RECOMMANDATIONS DE SÉCURITÉ POUR L'ARCHITECTURE D'UN SYSTÈME DE JOURNALISATION

GUIDE ANSSI

ANSSI-PA-012/ANSSI/SDE
28/01/2022

PUBLIC VISÉ :

Développeur **Administrateur** **RSSI** **DSI** Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations de sécurité pour l'architecture d'un système de journalisation »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`. Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [18].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	02/12/2013	Version initiale
2.0	28/01/2022	Mises à jour détaillées en annexe E

Table des matières

1
Introduction

1.1 Objectifs du guide

La journalisation est une activité technique indispensable à la sécurité des systèmes d'information. Elle est parfois imposée par la réglementation. En préventif, la journalisation est un prérequis pour certaines mesures de durcissement essentielles (p. ex. dresser l'inventaire des applications d'un SI en vue de définir une politique de restrictions logicielles). En réactif, l'analyse continue des journaux d'évènements permet de repérer des activités inhabituelles, tandis que l'archivage des journaux rend possible les levées de doutes *a posteriori* [1]. En ce sens, la journalisation constitue également le prérequis indispensable à la mise en œuvre d'une capacité de détection, d'analyse et de réponse aux incidents de sécurité.

Attention

Ce guide est consacré à la seule fonction de journalisation, c'est-à-dire à la collecte des journaux d'évènements. Ce guide n'est pas consacré au traitement et à l'analyse en continu de ces journaux. Ce parti pris éditorial ne doit pas occulter le fait qu'un SI ne pourra prétendre être sécurisé qu'à la condition de non seulement collecter les évènements de sécurité mais encore d'en assurer une exploitation en continu, seule à même de permettre une détection proactive des incidents de sécurité. L'annexe C donne un aperçu sommaire de la démarche visant à mettre en œuvre un système de détection des incidents de sécurité.

La journalisation sera d'autant plus pertinente qu'elle s'appliquera à un large spectre d'équipements du SI (postes de travail, équipements réseaux, serveurs, etc.) et que son évolution sera corrélée aux évolutions du SI.

Ce document a pour objectif de présenter les principes généraux régissant la mise en œuvre d'un système de journalisation sécurisé. Ces principes sont applicables à tous les types de SI (SI bureautiques, SI industriels…) et sont agnostiques des technologies des systèmes qui génèrent les journaux (équipements réseau, *appliances*, systèmes d'exploitation, applications…). Le lecteur trouvera dans d'autres publications de l'ANSSI une déclinaison de ces principes généraux à des technologies spécifiques [2].

Ce document n'a pas vocation à présenter la liste détaillée des évènements à journaliser (ceux-ci étant dépendants des systèmes d'exploitation et des applications employées) mais il peut faciliter

1. Sous réserve d'être compatibles avec les durées légales maximales de conservation des journaux (voir annexe D), les recherches de marqueurs de compromission pourront porter sur des évènements de sécurité relativement anciens.
2. Par exemple, pour plus d'information concernant le mise en pratique de la journalisation sur des systèmes Microsoft Windows en environnement Active Directory, se reporter au guide [13].

la formalisation d'une politique de journalisation. En particulier, l'annexe A donne un aperçu des catégories d'évènements qu'il est recommandé de journaliser pour constituer un *socle minimal de journalisation*.

1.2 Organisation du guide

Ce guide est organisé en deux parties :

- le chapitre 2 liste les prérequis à la mise en place d'un système de journalisation ;
- le chapitre 3 donne des recommandations pour l'architecture et la conception d'un système de journalisation.

Quatre annexes complètent ce guide :

- l'annexe A donne un aperçu des types d'évènements de sécurité qu'il est pertinent de collecter pour constituer un *socle minimal de journalisation* ;
- l'annexe B présente des schémas d'architectures possibles pour un système de journalisation ;
- l'annexe C introduit le sujet de la détection des incidents de sécurité ;
- l'annexe D porte sur les aspects juridiques et réglementaires applicables à la journalisation ;
- l'annexe E liste les principaux changements entre la version 1.0 du guide et les versions ultérieures.

1.3 Conventions de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*.

Pour certaines recommandations, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R +

Recommandation renforcée

Cette recommandation permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information.

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information [3], la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

La liste récapitulative des recommandations est disponible en page 44.

3. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [8].

2
Prérequis à la mise en place d'un système de journalisation

Objectif

Ce chapitre précise les conditions que doivent remplir les équipements d'un système d'information (SI) pour permettre la mise en place de la journalisation : capacité à générer des évènements enregistrés dans des journaux, possibilité d'horodater ces évènements grâce à une source de temps commune et dimensionnement adéquat du stockage des journaux sur les équipements.

2.1 Fonction de journalisation

Pour pouvoir journaliser l'activité d'un SI, il est nécessaire que les équipements de ce SI aient la capacité de générer des évènements qui seront préférentiellement stockés dans des journaux locaux, et, dans des cas plus rares, qui seront transférés, via le réseau, sur un serveur du SI.

Si les systèmes d'exploitation incluent en général nativement des fonctionnalités de journalisation, cela n'est pas forcément le cas pour des applications, et en particulier des applications développées pour des besoins métier spécifiques. C'est la raison pour laquelle la fonctionnalité de journalisation doit être prise en compte dans les cahiers des charges fonctionnels et techniques au lancement d'un projet informatique. Il doit ainsi être possible d'enregistrer des évènements liés à la sécurité (p. ex. l'authentification des utilisateurs) ainsi qu'à l'activité correspondant au service fourni par l'applicatif (par exemple l'accès à une ressource). C'est également dès la phase de conception que doivent être prises en compte les exigences réglementaires en matière de journalisation. S'agissant notamment des journaux métier, il convient de minimiser l'inclusion de données à caractère personnel dans les données de journalisation et de prévoir un mécanisme permettant leur suppression automatique au delà de leur durée de rétention réglementaire [4].

Les journaux doivent être générés dans un format interprétable, c'est-à-dire compréhensible à la lecture par un humain et structuré pour être analysable de manière automatique par des outils informatiques. Les évènements inscrits dans les journaux doivent être composés de champs fixes à la grammaire bien définie, celle-ci pouvant évoluer en fonction des versions des logiciels qui génèrent les journaux [5].

4. Pour plus d'informations concernant les durées de rétention des journaux, se reporter à la section 3.4.5.
5. Il est recommandé que les mises à jour entraînant un changement de syntaxe ou de sémantique soient facilement distinguables, par exemple, au moyen d'un champ numérique « version » systématiquement incrémenté.

Un évènement doit contenir en particulier une source identifiable (un équipement, un utilisateur, un nom de processus ou plusieurs de ces éléments) permettant de déterminer avec le plus de précision possible son origine. Les identifiants utilisés pour nommer les sources doivent être intelligibles (p. ex. pour désigner un serveur de messagerie, l'identifiant « SRV-MSG-001 » sera préféré à l'identifiant « 47834456678 »).

L'absence de journaux rend difficile, voire impossible, la production de rapports et le diagnostic en cas de problème et peut, dans certains cas, constituer une infraction (se reporter à l'annexe D). La présence et l'exploitation des journaux contribuent au maintien en conditions de sécurité de l'ensemble des briques qui constituent un SI et sont un prérequis à la détection des incidents de sécurité (se reporter à l'annexe C).

R1

Utiliser des solutions disposant d'une fonction de journalisation native

Il est fortement recommandé d'utiliser des systèmes et des applications disposant nativement d'une fonction de journalisation. Cette fonction de sécurité doit être exigée par les responsables de SI en phase amont de tout projet informatique (en étant intégrée aux appels d'offres) et être spécifiée au plus tôt par les concepteurs de nouveaux produits informatiques (éditeurs logiciels, industriels…).

La détection des incidents est d'autant plus efficace que le périmètre de collecte des journaux tend vers l'exhaustivité : journaux de tous les systèmes d'exploitation, journaux des équipements réseau (*proxy*, pare-feux, etc.), journaux des postes de travail (p. ex. générés par une solution de type *EDR* [6]), journaux des applications. La journalisation des équipements du SI les plus exposés et les plus critiques doit être prioritaire.

R2

Activer la journalisation sur un nombre important d'équipements du SI

La journalisation doit être activée et paramétrée sur un large nombre d'équipements du SI, en commençant par ceux qui composent les *passerelles Internet sécurisées* [10] et par ceux qui supportent les valeurs métiers [14] les plus importantes ou qui disposent d'un chemin de contrôle permettant d'accéder à ces données (postes d'administration, serveurs de mise à jour, serveurs d'annuaire, hyperviseurs, serveurs de sauvegarde…).

Attention

Étendre le périmètre de journalisation ne signifie pas que la sélection des types d'évènements à collecter ou que les niveaux de verbosité doivent être configurés de façon maximaliste. Au contraire, cette sélection et cette verbosité doivent être adaptées au contexte du système d'information considéré et aux objectifs de détection qui y sont associés. L'annexe A liste les catégories d'évènements qu'il est pertinent de collecter pour constituer un *socle minimal de journalisation*.

6. *Endpoint detection and response*.

