Carnet d’investigation et de relève SOC

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

Version du modèle : 3.0. Ce carnet est conçu pour une PME pouvant confier l’informatique et la surveillance à des prestataires. Il ne suppose ni une équipe forensique interne ni une disponibilité permanente. Le coordinateur interne reste responsable du dossier et des décisions métier ; le prestataire exécute et documente les tâches qui lui sont confiées.

Mode d’emploi. Les sections 1–6 donnent le fil opérationnel. Utiliser les responsabilités, contrôles de provenance et formulaires des sections 7–9 avant la collecte, puis les tenir à jour pendant l’enquête. La section 10 fournit l’exemple ; la section 11 sert à accepter la relève. Les approfondissements s’appliquent au moment de l’action concernée : leur position après le résumé ne signifie pas qu’il faut préparer la collecte après la clôture.

Type : carnet opérationnel à remplir. Dupliquez ce document pour chaque incident. Il organise les preuves, les hypothèses et les décisions sans remplacer votre politique de réponse ni une acquisition forensique spécialisée. Les champs entre crochets doivent être adaptés avant utilisation.

Approbation et périmètre

Champ	Valeur à renseigner
Organisation et référence du modèle	[À RENSEIGNER : organisation, référence]
Version, propriétaire, approbateur	[À RENSEIGNER : version, responsable SOC, validateur]
Approbation et prochaine révision	[À RENSEIGNER : dates]
Référence incident et classification	[À RENSEIGNER : identifiant, confidentialité]
Responsable et suppléant	[À RENSEIGNER : noms, contacts sûrs]
Systèmes et période autorisés	[À RENSEIGNER : périmètre, bornes temporelles]

Le responsable d’incident décide des priorités. L’analyste documente les observations et leurs limites. Le dépositaire des preuves contrôle stockage et accès. Les propriétaires techniques valident les actions sur leurs systèmes. Le référent juridique ou protection des données détermine les règles de collecte, de conservation et de notification applicables.

1. Ouvrir le dossier

☐ Inscrire le signalement initial, son auteur et l’heure de réception avec fuseau.

☐ Décrire l'impact constaté, distinct de l'impact redouté.

☐ Fixer la question d'enquête : compte, terminal, flux ou opération à expliquer.

☐ Identifier les services concernés et leurs responsables.

☐ Consigner l'autorité permettant la collecte et les restrictions connues.

☐ Prévoir un prochain point de situation : [À RENSEIGNER : heure, participants].

Résumé initial à compléter : « Nous observons [À RENSEIGNER : fait vérifiable] sur [À RENSEIGNER : périmètre]. Nous cherchons à établir [À RENSEIGNER : question]. À ce stade, [À RENSEIGNER : incertitude principale] reste inconnu. » Évitez de qualifier une personne ou une intention sur la seule base d'une adresse IP.

2. Tenir le registre des éléments

Attribuez un identifiant stable à chaque pièce. Préservez l'original dans l'espace contrôlé ; travaillez sur une copie lorsque cela est possible. Une empreinte permet de contrôler la stabilité d'un fichier, pas de prouver à elle seule l'exactitude de son contenu ou l'identité de son auteur.

Pièce	Source, collecte et opérateur	Emplacement et intégrité	Limites
E-001	[À RENSEIGNER : système, méthode, filtre, heure, personne]	[À RENSEIGNER : dépôt, empreinte, contrôle]	[À RENSEIGNER : couverture, pertes, horloge]

Pour chaque transfert, ajoutez expéditeur, destinataire, date, motif et contrôle d'intégrité. N'insérez pas de secrets dans le carnet : conservez seulement une référence vers leur stockage autorisé. Fixez la conservation et la suppression selon [À RENSEIGNER : règles internes, contraintes de préservation]. Vérifiez aussi les droits du dossier partagé et les accès des intervenants externes.

3. Construire la chronologie

Gardez séparément heure de l'événement, heure d'ingestion et heure d'observation. Notez le fuseau d'origine avant normalisation. Toute correction d'horloge doit rester explicite. Une absence de log peut traduire une absence de collecte, une expiration ou une panne.

