Politique de journalisation et de surveillance de sécurité

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

Version du modèle : 3.0. Type : politique et procédures de mise en service, de surveillance et de traitement des écarts. Profil d'adaptation : PME d'environ 80 personnes, avec infogérance et MSSP possibles. Ce profil n'affirme pas que vos outils collectent les événements décrits. L'entreprise doit conserver un responsable interne pour les usages, les droits, la couverture acceptée et les risques des sources manquantes.

Après adaptation et adoption, les consignes et « doit » constituent des exigences internes sur le périmètre approuvé. Avant adoption, ce sont des propositions. Le propriétaire doit confirmer les capacités, contrats et personnes, puis faire approuver paramètres et exceptions. Le document ne garantit ni détection exhaustive, ni conformité, ni valeur probante automatique. Les horaires, fréquences, seuils et durées doivent être décidés localement.

1. Objet, périmètre et approbation

La journalisation doit permettre de répondre à des questions de sécurité définies : accès, changements sensibles, opérations et état des protections. La surveillance doit relier ces observations à une personne chargée de qualifier et d'agir. Accumuler des logs sans usage, accès maîtrisé ou destinataire d'alerte ne constitue pas une capacité démontrée. Le propriétaire doit distinguer collecte, recherche, détection et réponse réellement disponibles.

Le périmètre doit couvrir les services prioritaires et leurs dépendances : identité, terminaux, accès distants, réseau, applications, hébergement et chaîne de collecte. Les services externalisés doivent préciser catégories accessibles, export, licence, localisation, responsabilités et limites contractuelles. Les équipements personnels ou industriels exigent une autorisation et une méthode adaptées. Une source non intégrée doit rester visible, avec les questions d'enquête qu'elle empêche de traiter.

Paramètre	Décision locale	Responsable	Preuve avant adoption
Usages et périmètre	[À RENSEIGNER : services, scénarios, exclusions]	Propriétaire interne et métiers	Registre des questions et sources
Surveillance	[À RENSEIGNER : horaires, astreinte réelle, secours]	Responsable interne et MSSP	Contacts et exercice de réception
Protection et accès	[À RENSEIGNER : stockage, rôles, export, administration]	Exploitation et sécurité	Tests d'accès et de séparation
Conservation et données	[À RENSEIGNER : catégories, justifications, durées, suppression]	Fonctions compétentes	Décision par usage et contraintes
Contrôle documentaire	[À RENSEIGNER : version, effet, approbateur, révision]	Direction	Approbation et diffusion contrôlée

Avant l'effet de la politique, le propriétaire doit obtenir une démonstration d'une source jusqu'au traitement d'un événement bénin. Il doit aussi tester une panne et un accès refusé. Les résultats doivent préciser ce qui manque. L'adoption ne doit pas qualifier une intégration d'opérationnelle simplement parce qu'un agent est installé ou qu'un tableau affiche un volume.

2. Responsabilités et limites des prestataires

Fonction	Responsabilité	Limite de décision	Relais prévu
Propriétaire interne	Arbitrer usages, couverture, exceptions et moyens	Acceptation du risque interne	Suppléant avec accès au registre
Propriétaire de source	Autoriser configuration, catégories et changements	Ne promet pas un export non vérifié	Responsable du service de secours
Infogérant	Configurer, transporter, stocker, surveiller les collecteurs	Pas de réduction silencieuse de collecte	Escalade technique et opérateur habilité
MSSP ou analystes	Qualifier alertes, documenter scénarios et limites	Aucune action métier hors délégation	Relève et contact contractuel
Sécurité et gestion des accès	Définir et vérifier les permissions	Accès justifié, pas ouverture générale	Référent nommé
Fonctions juridique et données	Évaluer usages, conservation et obligations	Pas de règle légale universelle issue du modèle	Conseil ou référent de secours

Le responsable interne doit faire préciser au fournisseur qui configure une source, qui contrôle les rejets, qui reçoit l'alerte d'arrêt et qui vérifie la correction. Le contrat doit définir les droits aux données, la restitution et la fin de service. Une surveillance externalisée ne doit pas supprimer la capacité de l'entreprise à connaître ses lacunes ou à récupérer ses éléments autorisés.