2.2 Horodatage des évènements

Un évènement journalisé n'est pertinent que si celui-ci peut être situé dans le temps, et ce pour plusieurs raisons :

- la signification de cent occurrences d'un même évènement n'est pas la même selon que ces évènements sont générés en une journée ou en dix minutes. Dans le premier cas, il peut s'agir par exemple d'un fonctionnement normal, alors que dans le second, cela peut être caractéristique d'un incident de sécurité. La fréquence d'occurrence d'un évènement peut donc être un élément essentiel pour détecter un incident de sécurité et apprécier sa gravité ;
- l'horodatage d'un évènement peut aider à déterminer la nature de celui-ci. Par exemple, un évènement sera interprété différemment suivant qu'il survient le jour ou la nuit ;
- la détection d'un incident ou sa compréhension *a posteriori* nécessite généralement le croisement de journaux issus de différents équipements. L'absence d'horodatage homogène des évènements rend très difficile le recoupement des informations (se référer à la section 2.3).

R3

Horodater les évènements

L'horodatage doit être activé pour l'ensemble des évènements afin de permettre une meilleure exploitation des journaux.

R4

Homogénéiser les paramètres d'horodatage

Une attention particulière doit être accordée à l'homogénéité de la configuration des paramètres d'horodatage (fuseau horaire de référence, précision de la date…) faute de quoi l'agencement de évènements dans les journaux pourrait ne pas refléter le déroulement chronologique réel des faits ayant conduit à l'enregistrement de ces évènements. Une synchronisation des horloges avec une précision minimale à la seconde est recommandée.

2.3 Synchronisation des horloges

L'ensemble des équipements informatiques dispose normalement d'une horloge interne utilisée entre autres pour horodater les journaux d'évènements. Cependant, les horloges de tous les équipements dérivent naturellement dans le temps. Si les écarts peuvent paraître minimes de prime abord, ils peuvent se mesurer en secondes voire en minutes après plusieurs semaines.

Il est par conséquent crucial de disposer d'équipements synchronisés sur la même source de temps, sans quoi des évènements pourraient ne pas être pris en compte dans l'analyse, rendant celle-ci moins efficace. Il est ainsi recommandé de disposer de sources de temps fiables et utilisées par l'ensemble des équipements qui composent le SI.

NTP (*Network Time Protocol*) est le protocole le plus fréquemment utilisé pour la synchronisation des horloges des équipements avec des sources de temps. Il est disponible pour la plupart des systèmes d'exploitation, quel que soit le type d'équipement. Une architecture NTP comprend

généralement un ou plusieurs serveurs NTP internes sur lesquels se synchronise l'ensemble des machines du SI. Ces serveurs référents peuvent, quant à eux, calibrer leurs horloges à l'aide de matériel spécifique (intégrant une horloge atomique ou utilisant les signaux radio ou satellitaires par exemple) ou bien se synchroniser avec des serveurs accessibles publiquement sur Internet [7]. Pour les besoins de journalisation, la cohérence des horloges au sein du SI est nécessaire. La recherche d'une précision accrue vis-à-vis du temps universel sera motivée uniquement par des besoins métier spécifiques.

Dans le cas de SI physiquement isolés, il n'est en général pas nécessaire, ni même recommandé, de disposer de serveurs de temps synchronisés sur des sources externes ; en revanche, il est indispensable que les équipements soient synchronisés sur les mêmes sources de temps internes cohérentes entre elles.

R5

Synchroniser les horloges des équipements sur des sources de temps cohérentes entre elles

Les horloges des équipements doivent être synchronisées sur plusieurs sources de temps internes cohérentes entre elles. Ces dernières peuvent elles-mêmes être synchronisées sur plusieurs sources de temps externes fiables, sauf dans le cas particulier de réseaux physiquement isolés. Si NTP est utilisé, il est recommandé d'utiliser la même version du protocole sur l'ensemble du SI et d'en assurer le maintien en condition de sécurité.

Lorsque les équipements sont répartis géographiquement sur des fuseaux horaires différents, il est important d'adopter une logique de configuration adéquate. Cette configuration doit permettre à la fois de reconstituer une cohérence temporelle des journaux au niveau des serveurs de collecte (et ainsi permettre la corrélation d'évènements issus d'équipements différents) mais aussi de pouvoir appliquer des règles de détection s'appuyant sur l'horaire « local » de l'équipement (p. ex. détection d'évènements suspicieux survenant en heures non ouvrées).

Dans certains cas, le choix d'un même fuseau horaire sur l'ensemble des équipements peut être nécessaire (p. ex. il peut être pertinent de configurer l'heure UTC s'il n'est pas certain que les systèmes gèrent correctement les passages heure d'été/heure d'hiver).

Information

La nome internationale ISO 8601 [1] peut être utilisée pour uniformiser le format des horodatages des évènements de sécurité.

2.4 Configuration des politiques de journalisation sur les équipements

Il est important de procéder à la sélection des évènements journalisés par les différents équipements du SI. Journaliser la totalité des évènements peut entraîner une consommation excessive des ressources (processeur, mémoire, stockage, bande passante, etc.) et engendrer une quantité

7. Le site Web de RENATER propose par exemple une liste [17] de serveurs de temps français.

de données difficilement exploitable. À l'inverse, une politique de journalisation trop ciblée ne produira pas suffisamment de données utiles.

L'annexe A donne des éléments de réflexion pour définir une politique de journalisation minimale sur les équipements.

R6

Identifier la granularité de journalisation des équipements

Pour chaque équipement à journaliser, il est nécessaire de sélectionner les types d'évènements devant être stockés. Cette politique de journalisation prend notamment en compte les capacités de stockage, de collecte et de traitement des évènements ainsi que les besoins de sécurité de l'équipement.

Attention

Il convient d'être vigilant quant à l'utilisation de modes de configuration de la journalisation qui génèrent un nombre très important d'évènements (mode *debug*, mode *verbose*…). Outre que ces modes ne sont généralement pas recommandés en fonctionnement nominal, ils peuvent aussi être potentiellement révélateurs d'informations sensibles (typiquement des secrets).

Enfin, lorsque des fichiers malveillants ou potentiellement malveillants sont détectés par des solutions de sécurité (antivirus, anti-pourriels, etc.), des évènements de sécurité sont journalisés en conséquence, que ce soit dans des journaux du système d'exploitation ou dans des journaux au format propriétaire. Lorsque les solutions de sécurité le permettent, il est utile au service de détection des incidents que la journalisation de ces évènements inclue les empreintes associées à ces fichiers potentiellement malveillants [8].

R7

Journaliser les empreintes des fichiers potentiellement malveillants

Il est recommandé de configurer les solutions logicielles de sécurité déployées sur le SI pour qu'elles journalisent les empreintes des fichiers potentiellement malveillants.

2.5 Dimensionnement des équipements

2.5.1 Espace disque

Les journaux sont généralement stockés localement sur un équipement sous forme de texte compressé. Ils peuvent vite représenter des quantités de données importantes et provoquer une saturation de l'espace de stockage des équipements. Il est donc recommandé de prendre en compte les besoins d'espace disque nécessaires au stockage des journaux lors du dimensionnement des équipements. Les sections suivantes abordent la rotation des journaux (section 3.4.4) et la mise en place de mécanismes d'export (recommandations R9 et R9-), ces mesures peuvent contribuer à la mise en œuvre de cette recommandation.

8. Les empreintes se calculent généralement au moyen des fonctions de hachage (p. ex. : MD5, SHA-1, SHA-256).

R8

Estimer l'espace de stockage dédié aux journaux sur les équipements

Lors du dimensionnement des équipements qui génèrent des évènements, il est recommandé d'estimer l'espace de stockage local nécessaire à la conservation des journaux. Cette estimation de l'espace nécessaire doit notamment prendre en compte l'éventualité d'une indisponibilité temporaire des serveurs de collecte.

2.5.2 Résistance à la charge

Quel que soit le sous-ensemble qui génère des journaux (système d'exploitation, application, etc.) il est important de connaître son comportement vis-à-vis de l'activité de journalisation en cas de charge anormale prolongée. Il convient d'être en particulier attentif au fait que des évènements pourraient être perdus dans le cas où les ressources disponibles s'avéreraient insuffisantes. En conséquence, le dimensionnement système (CPU, RAM, espace disque…) de l'équipement et la configuration du niveau de verbosité des services de journalisation doivent être adaptés au contexte d'usage.

3
Architecture et conception d'un système de journalisation

Objectif

Le présent chapitre donne les recommandations visant à concevoir un système de journalisation et à l'insérer de façon cohérente au sein d'un système d'information (SI) sécurisé.

3.1 Collecte et centralisation des journaux

L'export des journaux consiste à copier les évènements vers une machine différente de celle qui les a générés.

Cette mesure est nécessaire pour plusieurs raisons :

- les équipements qui génèrent les journaux peuvent ne pas disposer de l'espace disque nécessaire pour stocker une quantité suffisante de journaux au regard des contraintes métier ou réglementaires (se reporter à l'annexe D). La copie des journaux doit donc être réalisée vers des équipements différents, correctement dimensionnés ;
- si l'analyse des journaux a lieu dans le cadre d'investigations faisant suite à un incident de sécurité, il est possible que les journaux ne soient plus présents sur l'équipement source (effacement volontaire par un attaquant, défaillance matérielle, etc.). L'export permet de disposer d'une copie sur des équipements physiquement distincts.