Heure originale / normalisée	Événement observé	Pièce	Interprétation et confiance
Exemple fictif : 10:05 UTC / 10:05 UTC	Une règle de transfert apparaît sur le compte de test A	E-001, exemple fictif	Création confirmée ; auteur humain non attribué
[À RENSEIGNER : heure et précision]	[À RENSEIGNER : opération, résultat, cible]	[À RENSEIGNER : pièce]	[À RENSEIGNER : interprétation]

4. Tester les hypothèses

Hypothèse	Éléments favorables	Éléments contradictoires	Vérification suivante et propriétaire
[À RENSEIGNER : explication testable]	[À RENSEIGNER : pièces]	[À RENSEIGNER : pièces ou inconnu]	[À RENSEIGNER : action, responsable, échéance]

Recherchez une explication autorisée et une observation indépendante. Distinguez « non trouvé dans les sources consultées » et « absent ». Révisez une conclusion si une nouvelle pièce la contredit ; conservez la conclusion précédente et la raison de son changement. Une corrélation temporelle seule ne démontre ni causalité ni attribution.

5. Enregistrer les décisions et leurs effets

Décision	Motif et preuves	Autorisation	Exécution et vérification
[À RENSEIGNER : action, cible]	[À RENSEIGNER : bénéfice, risque, alternatives]	[À RENSEIGNER : décideur, heure]	[À RENSEIGNER : opérateur, résultat, contrôle, retour arrière]

Si l'urgence impose le confinement avant une collecte, écrivez quelles preuves deviennent indisponibles. Pour une mesure différée, indiquez le risque accepté, le responsable et le moment de réexamen. Une commande exécutée n'est pas une preuve suffisante que l'effet recherché a été obtenu.

6. Préparer la relève et la clôture

☐ Résumer faits établis, hypothèses ouvertes, impact et périmètre non couvert.

☐ Transmettre les pièces accessibles et la liste des restrictions.

☐ Lister actions en attente, propriétaires, échéances et critères d'escalade.

☐ Confirmer canal de coordination et prochaine relève.

☐ Faire reformuler les priorités par l'analyste entrant ; enregistrer l'acceptation.

☐ À la clôture, fixer surveillance résiduelle, corrections et propriétaire du suivi.

☐ Vérifier conservation, restrictions et suppression des copies temporaires autorisées.

Limites : ce carnet ne garantit pas la recevabilité judiciaire d'une preuve. Les investigations sur personnes, données sensibles ou systèmes critiques exigent des autorisations adaptées. Les délais de notification dépendent des obligations applicables ; faites-les déterminer par les responsables compétents.

Mise en service et contrôle du carnet

Avant le premier usage, le propriétaire du modèle vérifie que les intervenants peuvent ouvrir le dépôt de preuves, retrouver un événement source et utiliser le canal de relève. Un champ rempli sans référence vérifiable ne transforme pas une hypothèse en fait. Si une source manque, noter qui peut la fournir, la période encore récupérable et la décision rendue impossible. Les objectifs de suivi sont fixés localement, selon l'urgence et les moyens disponibles.

Contrôle de qualité proposé	Résultat à conserver
Un collègue retrouve une pièce à partir du carnet	[À RENSEIGNER : pièce, contrôleur, résultat]
Une décision renvoie à son autorisation et à son effet vérifié	[À RENSEIGNER : décision, contrôle, écart]
La relève connaît les inconnues et les actions prioritaires	[À RENSEIGNER : réception, responsable, prochaine étape]

Le responsable relit la synthèse avant diffusion : chaque conclusion importante doit renvoyer à une pièce ou être explicitement présentée comme une hypothèse. Préparer une version restreinte si les destinataires n'ont pas besoin des détails personnels ou techniques. Toute correction conserve la référence de la version précédente, l'auteur et le motif. L'acceptation d'une relève transfère la conduite des actions convenues ; elle n'efface pas les incertitudes documentées.

7. Préparer un dossier réellement utilisable

Pour une organisation d'environ 80 personnes, désigner une personne interne capable de joindre les métiers, autoriser les dépenses prévues et arbitrer une interruption. Le prestataire informatique peut collecter les traces ; le MSSP peut analyser ses alertes. Aucun des deux ne doit être présumé propriétaire de toutes les données SaaS. Vérifier, service par service, qui possède les droits d'export et qui peut attester une action.

Fonction proposée	Responsabilité de décision	Exécution et suppléance
Coordinateur interne	Priorités, destinataires, suivi et demandes d'arbitrage	[À RENSEIGNER : titulaire, suppléant, canal indépendant]
Propriétaire métier	Impact, accès aux informations sensibles, acceptation de reprise	[À RENSEIGNER : direction ou responsable concerné]
Informatique ou fournisseur SaaS	Autorisation technique selon délégation	[À RENSEIGNER : prestataire, contact de secours, droits disponibles]
Analyste interne ou MSSP	Conclusions techniques et limites	[À RENSEIGNER : analyste, relecteur, relais hors couverture]

Avant collecte, compléter la fiche de périmètre : actifs, identités, services SaaS, télétravail, accès fournisseurs, période recherchée et exclusions. Ajouter l'emplacement réel des données, la capacité d'export, les conditions contractuelles et le propriétaire qui autorise l'accès. Les équipements personnels ou systèmes industriels exigent une décision spécifique ; ce carnet ne crée aucune autorisation d'y intervenir.