En cas d'absence, les tâches doivent être transférées et acceptées. Si le MSSP n'assure pas une période, l'entreprise doit décider qui reçoit les signaux urgents ou accepter explicitement ce risque. Une automatisation sans destinataire ne doit pas être décrite comme une prise en charge. Le propriétaire doit tester le relais et conserver le résultat.

3. Construire une couverture par question d'enquête

Pour chaque service prioritaire, le métier et la sécurité doivent formuler les questions : quel compte a accédé, quelle opération a réussi, quel droit a changé, quel équipement a observé la connexion ? Chaque question doit être liée à une catégorie, aux champs nécessaires, au propriétaire et à un événement de test. Une liste de produits ne remplace pas ce travail.

Question proposée	Observation requise	Vérification locale	Limite à consigner
Qui a obtenu un accès ?	Identifiant stable, service, résultat, période	Connexion de test retrouvée	Compte partagé, catégorie absente, contexte manquant
Quel droit a changé ?	Avant/après si disponible, auteur technique, cible	Changement bénin autorisé	Historique incomplet ou attribution humaine inconnue
Quelle opération applicative ?	Type, cible, résultat et référence	Action connue recherchée	Collecte partielle ou lien de session absent
Le dispositif fonctionne-t-il ?	État agent, transport, parsing, stockage	Arrêt ou retard simulé	Surveillance dépendante du composant défaillant

Le registre doit distinguer source prévue, émission vérifiée, réception, interprétation et usage de détection testé. Une source qui émet mais dont le parser rejette un champ critique n'est pas intégralement opérationnelle. Le propriétaire doit approuver le statut réel. Le MSSP doit voir la limitation lorsqu'il qualifie une alerte, pas seulement dans un document administratif éloigné.

Les priorités doivent suivre les risques et les moyens disponibles. L'intégration d'un service doit préciser catégories activées et désactivées, coûts ou limites de licence, historique disponible et période perdue.

Une catégorie activée aujourd'hui ne crée pas rétrospectivement des événements. Le fournisseur doit confirmer les limites d'export et l'entreprise doit décider leurs conséquences sur les enquêtes prévues.

4. Configurer et accepter une source

Le propriétaire de source doit fournir identifiant, version, configuration, compte technique, protocole, destination et responsabilité de maintenance. L'exploitant doit utiliser un changement autorisé, limiter les permissions et prévoir un retour si la collecte perturbe le service. Les systèmes sensibles doivent être testés avec leur exploitant ; la journalisation ne doit pas être activée mécaniquement à un niveau incompatible avec leur fonctionnement.

L'opérateur doit produire un événement bénin identifiable, puis le retrouver à chaque étape disponible : source, collecteur, stockage et recherche. Il doit comparer champs, heure, résultat et origine. Les transformations doivent conserver le sens et une référence vers le format d'origine lorsque nécessaire. Les filtres et exclusions doivent être connus ; un rejet silencieux ne doit pas être présenté comme une donnée inexistante.

Contrôle de recette	Entrée et exécutant	Preuve attendue	Échec et décision
Émission	Propriétaire ; événement autorisé	Trace source et configuration	Corriger ou constater une capacité absente
Transport	Exploitant ; route et identité technique	Réception liée à l'origine	Isoler panne, droits ou format
Interprétation	Analyste ; champs attendus	Comparaison source/recherche	Corriger parser ; limiter les scénarios concernés
Usage et prise en charge	MSSP ; règle ou recherche de test	Résultat et destinataire identifié	Ne pas annoncer une détection opérationnelle

La fiche de recette doit nommer contrôleur, date, périmètre et réserves. Le propriétaire interne doit accepter ou refuser la mise en service. Un refus ne doit pas entraîner suppression des traces utiles déjà disponibles ; il doit préciser l'usage limité autorisé. Les corrections doivent être testées à nouveau et l'ancien résultat conservé.