La centralisation des journaux est un moyen d'exporter les journaux et de faciliter leur exploitation. Ce mode de fonctionnement comporte plusieurs avantages :

- la consultation des journaux est simplifiée : les personnes en charge de leur exploitation n'ont pas à se connecter sur plusieurs équipements pour rechercher de l'information ;
- le recoupement d'informations provenant de journaux d'équipements différents est plus aisé lorsque ceux-ci sont stockés au même endroit ;
- la sauvegarde des journaux est facilitée.

R9

Centraliser les journaux

Les journaux de l'ensemble des équipements du SI doivent être collectés puis transférés sur un ou plusieurs serveurs centraux dédiés.

S'il n'est pas possible de mettre en œuvre la centralisation des journaux, une recommandation dégradée est de les exporter vers un autre équipement de manière à réduire le risque de perte et de permettre des investigations en cas d'incident de sécurité.

R9 -

Exporter les journaux vers un autre équipement

À défaut de mettre en œuvre la centralisation des journaux, il est recommandé d'exporter les journaux générés par un équipement vers un autre équipement.

Si la taille du SI est très importante (plusieurs milliers d'équipements) ou si celui-ci est composé de nombreuses entités (sites physiques, entités fonctionnelles), il est nécessaire d'assurer la résilience du système de journalisation. En effet, une indisponibilité même de courte durée peut entraîner la perte de journaux.

R10

Construire un service résilient de collecte des journaux

Si le parc d'équipements qui génère des journaux est important, le système de journalisation doit être redondé afin d'accroître la disponibilité du service de collecte de journaux.

Dans certains cas, il peut être pertinent d'adopter une organisation hiérarchique du système de journalisation. Des serveurs intermédiaires collectent les journaux des équipements correspondant à leur périmètre physique ou fonctionnel, puis ils les transmettent aux serveurs de collecte centraux qui ont la charge d'agréger la totalité des journaux du SI ou d'un sous-ensemble spécifique (base de données, système, etc.). Les serveurs de collecte intermédiaires dupliquent également les journaux et les conservent localement afin d'éviter les pertes en cas de dysfonctionnement lors du transfert au niveau supérieur. Une organisation de ce type comporte plusieurs avantages :

- la résilience de l'architecture de journalisation est meilleure : les serveurs intermédiaires peuvent pallier une indisponibilité des serveurs centraux. La copie des journaux conservée sur ces serveurs intermédiaires pourra être transmise au niveau central une fois la communication rétablie. Cela nécessite la configuration d'une politique de rétention adéquate, c'est-à-dire adaptée à la volumétrie et aux exigences de disponibilité des serveurs centraux ;
- le nombre de flux réseau de journalisation est réduit, ce qui peut contribuer à un meilleur contrôle des matrices de flux des équipements de filtrage réseau ;
- les serveurs intermédiaires peuvent apporter des fonctionnalités additionnelles dans la transmission des journaux (comme la compression ou le chiffrement), ce qui est particulièrement utile si des liens de faible capacité ou non sûrs sont utilisés pour véhiculer les journaux jusqu'aux serveurs centraux.

Conformément à la recommandation R10, il est recommandé de redonder également les serveurs de collecte intermédiaires.

R11

Hiérarchiser les serveurs constituant le système de journalisation

Si la taille ou la typologie du SI le nécessite, une approche hiérarchique pour l'organisation des serveurs de collecte, associant serveurs de collecte intermédiaires et centraux, doit être retenue.

L'annexe B donne des exemples d'architectures possibles pour un système de journalisation.

Attention

La recommandation R11 ne doit pas être recherchée à tout prix. Les serveurs intermédiaires complexifient l'architecture et peuvent affaiblir la robustesse du système de journalisation (panne, absence de redondance des serveurs intermédiaires…). Dans certains cas, il peut être préférable d'opter pour une architecture plus simple mais mieux maîtrisée par les exploitants du SI.

3.2 Supervision de la chaîne de collecte des évènements de sécurité

Il arrive de constater que des solutions logicielles en œuvre sur le SI ne remplissent pas les missions pour lesquelles elles ont été déployées. Cela peut être dû à des défauts de configuration, des dysfonctionnements matériels, des défauts de conception, etc. C'est ce qui amène, par exemple, à ce qu'un plan de reprise d'activité insuffisamment testé s'avère non opérationnel le jour où un incident majeur se produit. De la même manière, la chaîne de collecte des évènements de sécurité est un sous-ensemble critique du SI. À ce titre, les serveurs qui la constitue doivent eux-mêmes être configurés pour générer des journaux et leur bon fonctionnement doit être régulièrement contrôlé.

R12

Contrôler régulièrement la couverture de la chaîne de collecte des évènements

Il est recommandé de vérifier régulièrement que tous les systèmes du SI sont bien journalisés (sauf exceptions dûment identifiées) et transfèrent leurs évènements à des serveurs de collecte des journaux. Le bon fonctionnement de ces serveurs de collecte (intermédiaires et centraux) doit également être vérifié en continu (supervision opérationnelle et supervision de sécurité).

3.3 Protection des données échangées

3.3.1 Prétraitement des journaux

Lorsque le responsable d'un SI a la possibilité de spécifier les formats des journaux qui seront nativement produits par des systèmes ou des applications, alors il est judicieux de s'efforcer d'harmoniser ces formats autant que possible. Au contraire, dans le cas où le responsable du système d'information n'a pas cette latitude (p. ex. utilisation de logiciels commerciaux), il est déconseillé de modifier le format des journaux sur les machines émettrices avant leur envoi vers des serveurs de collecte. En effet, ce traitement en amont qui viserait à unifier au plus tôt la mise en forme des journaux pourrait conduire à dénaturer les évènements et induire des pertes d'information. Les actions de conversion doivent être réalisées de préférence à l'aide d'outils installés sur les serveurs centraux, une copie non altérée des journaux y étant conservée pour archivage.

R13

Conserver les journaux dans leur format natif avant leur transfert

Il est recommandé de ne pas effectuer de traitement sur les journaux avant leur transfert vers les serveurs centraux.

Attention

Une attention particulière doit être accordée au sous-système de journalisation natif d'un équipement quand ce sous-système ne stocke pas, dans un évènement, un intitulé textuel explicite mais un code qui sera utilisé, à la réception, pour reconstituer un contenu signifiant pour l'administrateur. Dans ce cas, il convient de veiller à ce que les serveurs de journalisation centraux auront la capacité à recouvrer l'information pertinente par une analyse de ces codes ou, en alternative, de remplacer ce sous-système de journalisation natif par un sous-système tiers qui ne met pas en œuvre cette couche d'abstraction.

3.3.2 Transfert en temps différé ou en « temps réel »

Il existe deux modes de transfert de journaux vers les serveurs centraux : soit en « temps réel », soit en temps différé. Chacun de ces deux modes a des avantages et des inconvénients.

Transfert en « temps réel »

Ce mode consiste à transférer les journaux vers les serveurs centraux au moment où ils sont produits, une copie étant généralement conservée localement par l'équipement qui génère les évènements. Ce mode présente l'avantage de rendre les journaux rapidement disponibles en consultation sur les serveurs centraux mais peut poser des problèmes réseau. En effet, l'envoi de journaux peut consommer une bande passante très importante et perturber les autres services (flux d'administration ou de supervision par exemple) même si ces données transitent sur un réseau dédié à l'administration (se reporter au paragraphe 3.3.6).

Transfert en temps différé

Ce mode consiste à transférer périodiquement les journaux sur des serveurs centraux (tous les jours par exemple). Il présente l'avantage de ne pas consommer de façon permanente de la bande passante. Par exemple, le transfert de l'ensemble des journaux peut être réalisé pendant les horaires non ouvrés afin d'éviter d'influer sur les autres services au niveau du réseau. Ce mode présente cependant l'inconvénient de retarder la mise à disposition des journaux en consultation au niveau central. Il est également plus risqué dans la mesure où si un incident de sécurité se produit entre deux envois de journaux, il ne pourra pas forcément être détecté (par exemple si un attaquant efface ou modifie volontairement les journaux pour masquer son activité).

Le mode de transfert en « temps réel » présente l'avantage de rendre les journaux immédiatement disponibles sur les serveurs de collecte. Il doit être mis en œuvre après une évaluation de son impact sur la bande passante.

R14

Privilégier un transfert des journaux en « temps réel »

Chaque fois que le contexte le permet, le transfert en « temps réel » des journaux vers les serveurs de collecte doit être privilégié.

R14 -

Adopter un transfert des journaux en temps différé

À défaut de pouvoir transférer les journaux en « temps réel », il est recommandé d'automatiser leur transfert vers les serveurs de collecte au plus tard quelques heures après leur génération.

3.3.3 Transfert en mode pull ou en mode push

Le transfert des journaux vers les serveurs centraux, qu'il soit fait en temps différé ou en temps réel, peut être provoqué soit par l'équipement qui les génère (mode *push*), soit par le serveur de collecte (mode *pull*). Il n'existe pas de recommandation générique qui permettrait de préférer un mode à l'autre, quelle que soit l'implémentation retenue. Le choix doit être fait sur la base du niveau de sensibilité de l'équipement qui génère les journaux mais aussi par les risques induits que l'ajout de ce mode de journalisation fait peser sur le SI. À titre d'illustration, le mode *push* authentifié ouvre la voie aux attaques par relais d'authentification, tout en augmentant la surface d'attaque des serveurs centraux, tandis que le mode *pull* peut nécessiter un compte de service disposant de droits d'authentification sur de nombreuses ressources du SI. Une fois le mode de transfert des journaux retenu, une attention particulière doit être portée sur la minimisation des risques induits (p. ex. : mettre en place un filtrage IP pour permettre l'envoi des journaux vers les seuls serveurs de collecte, utiliser un compte de service pour le mode *pull* doté d'un mot de passe robuste et régulièrement changé et disposant de privilèges réduits, forcer l'authentification par Kerberos pour minimiser les attaques par relais…).