Si un contact manque, le coordinateur utilise le secours puis le circuit contractuel d'escalade. Il consigne tentatives, heure, conséquence et prochain rendez-vous. Une demande envoyée au fournisseur reste « demandée », pas « réalisée ». En attendant, le décideur interne peut faire limiter une activité par les moyens autorisés disponibles ; il doit aussi pouvoir accepter explicitement un risque temporaire documenté.

8. Maîtriser provenance, qualité et horloges

Pour chaque export, noter l'interface ou la requête, les paramètres temporels, le fuseau sélectionné, le filtrage et la pagination. Vérifier que la plage exportée correspond à la demande. Noter une limite de licence, un échantillonnage ou une troncature. Si le prestataire ne livre qu'une capture d'écran, préciser ce qu'elle montre et demander les événements sources quand ils sont nécessaires au raisonnement.

Séparer quatre états de qualité : trace native disponible, export documenté, observation indirecte, information rapportée. Ce classement est une proposition de travail, pas une échelle universelle de valeur probante. Un témoignage utile peut orienter une recherche sans devenir une preuve de connexion. Un outil de détection peut avoir normalisé une valeur ; conserver le lien vers sa source avant d'interpréter le champ.

Contrôle de qualité	Question à poser	Conséquence à documenter
Couverture	La catégorie était-elle activée pendant les faits ?	[À RENSEIGNER : période couverte ou inconnue]
Temps	Heure source, fuseau et décalage sont-ils connus ?	[À RENSEIGNER : conversion, marge, ordre incertain]
Complétude	Export complet, paginé ou limité ?	[À RENSEIGNER : exclusions et nouvelle collecte]
Transformation	Champ original ou enrichissement ?	[À RENSEIGNER : correspondance, version, limite]

Ne forcez pas un ordre précis entre deux événements si la précision ou le décalage d'horloge ne le permet pas. Écrivez « dans cette fenêtre » et conservez les deux possibilités. Le NIST SP 800-86 décrit notamment les différences d'horloge et de fuseau entre systèmes ; la marge retenue ici doit être justifiée par les observations locales, sans tolérance chiffrée universelle.

Une empreinte calculée après réception contrôle la stabilité de la copie reçue ; elle ne démontre pas à elle seule que le fournisseur a exporté toute la source. Demander son mode de collecte et préserver ses réponses. Toute conversion utile à l'analyse produit une copie identifiable ; ne remplacez pas silencieusement l'original. En cas de correction, conservez l'ancien fichier et expliquez pourquoi il est remplacé.

9. Formulaires complémentaires à dupliquer

Fiche de transfert	Valeur à renseigner
Pièce, version et motif	[À RENSEIGNER : identifiants, usage autorisé]
Émetteur et destinataire	[À RENSEIGNER : identité, fonction, autorisation]
Départ, réception et canal	[À RENSEIGNER : heures avec fuseau, moyen sécurisé]
Contrôle à réception	[À RENSEIGNER : empreinte ou contrôle adapté, résultat, réserve]

Fiche d'incertitude	Valeur à renseigner
Question non résolue	[À RENSEIGNER : attribution, période ou opération]
Données consultées et manquantes	[À RENSEIGNER : pièces, couverture et raisons]
Décision encore possible	[À RENSEIGNER : protection proportionnée et limites]
Prochain contrôle	[À RENSEIGNER : propriétaire, source attendue, point de décision]

Le registre des exceptions précise l'exigence non satisfaite, le motif, les risques et les protections compensatoires réellement disponibles. Le propriétaire métier ou l'autorité désignée accepte ou refuse ; l'analyste ne transforme pas un défaut de preuve en validation. Une expiration et un événement de réexamen sont obligatoires dans le modèle adopté, avec une durée choisie localement. L'expiration impose une nouvelle décision, pas une reconduction tacite.