5. Maîtriser les heures et les identifiants

L'exploitant doit vérifier la cohérence des horloges et des références de temps retenues. Il doit conserver heure d'événement, fuseau ou référence, heure de réception et décalages connus. La configuration doit permettre de comprendre les conversions et changements saisonniers. Une correction d'horloge ne doit pas réécrire silencieusement l'histoire utilisée dans une enquête.

Le contrôle doit comparer un événement connu sur la source et dans l'outil de recherche. La tolérance acceptable doit être justifiée par les usages : [À RENSEIGNER : référence, tolérance et méthode]. Si elle est dépassée, le propriétaire doit limiter les conclusions temporelles, informer les analystes et faire corriger la cause. Un retard de réception doit être distingué d'une heure source incorrecte.

Les identifiants doivent rester stables ou interprétables : compte, terminal, service, locataire ou contexte réseau selon la source. Une adresse réutilisée ne suffit pas à identifier un poste historique ; un nom de compte affiché ne prouve pas une personne. Les règles de normalisation doivent préserver les inconnues et éviter de remplacer une valeur manquante par une identité supposée.

6. Protéger transport, stockage et confidentialité

L'exploitant doit choisir un transfert et un stockage adaptés à la sensibilité, aux pertes possibles et aux contraintes. Les chemins, permissions, identités techniques et protections de transfert doivent être documentés. L'organisation doit vérifier si une panne ou saturation détruit les événements, les conserve localement ou les retransmet. La capacité annoncée doit être confrontée aux conditions de fonctionnement retenues.

Les permissions doivent distinguer recherche, export, modification de configuration, administration et suppression. Une personne qui enquête n'a pas automatiquement besoin d'administrer les collecteurs. Les accès exceptionnels doivent être nominatifs, autorisés et retirés à leur fin. Les comptes techniques doivent être limités et suivis ; partager un compte d'administration empêche d'obtenir la même traçabilité qu'un accès individuel.

Usage	Autorité et action	Preuve	Contrôle négatif
Lecture d'enquête	Responsable autorise un périmètre	Identité, dossier et accès	Un utilisateur hors rôle est refusé
Export	Propriétaire autorise contenu et destination	Référence, destinataire, durée	Absence de dépôt public ou non approuvé
Administration	Exploitant habilité applique le changement	Accord, configuration et contrôle	Analyste sans droit ne modifie pas
Suppression ou rétention	Autorité définie valide la règle	Justification et exécution testée	Suppression non autorisée refusée et signalée

Mots de passe, clés privées, cookies et tokens utilisables ne doivent pas être collectés volontairement comme contexte d'enquête ordinaire. Les données personnelles inutiles doivent être réduites. Une exception indispensable doit préciser accès, stockage et durée avec les fonctions compétentes. Les exports, pièces de dossier, sauvegardes et copies locales doivent suivre leurs propres restrictions ; les protéger à la source ne protège pas automatiquement les copies.

7. Détecter panne, retard et altération

L'exploitant doit surveiller la chaîne elle-même : source muette, agent arrêté, file en attente, rejet de parsing, saturation, espace et erreurs d'accès. Les seuils doivent être définis par source et usage, pas copiés comme universels. Une source normalement silencieuse exige un contrôle adapté ; l'absence de volume ne signifie pas toujours une panne, et un volume élevé n'établit pas une bonne qualité.

Symptôme	Vérification initiale	Action et preuve	Escalade
Source muette	Activité attendue, état source, émission connue	Localiser la rupture et consigner la période	Propriétaire de service et MSSP
Retard	Heure source, réception et files	Définir fraîcheur réelle ; suivre rattrapage	Responsable interne si enquête affectée
Champ critique perdu	Comparaison au format d'origine	Limiter la règle ; corriger et rejouer le test	Analyste et exploitant
Suppression ou changement suspect	Autorisations, trace indépendante disponible	Préserver, restreindre sous autorité, ouvrir un incident si justifié	Pilote de réponse

La réception d'une alerte de panne doit être testée par un canal qui ne dépend pas exclusivement du composant en panne. Si cette indépendance est impossible, la limite doit être connue et compensée ou acceptée. La demande fournisseur doit préciser la période possiblement perdue, le rétablissement attendu et le contrôle nécessaire. Un service redémarré ne prouve pas que tous les événements ont été récupérés.