R15

Faire une analyse de risque pour déterminer le mode de transfert des journaux

Le choix du mode de transfert des journaux (mode *pull* ou mode *push*) doit être déterminé au cas par cas après une analyse de risque prenant en comptes le niveau de sensibilité du serveur collecté et du collecteur, ainsi que la surface d'attaque induite par la solution technique retenue pour ce transfert.

3.3.4 Fiabilisation du transfert des journaux

Les applications de transfert de journaux reposent sur les protocoles TCP ou UDP pour acheminer les données vers les équipements centraux. Le plus simple des deux, le protocole UDP, présente l'avantage de prendre le minimum de ressources mais il a l'inconvénient d'être peu fiable car sujet aux pertes définitives de paquets. Le protocole TCP, quant à lui, améliore la fiabilité du transfert des journaux en ajoutant des fonctions de ré-émission de paquets, de mise en cache du côté de l'émetteur et d'acquittement envoyés par le destinataire. Il est donc à privilégier par rapport au protocole UDP.

R16

Utiliser des protocoles fiables pour le transfert des journaux

Il est recommandé d'utiliser des protocoles d'envoi de journaux reposant sur TCP pour fiabiliser le transfert de données entre les machines émettrices et les serveurs.

Cependant, l'usage du protocole TCP ne suffit pas à lui seul à garantir l'absence de perte de données. D'autres mécanismes présents au niveau applicatif permettent d'améliorer encore la fiabilité du transfert en ajoutant des fonctionnalités de cache et d'acquittement plus efficaces.

3.3.5 Sécurisation du transfert des journaux

Il est nécessaire de mettre en place des mécanismes de protection garantissant la confidentialité et l'intégrité des flux de transfert des journaux, en particulier lorsque les données transitent sur des réseaux non maîtrisés. Le besoin en confidentialité est aussi fonction de la sensibilité des informations journalisées. L'idéal est de mettre en place un canal de transmission dédié réalisé à l'aide de mécanismes cryptographiques robustes [11]. Idéalement, ce canal doit être établi après authentification mutuelle de la machine émettrice et du serveur de collecte en utilisant des certificats issus d'une autorité de certification de confiance. Il existe pour certains protocoles de transfert de journaux une version sécurisée utilisant TLS [9] qui permet de répondre à ces exigences. Si le protocole de transfert de journaux ne dispose pas nativement de mécanismes de chiffrement ou de signature, il est possible de s'appuyer sur des protocoles tels que SSH [4] ou IPsec [7].

R17

Utiliser des protocoles sécurisés pour le transfert des journaux

Il est recommandé d'assurer la confidentialité et l'intégrité des journaux transférés, ainsi que l'authentification des serveurs de collecte, à l'aide de protocoles qui s'appuient sur des mécanismes cryptographiques robustes, en particulier lorsque les données transitent sur des réseaux non maîtrisés.

Attention

Si les protocoles sécurisés mettent en œuvre des certificats numériques, une attention particulière doit être accordée à la gestion de leur cycle de vie (expiration, révocation …), pour ne pas risquer de porter atteinte à la disponibilité du service de journalisation.

3.3.6 Bande passante

Quel que soit le mode de transfert utilisé pour acheminer les journaux des machines sources vers les serveurs centraux (temps réel ou temps différé), il est nécessaire de garder la maîtrise de l'usage des ressources réseau en cas de transferts volumineux. L'activation des mécanismes de limitation de bande passante ou de priorisation des flux permet d'atteindre cet objectif, et ce même si l'envoi des journaux a lieu en dehors des horaires métier (en temps différé). À défaut, il est possible de superviser les flux réseau et de déclencher des alertes en cas de contention réseau.

R18

Maîtriser le flux réseau consommé par les transferts de journaux

Il est recommandé de limiter la consommation de bande passante des flux réseau utilisée pour transférer les journaux d'évènements. Si la limitation de bande passante ou la priorisation des flux n'est pas possible, il est recommandé de superviser ces flux.

3.3.7 Sécurisation des serveurs de collecte

Le mode *pull* décrit en section 3.3.3 peut présenter des risques importants si un serveur de collecte est compromis ; l'attaquant peut ainsi obtenir des authentifiants valides sur un ensemble conséquent de machines du SI.

En outre, les informations stockées sur les serveurs de collecte sont susceptibles d'être des cibles de choix pour un attaquant cherchant à effacer ses traces, dissimuler ses activités et complexifier les activités de détection des incidents de sécurité.

Il est donc indispensable de sécuriser les serveurs de collecte : la configuration système de ces serveurs doit être durcie et ils doivent être cloisonnés d'un point de vue réseau.

R19

Durcir et maintenir à jour les serveurs de collecte

Les serveurs de collecte doivent être durcis et une attention particulière doit être accordée à leur maintien en condition de sécurité.

L'utilisation d'un SI d'administration dédié est une bonne pratique qui doit être privilégiée (se reporter au guide ANSSI portant sur l'administration sécurisée d'un SI [12]). Lorsqu'il existe, ce SI doit être utilisé en priorité pour faire transiter les flux de collecte des journaux générés par les équipements administrés. Cette solution met à disposition de fait une bande passante plus importante sans affecter la disponibilité des services métier et peut, lorsque la sensibilité des informations transmises le justifie, apporter une protection supplémentaire.

Les serveurs de collecte, intermédiaires ou centraux, doivent être hébergés préférentiellement dans une zone dédiée du SI d'administration et sans lien logique avec les serveurs outils d'administration [9].

R20

Cloisonner les serveurs de collecte au sein d'un SI d'administration

Lorsque le besoin de sécurité pour le traitement des journaux est important, celui-ci doit se faire dans une zone dédiée du SI d'administration ; les serveurs de collecte intermédiaires et centraux doivent être hébergés sur ce SI d'administration.

R20 -

Cloisonner les serveurs de collecte dans une zone dédiée

S'il n'existe pas de SI d'administration dans l'architecture pour accueillir les serveurs de collecte intermédiaires et centraux, ils doivent être placés dans une zone interne dédiée, non exposée directement à des réseaux qui ne sont pas de confiance (p. ex. Internet).

9. Se reporter au guide [12] pour en savoir plus sur les *serveurs outils*.

3.4 Stockage

Les recommandations qui suivent sont applicables à l'ensemble des équipements qui composent l'architecture de journalisation : équipements source, serveurs de collecte intermédiaires et centraux.

3.4.1 Partition dédiée

Sur les équipements qui produisent ou collectent des journaux, si les fichiers de journalisation n'ont pas une taille maximale fixée, il est recommandé de créer une partition dédiée aux journaux d'évènements et disposant de droits d'accès restreints. Cette mesure permet d'éviter la défaillance du système ou de certains services qui n'auraient pas d'espace disque suffisant pour fonctionner correctement.

R21

Dédier une partition disque au stockage des journaux

Une partition disque doit être dédiée au stockage des journaux d'évènements sur les équipements qui les génèrent ou qui les collectent. Cette recommandation n'est réellement pertinente que dans le cas où les fichiers de journalisation n'ont pas des tailles maximales fixées.

Attention

Des journaux pourraient être perdus si la partition dédiée venait à être saturée à son tour, ou, dans le cas où les fichiers de journalisation ont une taille maximale fixée, si ces fichiers venaient à être saturés d'évènements. Pour ces raisons, l'accès en écriture à la partition dédiée doit être réservé aux seuls processus dûment autorisés par l'administrateur de l'équipement et une politique adéquate de rotation et de supervision des journaux doit être mise en œuvre en complément de cette mesure (se reporter aux sections 3.4.4 et 3.4.2).

3.4.2 Supervision de l'espace disque

Il est recommandé de superviser l'espace disque restant sur les espaces de stockage locaux des équipements qui génèrent ou collectent les journaux pour plusieurs raisons :

- de nombreux incidents opérationnels entraînant l'indisponibilité de services ont pour origine une saturation de l'espace de stockage local par les journaux ;
- si l'espace disque est saturé, des journaux pourraient être perdus (p. ex. en cas de mauvaise configuration de la politique de rotation des journaux) ;
- une activité de journalisation anormale peut être détectée. Si un équipement journalise dans des proportions inhabituelles par rapport à une activité normale ou s'il ne journalise pas du tout, il est possible qu'un incident soit en cours sur la machine ;
- l'ajout de nouveaux équipements dans le SI induit l'envoi de nouveaux journaux, il est important d'anticiper les besoins en espace disque des équipements centraux.

R22

Superviser l'espace disque de stockage des journaux

L'espace disque des équipements qui génèrent et stockent les journaux doit être supervisé.