Fiche d'exception	Décision à compléter
Écart et périmètre	[À RENSEIGNER : contrôle manquant, systèmes, période]
Protection et limites	[À RENSEIGNER : mesure, preuve, risque restant]
Autorité et justification	[À RENSEIGNER : décideur, motif, date]
Fin et réexamen	[À RENSEIGNER : expiration, déclencheur, propriétaire de correction]

10. Exemple complet, intégralement fictif

L'entreprise fictive Atelier-80 emploie 80 personnes et utilise une messagerie SaaS administrée par un prestataire. À 08:20 UTC, la comptabilité signale un transfert de messages non reconnu. La coordinatrice interne ouvre INC-EX-01 ; le prestataire collecte les traces, le MSSP n'ayant accès qu'aux alertes. Aucune personne, adresse ou opération décrite ici ne correspond à un incident réel.

Pièce fictive	Provenance et collecte	Stockage et contrôle	Limite
EX-E1	Export audit SaaS, filtre compte A, 08:35 UTC, opérateur prestataire	Dépôt restreint EX, copie reçue et empreinte enregistrées dans le journal fictif	Export 07:00–08:35 UTC uniquement
EX-E2	Capture de la règle, 08:39 UTC, propriétaire messagerie	Même dépôt, original et copie distingués	Ne prouve pas à elle seule l'auteur humain
EX-E3	Compte rendu du propriétaire métier, 08:45 UTC	Note datée, auteur identifié	Besoin autorisé non retrouvé, déclaration à corroborer
EX-E4	Confirmation du prestataire et contrôle distinct, 09:05 UTC	Nouvelle note datée, opérateur et service identifiés	Contrôle de la règle uniquement ; sessions encore à vérifier

Heure fictive	Fait et pièce	Hypothèse ou limite	Action suivante
08:12 UTC	Création de règle sur compte A, EX-E1	Opération confirmée ; rattachement à une session inconnu	Demander logs de connexion disponibles
08:20 UTC	Signalement comptable, EX-E3	Ne prouve pas une exfiltration	Identifier messages et période concernés
08:50 UTC	Retrait de règle demandé	Pas encore exécuté	Obtenir contrôle d'état auprès du prestataire
09:05 UTC	Prestataire confirme retrait et vérification, EX-E4	Sessions applicatives encore à vérifier	Poursuivre confinement côté identité et application

La direction fictive accepte une restriction temporaire du compte malgré un retard de traitement des commandes. Décision EX-D1 : coordinatrice mandatée, exécution prestataire, effet vérifié sur la règle, contrôle des sessions encore ouvert. L'hypothèse « changement métier autorisé » reste possible tant que l'historique d'approbation n'est pas vérifié. La conclusion intermédiaire est donc une opération contestée, pas une personne identifiée.

À la relève fictive de 09:30 UTC, l'analyste entrant retrouve EX-E1, reformule les deux inconnues et accepte trois actions : contrôler les sessions, préciser les messages touchés et retrouver une éventuelle autorisation métier. La coordinatrice conserve la responsabilité de l'arbitrage. Le dossier ne peut être clos uniquement parce que la règle a disparu ; les actions résiduelles doivent être attribuées et la conclusion rédigée à leur niveau réel.

11. Vérifier la complétude et accepter la relève

☐ Un responsable interne et un suppléant sont joignables sans dépendre du compte suspect.

☐ Chaque conclusion importante possède une pièce, une limite ou le statut explicite d'hypothèse.

☐ Les requêtes et plages consultées peuvent être reproduites par un intervenant autorisé.

☐ Les transferts et corrections conservent provenance et versions.

☐ Les actions demandées, exécutées et vérifiées sont distinguées.

☐ Les décisions sous incertitude indiquent décideur, risque, compensation et réexamen.

☐ L'entrant confirme accès aux pièces, priorités, contacts et prochaines décisions.

☐ Les copies temporaires et accès fournisseurs ont une condition de retrait.

La clôture est une décision distincte de la relève. Elle contient le périmètre couvert, les faits, les inconnues acceptées, les conséquences métier et les actions suivies ailleurs. Le responsable valide la diffusion et le stockage ; les fonctions compétentes déterminent conservation et obligations applicables. Un examen ultérieur doit pouvoir comprendre pourquoi une décision était raisonnable avec les informations disponibles à cet instant.

Références de travail

Le NIST SP 800-61 révision 3 situe la réponse aux incidents dans la gestion du risque. Le NIST SP 800-86, publié en 2006, fournit un cadre de collecte et d'analyse forensique ; ses exemples techniques doivent être actualisés. Les tableaux et procédures ci-dessus sont des propositions éditoriales à adapter, sans certification ni garantie de conformité.