L'opérateur doit préserver les éléments utiles lorsqu'une altération est suspectée et éviter de masquer les traces par une réparation non consignée. Une alerte d'intégrité n'établit pas à elle seule une intention malveillante ; les changements autorisés et erreurs doivent aussi être examinés. La décision doit séparer restauration de collecte et enquête sur la cause.

8. Rétention, protection des données et conservation exceptionnelle

Le propriétaire doit définir les durées par catégorie et usage avec les fonctions compétentes : besoin de recherche, accès courant, archivage éventuel, contrat et obligations applicables. Il doit justifier le niveau de détail et l'accès. Ce modèle ne prescrit aucune durée universelle. Une durée vendue par un outil ne constitue pas, seule, une justification pour conserver chaque catégorie de données.

Le cycle doit inclure suppression et copies. L'exploitant doit tester qu'une donnée expirée disparaît des emplacements concernés selon les mécanismes disponibles, sans affecter une préservation autorisée. Si une sauvegarde ne permet pas d'effacement individuel, la contrainte et le traitement doivent être examinés. L'équipe ne doit pas promettre un effacement immédiat qu'elle ne sait pas réaliser.

Décision	Informations à conserver	Contrôle	Réévaluation
Durée ordinaire	Catégorie, usage, justification, autorité	Recherche et suppression testées	Changement d'obligation ou d'usage
Accès restreint	Rôle, objectif, population autorisée	Tests d'accès et revue	Changement de fonction ou mission
Préservation de dossier	Périmètre, motif, autorité, échéance de revue	Copies identifiées et accès	Fin de besoin ou décision compétente
Export fournisseur	Conditions, destination, restitution	Exemple récupérable et lisible	Fin de contrat ou capacité modifiée

Une conservation exceptionnelle doit rester limitée au dossier et être réexaminée ; elle ne doit pas devenir un archivage illimité de toutes les sources. Les personnes compétentes doivent décider des contraintes juridiques spécifiques. L'analyste doit conserver la référence de l'autorisation plutôt que diffuser son raisonnement juridique ou des données personnelles inutiles dans chaque ticket.

9. Triage et traitement d'une alerte

Chaque scénario doit définir objectif, sources, conditions connues, propriétaire, preuve attendue et procédure de qualification. L'analyste doit vérifier l'événement d'origine, la cible, la période et la couverture avant de conclure. Il doit chercher une explication autorisée et une observation indépendante. Une alerte n'est ni une preuve complète d'incident, ni une mesure de confinement exécutée.

Étape	Action de l'analyste	Preuve utile	Échec à escalader
Prendre en charge	Accepter le dossier et vérifier le périmètre	Responsable et prochaine décision	Absence de destinataire ou droits
Qualifier	Comparer trace, contexte et hypothèses	Requête, événements, inconnues	Source manquante ou incohérence
Décider	Classer avec motif ou déclencher réponse	Conclusion et autorité	Compromission plausible non maîtrisée
Ajuster	Faire autoriser et tester une modification	Version, test, portée	Réduction silencieuse de couverture

Les ajustements doivent expliquer les alertes inutiles sans masquer un service. Une exclusion doit avoir propriétaire, raison, expiration si temporaire et test de non-régression. Une baisse du nombre d'alertes peut provenir d'une panne ; elle ne doit pas être présentée comme une amélioration sans contrôle de couverture. Le responsable interne doit accepter les réserves lorsqu'un scénario est mis en pause.

10. Exemple fictif de couverture et de panne

Atelier Rivage, PME fictive d'environ 80 personnes, utilise une application externalisée. Le MSSP reçoit des connexions mais pas les changements de droits. Le registre indique émission partielle et interdit de présenter le scénario de changement comme testé. L'infogérant active une catégorie autorisée et réalise une modification bénigne ; cette situation n'est pas une référence client.