L'analyse par des exploitants du SI des alarmes déclenchées lors du dépassement de seuils d'alerte (p. ex. pourcentage d'espace disque disponible restant) permet d'anticiper une saturation de l'espace de stockage des équipements.

3.4.3 Arborescence de fichiers ou base de données indexée

Un équipement générant des journaux peut être amené à stocker différents types d'évènements (système d'exploitation, applications, etc.). Il peut être utile de stocker les journaux dans une arborescence de répertoires définie à l'aide de thématiques : authentification, applicatifs métier, Web, etc.

R23

Classer les journaux suivant leur thématique

Il est recommandé de stocker les journaux d'évènements dans une arborescence de répertoires classés par thématiques.

D'autres solutions (équipements, applications, sous-système *cloud*…) n'offrent pas nécessairement la possibilité de stocker les journaux dans une arborescence de fichiers « à plat ». Leurs évènements sont stockés dans une base de données. L'indexation des évènements rend possible des recherches adaptées aux besoins de détection et d'analyse automatisées des incidents de sécurité.

R23 +

Privilégier le stockage des journaux dans une base de données indexée

Quand cela est possible, il est recommandé de privilégier des solutions permettant le stockage des journaux dans une base de données indexée et la conservation d'une copie des journaux non transformés.

Information

La recommandation R23 est applicable aux équipements générant des journaux. Pour les serveurs de collecte intermédiaires et les serveurs de collecte centraux, on privilégiera des fonctionnalités d'indexation poussées plutôt que de la classification par arborescence.

3.4.4 Rotation des journaux

La mise en œuvre d'une politique de rotation des journaux consiste à configurer des mécanismes de traitement automatique qui permettent de conserver l'exploitabilité des journaux dans la durée tout en limitant l'espace disque utilisé. Le déclenchement de la rotation des fichiers de journaux peut dépendre de contraintes temporelles (rotation tous les jours à minuit), ou de la taille du journal (rotation si le fichier atteint 100 Mo). Le choix dépend des exigences et des contraintes spécifiques au SI.

Voici les traitements qui peuvent être réalisés lors de la rotation des journaux :

- **séparation des fichiers** : un nouveau fichier est créé au moment de la rotation pour éviter que les évènements soient stockés dans un seul fichier de taille trop importante. Les fichiers ainsi générés sont généralement nommés selon un format qui inclut la date et l'heure de création ainsi que le type de journal ;
- **compression** : les fichiers créés au moment de la rotation sont habituellement compressés afin de réduire leur occupation sur le disque ;
- **effacement** : pour éviter la saturation de l'espace disque local, les fichiers de journaux les plus anciens peuvent être effacés automatiquement lors de la rotation. Il convient de s'assurer que les journaux détruits ont été correctement exportés au préalable. Une durée de rétention adéquate doit donc être définie, elle sera fonction de l'espace disque disponible ainsi que des contraintes éventuelles d'exploitation. Dans le cas des serveurs centraux, cette durée doit être supérieure à l'écart qui sépare deux sauvegardes. Dans les autres cas (équipements source et serveurs de collecte intermédiaires), cette durée doit être supérieure à l'écart qui sépare deux envois de journaux si le mode de transfert en temps différé est employé.

R24

Définir et appliquer une politique de rotation des journaux

Une politique de rotation des journaux d'évènements doit être formalisée et mise en œuvre sur l'ensemble des équipements du système de journalisation.

3.4.5 Durée de rétention des journaux

La durée de rétention des journaux est fixée par le cadre légal. D'autres exigences réglementaires spécifiques peuvent s'appliquer en fonction du contexte métier. Charge au lecteur de se renseigner auprès d'un organisme juridique afin de déterminer celles qui sont applicables au sien. L'annexe D aborde certaines exigences réglementaires relatives à la journalisation.

Dans le cas général, la Commission nationale de l'informatique et des libertés (CNIL) recommande une durée de conservation des journaux pendant une durée comprise entre six mois et un an [10]. Dans des cas particuliers, cette durée peut être portée à trois ans [11].

Il a été rappelé dans les objectifs du guide (section 1.1) l'importance d'exploiter en continu les journaux collectés sur un SI et de mettre en œuvre un système de détection des incidents de sécurité. La détection d'une attaque avérée ou suspectée est un cas valide pour justifier d'une conservation de journaux au-delà de leur durée réglementaire [12].

Tel que cela est précisé en section 2.1, il est recommandé de prévoir, dès la conception de toute solution génératrice de journaux, un mécanisme technique permettant la suppression automatique des évènements au-delà d'une durée de rétention qui aura été configurée conformément aux exigences réglementaires. Ce point est plus particulièrement applicable au cas des applications

10. Se reporter au point 8 du document [3] de la CNIL.
11. Se reporter au point 19 du document [3] de la CNIL. Ce point précise en outre *qu'il n'est pas possible de motiver la durée de conservation des données de traçabilité par la seule durée de prescription des infractions pénales délictuelles liées au mésusage des données du traitement par ceux qui y accèdent*.
12. Se reporter au point 20 du document [3] de la CNIL.

métier, lesquelles sont par nature plus susceptibles de générer des évènements contenant des données personnelles. Ce principe de suppression automatisée des journaux au-delà de leur durée de rétention légale est également applicable aux journaux collectés sur les serveurs de collecte (intermédiaires ou centraux).

R25

Configurer des durées de rétention des journaux conformes à la réglementation

La durée de conservation des fichiers de journaux étant soumise à des exigences réglementaires, il convient d'en prendre connaissance pour définir les moyens techniques nécessaire à la suppression des journaux. Dans la mesure du possible, il est recommandé d'automatiser cette suppression.

3.4.6 Protection des journaux

Par application du principe de moindre privilège, chaque journal doit être accessible uniquement à partir de comptes pour lesquels il existe des justifications opérationnelles à l'octroi de ces privilèges. Restreindre les accès aux journaux au seul personnel autorisé et sensibilisé [13] est également de nature à réduire le risque d'une réutilisation en détournement de finalité des données de journalisation collectées [14] (lesquelles sont susceptibles de contenir des informations personnelles résiduelles si le principe de minimisation des données à caractère personnel n'a pas pu être mis complètement en pratique).

R26

Restreindre au strict besoin opérationnel les droits d'accès en écriture aux journaux

L'accès à chaque journal doit être limité en écriture (pour l'écriture de nouveaux évènements) aux seuls comptes utilisateurs (compte de personne ou compte de service) dont le rôle ou la fonction le justifie.

R26 +

Restreindre au strict besoin opérationnel les droits de suppression des journaux

Si le système d'exploitation ou l'application le permet, il est recommandé que seuls les comptes utilisateurs dédiés à l'administration privilégiée des équipements disposent des droits de suppression des journaux.

R27

Restreindre au strict besoin opérationnel les droits d'accès en lecture aux journaux

L'accès à chaque journal doit être limité en lecture (pour la consultation des évènements journalisés) aux seuls comptes utilisateurs (compte de personne ou compte de service) dont le rôle ou la fonction le justifie.

13. Les administrateurs d'un SI doivent être sensibilisés à leurs droits et à leurs devoir. Se reporter au guide [12] de l'ANSSI relatif à l'administration sécurisée des SI.
14. Se reporter au point 11 du document [3] de la CNIL.

Les recommandations R26, R26+ et R27 s'appliquent aussi bien aux équipements qui génèrent des journaux qu'aux serveurs de collecte intermédiaires et centraux.

3.5 Externalisation

3.5.1 Journalisation en cas d'externalisation du SI

Dans le cas de l'externalisation de tout ou partie du SI, en particulier vers un *cloud* public, le sujet de la journalisation doit être explicitement traité, qu'il s'agisse des capacités du prestataire à générer des journaux ou à les exporter.

Quel que soit le niveau d'externalisation (une infrastructure complète, une application en mode *SaaS* [15] ou une situation intermédiaire dite « hybride »), il convient d'évaluer le prestataire sur :

- sa capacité à générer des journaux sur les solutions retenues ;
- sa capacité à stocker les journaux de manière sécurisée ;
- sa capacité à exporter les journaux et à les rendre disponibles pour le client [16] ;
- sa capacité à s'interconnecter au niveau réseau et à synchroniser la source de temps sur une horloge interne à l'entité ;
- la facturation de la bande passante sortante en prévision d'un éventuel export (cas fréquent dans les offres de *cloud* public).

À la lumière de cette évaluation et de la mise à jour de l'analyse de risque, l'entité peut maintenir un unique système de journalisation (nécessitant l'export des journaux générés par les systèmes externalisés chez le prestataire et leur importation vers le système de journalisation de l'entité) ou retenir l'option de systèmes de journalisation distincts.

R28

Étudier l'alternative d'un ou plusieurs systèmes de journalisation en cas d'externalisation

Si tout ou partie du SI de l'entité est externalisé, le choix de mettre en œuvre un ou plusieurs systèmes de journalisation doit être étudié suivant des critères fonctionnels et de sécurité.

Il est fréquent qu'une externalisation concerne uniquement un sous-système du SI de l'entité. Dès lors, ce sous-système peut impliquer des échanges de données avec le SI interne et requérir au préalable une interconnexion réseau et une fédération d'identité pour unifier l'authentification des utilisateurs. Afin de détecter toute tentative d'action malveillante sur ce point de passage critique, les journaux associés à l'interconnexion et à ses services (p. ex. concentrateurs VPN, serveurs de fédération d'identité) doivent être collectés, de préférence en interne.

