non vérifiés, suspendre l'admission ; conserver contrôle et décideur
Image ou support maîtrisé	Installer, corriger et configurer les systèmes retenus	Si origine douteuse, demander un support fiable ; consigner versions et contrôles
Sauvegarde candidate	Examiner date, intégrité et indicateurs pertinents dans l'environnement de test	Si doute non résolu, conserver la copie et choisir une autre piste ou faire accepter la limite
Service pilote restauré	Vérifier fonction métier, sécurité et dépendances	Si test échoue, ne pas élargir ; enregistrer défaut, propriétaire et nouveau test

Une date antérieure au chiffrement n'établit pas à elle seule qu'une sauvegarde est antérieure à toute compromission. Le choix du point de reprise doit tenir compte de la chronologie disponible et de ses inconnues. Le responsable de reprise expose la perte de données, le temps estimé avec ses limites et les alternatives ; l'autorité métier accepte le compromis avant d'étendre la restauration.

Les changements de comptes, secrets et accès fournisseurs suivent un ordre étudié pour éviter de perdre les moyens de remédiation ou de réintroduire un accès compromis. Les opérations précises appartiennent à une procédure technique validée, pas à une commande universelle de ce modèle. Après chaque changement sensible, vérifier les accès nécessaires et l'échec des accès effectivement ciblés par la mesure.

11. Contrôles de remise en service

☐ Le périmètre pilote et ses dépendances sont identifiés, avec tests réellement exécutés.

☐ Les chemins d'accès initiaux connus ou plausibles et la persistance identifiée ont un traitement ou une limite acceptée.

☐ Les accès d'administration et de sauvegarde ont été revus avec leurs propriétaires.

☐ Le métier réalise une opération représentative et contrôle la cohérence des données.

☐ Les protections et alertes utiles sont testées, avec un destinataire identifié.

☐ Les exceptions mentionnent risque, compensation vérifiée, autorité, expiration et réexamen.

☐ Les accès temporaires, environnements de secours et restrictions ont un propriétaire de retrait.

☐ Une réapparition de signe suspect possède un circuit d'escalade et une condition de suspension.

Exception de reprise	Valeur à compléter
Service, écart et effet métier	[À RENSEIGNER : périmètre, protection manquante, conséquences]
Compensation et preuve	[À RENSEIGNER : restriction, contrôle réalisé, limites]
Décision	[À RENSEIGNER : autorité, justification, date]
Fin	[À RENSEIGNER : expiration, événement de réexamen, propriétaire de correction]

12. Scénario de bout en bout, entièrement fictif

Atelier-80, PME fictive de 80 personnes, découvre à 09:00 UTC des fichiers chiffrés sur un partage. L'informatique est externalisée ; le MSSP voit des alertes endpoint mais n'administre pas le stockage. La coordinatrice interne ouvre EX-R1 et appelle le contact vérifié du prestataire. La messagerie étant douteuse, les décisions passent par le canal de secours prévu. Aucun résultat décrit ici n'est une mesure réelle.

À 09:08 UTC, le prestataire confirme l'isolement de deux postes fictifs. Il ne peut pas encore intervenir sur un ordinateur distant éteint ; ce poste reste « non contrôlé ». Le propriétaire métier autorise l'arrêt du partage concerné et un traitement manuel des commandes. La console de sauvegarde n'est pas déclarée saine : son accès et ses changements sont examinés par son responsable distinct.

Décision fictive	Motif et autorité	Preuve et inconnue
EX-D1 : arrêter le partage	Réduire les modifications ; direction mandatée	Contrôle d'accès effectué ; origine de l'intrusion inconnue
EX-D2 : préserver export et copie candidate	Enquête et préparation reprise ; coordinateur	Export reçu ; complétude de la période encore à vérifier
EX-D3 : restaurer un pilote séparé	Besoin métier prioritaire ; propriétaire des commandes	Opération de test réussie ; poste distant et période ancienne non vérifiés

La sauvegarde fictive de la veille permet de préparer le pilote, mais son ancienneté n'exclut pas une intrusion antérieure. Le prestataire décrit les contrôles possibles et la direction accepte une reprise limitée, sans reconnecter le poste non contrôlé. Les commandes créées après le point restauré sont rapprochées par le métier avant généralisation. L'exception EX-X1 porte sur une période de logs indisponible, avec surveillance ciblée, responsable et réexamen fixés localement.

L'exercice est accepté si un remplaçant retrouve décisions et preuves, si le métier démontre une opération cohérente et si les inconnues restent visibles. Il échoue si un ticket envoyé est compté comme un isolement effectué, si la sauvegarde est présumée saine ou si la direction ignore le risque résiduel. Les écarts deviennent des actions affectées avant de déclarer le playbook prêt.

Références de travail

La partie 2 du guide StopRansomware de la CISA propose une checklist de réponse, notamment pour l'isolement et la préservation. Le guide couvre aussi prévention, extorsion et reprise. L'ANSSI, Piloter la remédiation d'un incident cyber apporte un cadre de remédiation. Les cases et responsabilités proposées ici sont à adapter et à tester localement.