Événement fictif	Observation	Décision	Résultat attendu
Recette initiale	Connexion présente, changement absent	Couverture partielle acceptée avec réserve	Aucun scénario complet revendiqué
Changement de configuration	Catégorie ajoutée, test retrouvé	Recette de la question « quel droit ? »	Identifiant, cible et résultat contrôlés
Évolution de format	Auteur devenu vide dans la recherche	Pause de la conclusion d'attribution	Source originale et période affectée conservées
Réparation	Parser corrigé, test rejoué	Réouverture du scénario	Pertes éventuelles et limites encore visibles

L'exercice est accepté si un second analyste peut expliquer ce que la période partielle permet de conclure, retrouver la réserve et déterminer qui peut autoriser la reprise. Il doit distinguer une heure source incorrecte d'un retard d'arrivée. La simulation échoue si la présence d'un volume est utilisée pour déclarer toutes les questions couvertes.

11. Annexes utilisables et test d'adoption

Fiche de source vierge	Valeur à compléter	Propriétaire	Preuve de recette
Identité et usage	[À RENSEIGNER : service, identifiant, question]	[À RENSEIGNER]	Événement autorisé retrouvé
Catégories et champs	[À RENSEIGNER : activés, absents, formats]	[À RENSEIGNER]	Comparaison à l'origine
Temps et transport	[À RENSEIGNER : référence, retard attendu, pertes]	[À RENSEIGNER]	Horloges et panne testées
Protection et cycle	[À RENSEIGNER : droits, export, durée, suppression]	[À RENSEIGNER]	Tests positifs et refus
Surveillance	[À RENSEIGNER : horaires, contact, réponse, secours]	[À RENSEIGNER]	Réception et acceptation

☐ Retrouver une connexion et une opération sensible connues.

☐ Expliquer champs manquants et période non couverte.

☐ Vérifier horloge, fuseau, réception et retard.

☐ Déclencher une panne bénigne et obtenir une prise en charge.

☐ Refuser un accès non autorisé et contrôler un export.

☐ Tester suppression et préservation autorisée sans les confondre.

☐ Confirmer la relève et l'escalade hors horaires réellement couverts.

12. Exceptions, suivi et révision

Toute dérogation doit préciser objectif affecté, sources, cause, questions rendues impossibles, compensation, responsable, décideur et expiration. Une durée trop courte, un champ absent ou une

source non exportable doivent être évalués explicitement. Le fournisseur ne doit pas accepter seul le risque. À l'échéance, le propriétaire doit obtenir correction vérifiée ou nouvelle décision, sans renouvellement tacite.

Le responsable doit présenter à [À RENSEIGNER : instance et cadence] sources partielles, périodes perdues, scénarios non testés, accès exceptionnels et dérogations expirantes. Les indicateurs doivent décrire période, population et méthode. Les écarts doivent déclencher tâches, responsables et contrôles. Un statut inconnu ne doit jamais être compté comme opérationnel pour embellir le rapport.

Chaque changement de format, fournisseur, usage ou responsabilité doit déclencher une revue proportionnée et une recette concernée. La version doit garder auteur, motif, approbateur et anciennes références. Les preuves doivent être conservées dans [À RENSEIGNER : dépôt, droits et durée]. L'entreprise doit pouvoir reprendre les fiches et les traces autorisées lors d'une fin de contrat.

Sources et limites

Le guide ANSSI sur l'architecture d'un système de journalisation, version 2.0, janvier 2022 traite horodatage, couverture, transport, accès et rétention, notamment R3–R6, R9–R17 et R24–R27. Le NIST SP 800-61 révision 3 encadre qualification et protection des éléments d'enquête.

Les matrices, usages, niveaux de couverture, rôles et scénarios proposés sont des choix locaux à approuver et tester, non une promesse de capacité d'un produit. Les recommandations officielles doivent être adaptées aux systèmes et obligations réels. Le document ne remplace ni une analyse de protection des données, ni l'expertise technique nécessaire à une collecte fiable.