15. *Software as a service*.
16. La limite de fourniture des journaux entre ceux propres au prestataire et ceux mis à disposition de l'entité diffère suivant le service souscrit. Par exemple, pour une application *SaaS*, l'entité pourra prétendre à récupérer les journaux générés par l'application mais probablement pas ceux des couches sous-jacentes.

R29

Récupérer les journaux relatifs aux interconnexions en cas d'externalisation

En cas d'externalisation d'un sous-sytème du SI de l'entité et de la mise en œuvre d'une interconnexion, il est recommandé de récupérer, de préférence sur le système de journalisation interne de l'entité, tous les journaux liés à cette interconnexion (p. ex. concentrateurs VPN, serveurs de fédération d'identité).

3.5.2 Externalisation du stockage des journaux et de la détection des incidents de sécurité

Si l'entité souhaite avoir des garanties supplémentaires sur l'intégrité du stockage de ses journaux ou externaliser le service de détection des incidents, elle peut faire appel à un prestataire de détection des incidents de sécurité (PDIS) [16] qualifié par l'ANSSI.

R30

Recourir à un PDIS en cas d'externalisation du stockage ou de la corrélation de journaux

En cas d'externalisation du stockage ou de la corrélation de journaux, il est recommandé d'avoir recours à un prestataire de détection des incidents de sécurité qualifié par l'ANSSI.

L'annexe C introduit le sujet de la détection des incidents de sécurité.

3.6 Cas particulier des postes nomades

Les journaux des postes de travail nomades doivent continuer à être collectés lorsque ces postes sont en situation de nomadisme, c'est-à-dire dès lors qu'ils sont connectés à leur SI de rattachement au travers d'un tunnel VPN.

R31

Collecter les journaux des postes en situation de nomadisme

Il est recommandé de maintenir la collecte des journaux des postes en situation de nomadisme grâce à un tunnel VPN.

Lorsque la recommandation R31 est appliquée mais que le poste de travail ne peut pas joindre un serveur de collecte pendant une certaine durée alors qu'il est connecté au SI (p. ex. panne de la chaîne de collecte des journaux), ce poste se trouve dans une situation qui comporte des risques. En effet, un attaquant qui accéderait à un tel système en situation de nomadisme pourrait effacer les journaux d'évènements avant qu'ils ne soient transmis aux serveurs de collecte. S'il existe, il est recommandé de configurer le système de détection d'incidents pour déclencher des alarmes en cas de détection de ces situations anormales.

Lorsque la centralisation à travers un tunnel VPN est impossible et qu'un système se trouve déconnecté pour une durée moyenne à longue, la centralisation de ses évènements perd son intérêt. Il est dans ce cas nécessaire d'envisager d'autres stratégies de sécurisation et de supervision.

Annexe A
Socle minimal de journalisation

Le tableau 1 donne la liste les catégories génériques d'évènements de sécurité qu'il convient de collecter et de centraliser pour ainsi constituer un *socle minimal de journalisation*. Cette liste n'est ni exhaustive ni universelle : elle doit être adaptée en fonction des besoins de sécurité du SI et des volumétries d'évènements générés par les usages qui en sont faits. La journalisation de certaines catégories d'évènements peut être à l'origine d'un volume très important de données. Parmi les catégories présentées dans le tableau 1, celles *a priori* susceptibles d'être verbeuses sont repérées par le label « attention : volumétrie potentiellement forte ! ».

Le *socle minimal de journalisation* doit être développé progressivement. Il est préférable de se concentrer sur l'obtention rapide d'un premier ensemble d'évènements correctement journalisés et exploitables, même s'il parait très insuffisant, puis venir le compléter ultérieurement par ajout de nouvelles sources de journaux, de nouvelles catégories d'évènements ou de nouveaux évènements unitaires. Il faut rentrer dans le cycle d'amélioration continue le plus vite possible mais la recherche d'exhaustivité, tant en terme de sources de journaux (voir recommandation R2) qu'en terme de catégories à journaliser (voir tableau 1), ne doit être vue que comme un objectif final.

La justification de cette approche progressive tient au fait que l'ajout de nouveaux évènements va nécessiter de la part des exploitants un ajustement fin des paramètres de journalisation (niveau de verbosité, fréquence d'émission, volumétries induites, etc). Dans certains cas, l'ajout de nouveaux évènements pourra avoir des effets inattendus (p. ex. une augmentation significative de la volumétrie conduisant à une pollution du système de journalisation et à la complexification inutile de son exploitation), raison pour laquelle il est recommandé de tester ces ajustements de configuration du système de journalisation sur un nombre réduit d'équipements avant d'en étendre le déploiement.

Domaine	Catégorie d'évènements
Authentification	- ouvertures de sessions - réussites et échecs des authentifications - utilisation de privilèges
Gestion des comptes	- création de comptes, de groupes ou de rôles - désactivations et verrouillages de comptes - octroi de privilèges aux comptes - ajouts de membres dans des groupes - assignation de rôles - modifications des secrets d'authentification (p. ex. mots de passe)
Stratégies de sécurité	- modification des paramétrages de sécurité des systèmes et des applications - modification des stratégies d'audit (types d'évènements journalisés, tailles des journaux…) et effacement de journaux)
Accès aux ressources sensibles	- accès ou tentatives d'accès en lecture/écriture/exécution/suppression aux ressources sensibles (attention : volumétrie potentiellement forte !)
Activité des processus	- démarrages/arrêts (attention : volumétrie potentiellement forte !) - dysfonctionnements - chargements/déchargements de modules (attention : volumétrie potentiellement forte !) - exécution de scripts (attention : volumétrie potentiellement forte !)
Activité des systèmes	- démarrages - dysfonctionnements/surcharges du système - chargements/déchargements de modules noyau - activité matérielle (défaillances, connexions/déconnexions physiques, etc.)

TABLE 1 – Catégories d'évènements devant être collectés pour constituer un socle *minimal de journalisation*

Annexe B
Illustrations des architectures possibles pour un système de journalisation

Les figures 1 et 2 présentées dans cette annexe ont pour objectif d'illustrer deux types d'architectures de journalisation centralisées. La figure 1 représente un SI de dimension réduite et la figure 2 un système multi-sites.

B.1 Architecture de journalisation simple

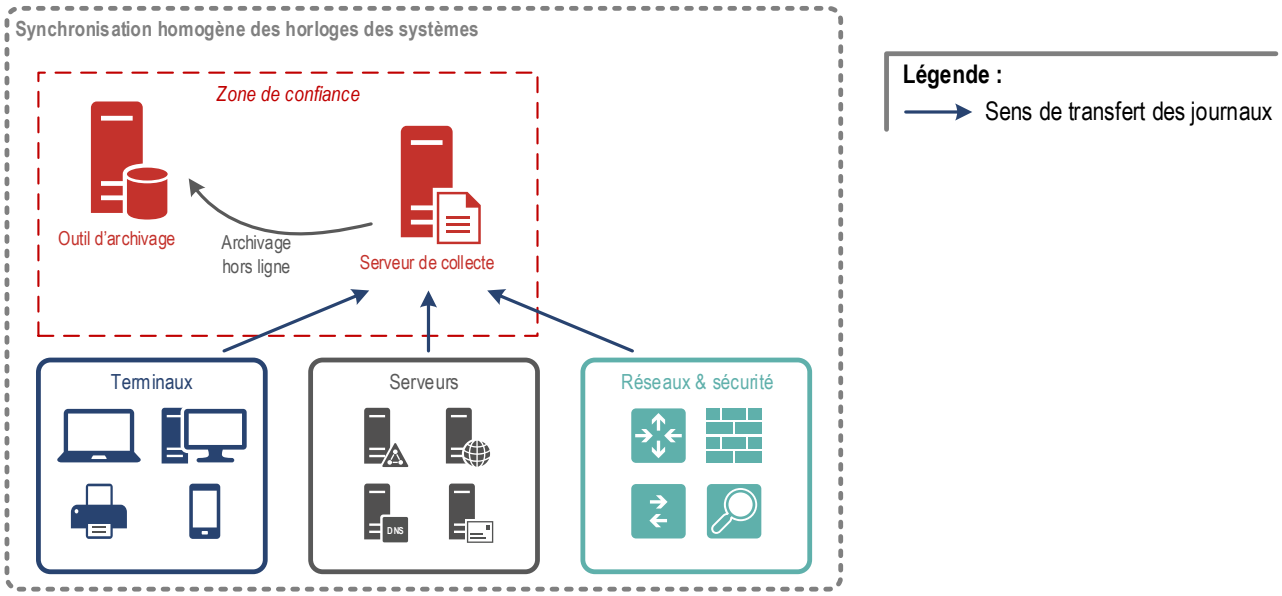

FIGURE 1 – Exemple d'architecture de journalisation simple

Cette architecture minimaliste ne comporte qu'un seul serveur de collecte, mais elle respecte les principes les plus importants : la collecte des journaux de l'ensemble des équipements, la centralisation des journaux, l'archivage hors ligne, et l'hébergement du système de journalisation dans une zone de confiance.

B.2 Architecture de journalisation multi-sites

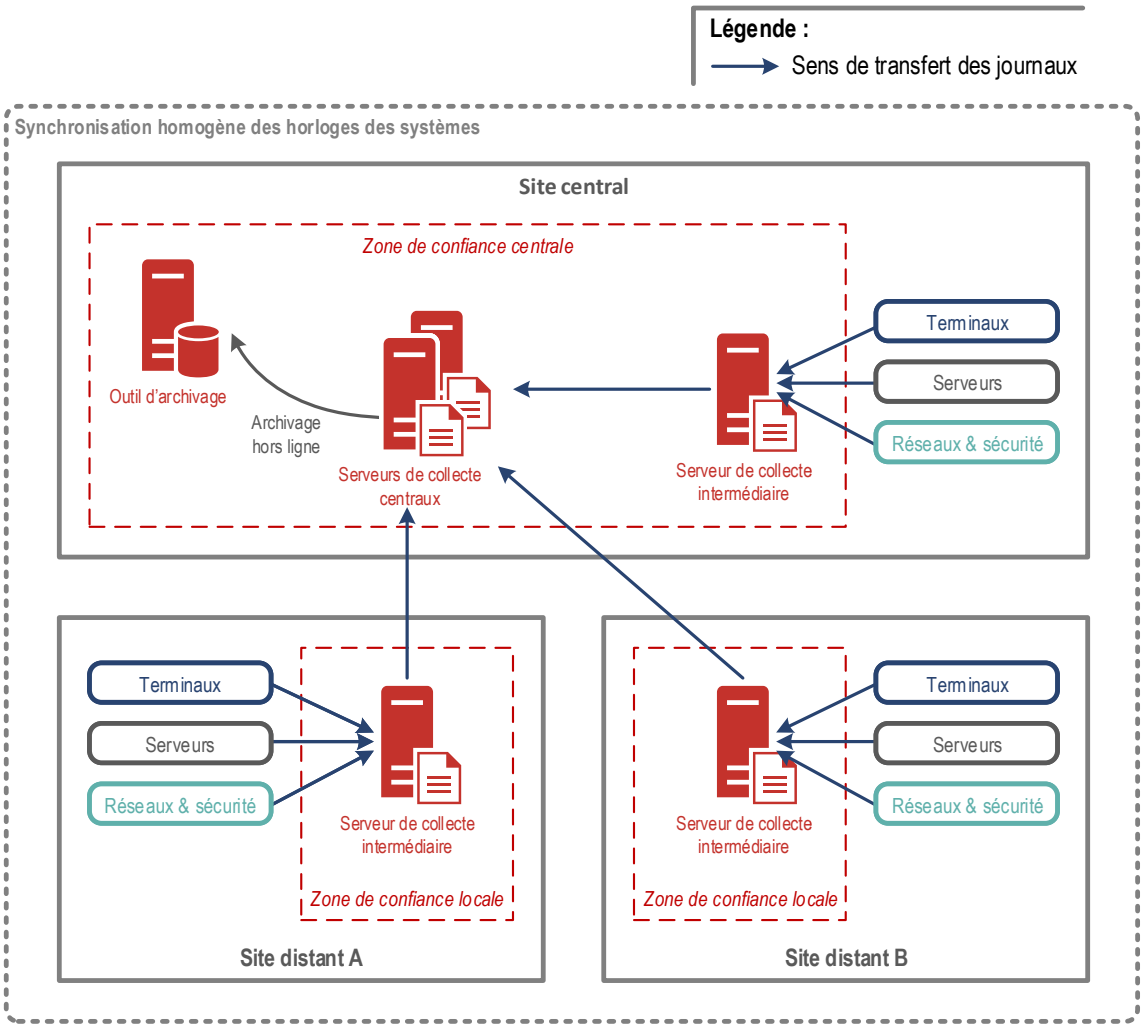

FIGURE 2 – Exemple d'architecture de journalisation multi-sites

Cet exemple plus complexe met en œuvre une architecture de collecte hiérarchique, avec des serveurs de collecte intermédiaires et centraux.

Ce type d'architecture est pertinent lorsque les journaux de plusieurs sites ou de plusieurs entités sont collectés sur un serveur central. Il permet de maîtriser les flux de communication entre les différents sites ou entités. Il est à noter qu'il n'existe aucune interaction directe entre les équipements qui génèrent les journaux et les serveurs de collecte centraux ; seuls des serveurs de collecte intermédiaires peuvent communiquer avec les serveurs centraux.

De plus, dans cet exemple, la résilience du système de journalisation est augmentée par la redondance des serveurs centraux (mais complexifie les opérations de maintien en condition opérationnelle et de maintien en condition de sécurité).

Annexe C
Introduction à la détection des incidents de sécurité

La mise en place d'un système de détection des incidents de sécurité et l'ajustement des processus organisationnels qui y sont associés est un exercice complexe. Cette mission doit être confiée à du personnel spécifiquement formé. Si cette activité est externalisée, il est recommandé de recourir aux services d'un prestataire qualifié (voir recommandation R30).

La journalisation des évènements est un prérequis nécessaire mais non suffisant pour détecter des incidents de sécurité. Le périmètre de ce guide est restreint au système de journalisation. Cette annexe a toutefois pour objectif de donner quelques grands principes pour mettre en œuvre un système efficace de détection et d'analyse des incidents de sécurité.

La figure 3 donne une représentation des liens fonctionnels qui existent entre le système de journalisation et le système de détection des incidents.

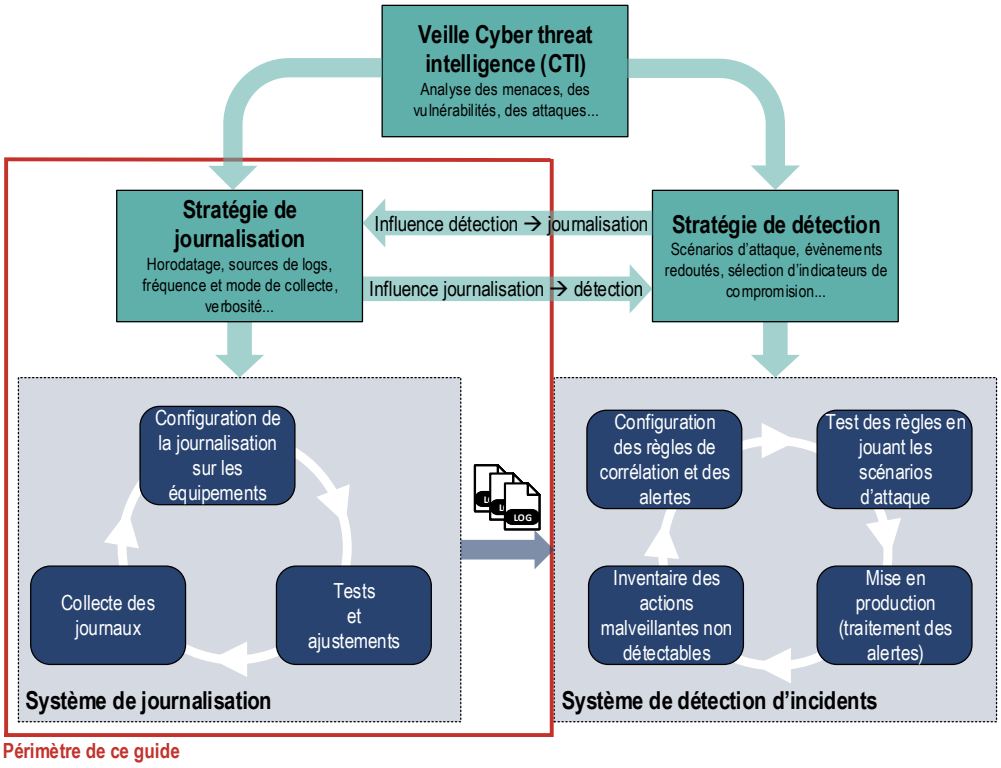

FIGURE 3 – Illustration de l'interdépendance entre le système de journalisation et le système de détection des incidents

Pour se doter d'une capacité de détection des incidents de sécurité, il est proposé une démarche en quatre étapes :

- Étape 1 : mettre en œuvre un système de journalisation
- Étape 2 : déployer un système de détection des incidents de sécurité
- Étape 3 : améliorer en continu le système de détection des incidents et le système de journalisation
  - Étape 3.1 : faire évoluer la politique de journalisation en fonction des scénarios d'attaque
  - Étape 3.2 : faire évoluer les capacités de détection en fonction de la connaissance du SI et de ses méthodes d'administration
- Étape 4 : orienter les politiques de journalisation et de détection en améliorant la connaissance des menaces

C.1 Étape 1 : mettre en œuvre un système de journalisation

C'est l'objet de ce guide de présenter les principes généraux régissant la mise en œuvre d'un système de journalisation, à savoir : identifier les prérequis techniques (synchronisation horaire, dimensionnement des espaces de stockage, etc.), comprendre l'architecture générale d'un système de journalisation (serveurs intermédiaires et serveurs centraux, sécurisation des flux, etc.), configurer les systèmes générateurs de journaux (verbosité, mode de transfert, etc.).

Une fois que les composants techniques du système de journalisation sont en place, il convient de sélectionner les thématiques des journaux qu'il permettra de collecter. Des conseils relatifs à la constitution d'un *socle minimal de journalisation* du SI sont donnés dans l'annexe A.

C.2 Étape 2 : déployer un système de détection des incidents de sécurité

Lorsque le système de journalisation est opérationnel, l'étape suivante consiste à déployer les outils d'exploitation des journaux et de gestion des incidents de sécurité.

Les journaux stockés de façon centralisée doivent être facilement exploitables à l'aide d'un outil adapté. Dans certains cas d'usage, il est nécessaire de trouver rapidement les informations recherchées dans les journaux. L'outil utilisé doit donc être réactif et facile à utiliser. Des contraintes techniques peuvent également intervenir dans le choix de l'outil (type de stockage, format des journaux, etc.). La richesse fonctionnelle offerte par les outils de journalisation peut être variée, allant d'un simple logiciel permettant de trouver rapidement les informations recherchées dans les journaux à des outils plus élaborés permettant de corréler les évènements et de déclencher des alertes (SIEM [17]).

17. *Security information event management.*

Conformément à la recommandation R2, la journalisation d'un SI doit être aussi exhaustive que possible. Toutefois, au sein d'un système de type SIEM, il convient d'intégrer les seuls journaux utiles à la détection des incidents et d'écarter les journaux spécifiquement collectés à des fins de conformité afin de maintenir un outil de recherche performant. En effet, la capacité et la rapidité de recherche dans les journaux sont cruciales pour pouvoir repérer les comportements suspects à l'échelle d'un SI.

Une entité souhaitant dépasser le stade de la journalisation simple pour aller vers la détection des incidents de sécurité et la réponse aux incidents mettra le plus souvent en œuvre plusieurs outils pour exploiter les journaux et se doter d'une capacité à gérer les incidents de sécurité.

Information

Les accès aux outils d'exploitation des journaux doivent être journalisés au même titre que pour n'importe quel autre service.

En fonction du contexte, plusieurs types de populations peuvent accéder aux outils mis à disposition sur les serveurs centraux pour exploiter les journaux. Ces groupes d'utilisateurs n'ont pas nécessairement besoin de disposer d'un accès en lecture à l'ensemble des journaux du SI (lesquels peuvent avoir des niveaux de sensibilité différents), c'est la raison pour laquelle il est recommandé de pratiquer un cloisonnement en définissant des rôles précis pour l'accès aux outils. De même, les différents métiers du SOC [18] doivent accéder aux seules fonctionnalités du SIEM nécessaires pour mener à bien les tâches qui leur sont confiés.

Ces rôles peuvent être calqués sur des entités métier qui ont besoin de consulter les journaux relatifs à leur activité (administrateurs système, administrateurs de bases de données, administrateurs de sécurité, etc.). L'usage d'un annuaire préexistant est recommandé pour authentifier les utilisateurs de ces outils ; les groupes d'utilisateurs qu'il contient pourront alors être utilisés comme référence pour définir les rôles et les accès aux outils.

C.3 Étape 3 : améliorer en continu le système de détection des incidents et le système de journalisation

C.3.1 Étape 3.1 : faire évoluer la politique de journalisation en fonction des scénarios d'attaque

Après avoir mis en place un système de journalisation et s'être doté des outils permettant d'exploiter et corréler les évènements, il est nécessaire de configurer les règles du SIEM de manière à détecter au mieux les différents scénarios d'attaque. Une entité peu mature se contentera de mettre en place une sélection standard d'évènements centralisés (le *socle minimal de journalisation* décrit à l'annexe A), sans chercher à savoir à quels scénarios de compromission elle répond. Au contraire, une entité souhaitant développer ses capacités de détection cherchera à faire évoluer sa politique de journalisation en fonction des scénarios d'attaques qu'elle redoute.

18. *Security operation center.*

L'exemple présenté ci-après va permettre d'illustrer cette notion de *scénario d'attaque* et de comprendre les conséquences concrètes d'un tel scénario sur la configuration du système de journalisation, dans le cas d'un SI sous Windows (section C.3.1.1) et dans le cas d'un SI sous Linux (section C.3.1.2).

Exemple de scénario d'attaque

Dans ce scénario, un utilisateur est victime d'une attaque par hameçonnage (*phishing*) et l'attaquant va utiliser ce point d'entrée sur le SI pour chercher à élever ses privilèges et rendre son attaque persistante. Un déroulement possible de cette attaque peut être le suivant :

- l'utilisateur est incité à cliquer sur la pièce jointe d'un courrier électronique contenant un code malveillant (*phishing*) ;
- l'utilisateur étant déjà administrateur local de sa machine, cette dernière est intégralement compromise par l'attaquant qui peut récupérer les authentifiants en mémoire d'autres comptes d'utilisateurs et de services ;
- l'attaquant réutilise un de ces comptes pour se connecter interactivement à distance à d'autres postes de travail et serveurs ;
- pour assurer la persistance de son attaque, l'attaquant ajoute un compte administrateur local à ces machines.

Ce scénario d'attaque est basique, mais fait intervenir plusieurs étapes d'une attaque classique (compromission initiale, élévation de privilèges, mouvement latéral, persistance), et il convient de s'assurer que chaque étape est correctement détectée avant de continuer le cycle d'amélioration avec des scénarios plus avancés. Pour cela, en jouant ce scénario dans un environnement contrôlé, les administrateurs identifient plusieurs évènements qui doivent être qualifiés puis ajoutés à la politique de journalisation (pour qu'ils soient générés) et à la liste des évènements centralisés (pour qu'ils soient transférés vers le SIEM).

Les sous-sections C.3.1.1 et C.3.1.2 illustrent respectivement comment cet exemple de scénario d'attaque peut influer sur la stratégie de journalisation des systèmes Windows ou des systèmes Linux.

C.3.1.1 Exemple d'évolution de la stratégie de journalisation sous Windows

Dans le cas où l'exemple de scénario de compromission présenté précédemment concerne des systèmes d'exploitation Windows, la configuration de la journalisation peut être modifiée de la manière suivante [19] :

1. L'exécution d'un programme génère un évènement 4688 [20] *Un processus a été créé* dans le canal *Sécurité* par le fournisseur *Microsoft-Windows-Security-Auditing*, avec un programme inhabituel comme descendant d'une application de bureautique [21]. Les administrateurs identifient également que les arguments des programmes ne sont pas journalisés par défaut, et qu'il faut

19. Pour plus d'information concernant le mise en pratique de la journalisation sur des systèmes Microsoft Windows en environnement Active Directory, se reporter au guide [13].
21. https ://docs.microsoft.com/fr-fr/windows/security/threat-protection/auditing/event-4688

activer la politique de sécurité *Configuration Ordinateur* > *Modèles d'administration* > *Système* > *Audit de création de processus* > *Inclure une ligne de commande dans les évènements de création de processus* [22] ;

2. L'exécution d'un outil malveillant pour récupérer les authentifiants d'autres utilisateurs en mémoire peut générer des alertes dans un journal antivirus, si celui-ci a été activé. Par exemple, par défaut, les évènements 1006 à 1009 et 1116 à 1119 du canal *Microsoft-Windows-Windows DefenderOperational* par le fournisseur *Microsoft-Windows-Windows Defender* [23] ;

3. L'ouverture de session interactive à distance génère un évènement 4624 *Un compte a été connecté avec succès* dans le canal *Sécurité*, par le fournisseur *Microsoft-Windows-Security-Auditing*, et une *IpAddress* source inhabituelle ne correspondant pas aux plages IP d'administrateurs. Pour que cet évènement soit généré, il faut activer la sous-catégorie *Ouvrir / Fermer la session* > *Auditer l'ouverture de session* pour les *Succès* [24] ;

4. L'ajout d'un compte administrateur génère un évènement 4735 [25] *Un groupe local dont la sécurité est activée a été modifié* dans le canal *Sécurité* par le fournisseur *Microsoft-Windows-/Security-Auditing* [26] avec pour *TargetUserName* le groupe administratif, et pour *SubjectUserName* un utilisateur illégitime.

C.3.1.2 Exemple d'évolution de la stratégie de journalisation sous Linux

Dans le cas où le l'exemple de scénario de compromission présenté précédemment concerne des systèmes d'exploitation GNU/Linux, la configuration de la journalisation du service *auditd* [5] peut être modifiée de la manière suivante :

1. L'exécution d'un programme par un utilisateur génère un évènement au moyen de règles *auditd* telles que [27] :

   ```
   auditctl -a always,exit -F arch=b64 -S execve,execveat -F 'auid'>=1000 -F 'auid !='unset -k user_exec
   auditctl -a always,exit -F arch=b32 -S execve,execveat -F 'auid'>=1000 -F 'auid !='unset -k user_exec
   ```

2. La récupération d'authentifiants en mémoire d'autres processus, si elle est faite au moyen des API de débogage, va générer des évènements au moyen de règles *auditd* telles que :

   ```
   auditctl -a always,exit -F arch=b64 -S process_vm_readv,process_vm_writev,ptrace -k debugging
   auditctl -a always,exit -F arch=b32 -S process_vm_readv,process_vm_writev,ptrace -k debugging
   ```

   Si elle est faite au moyen d'un module noyau, elle va générer des évènements au moyen de règles *auditd* telles que :

   ```
   auditctl -a always,exit -F arch=b64 -S init_module,finit_module -k kernel_driver
   auditctl -a always,exit -F arch=b32 -S init_module,finit_module -k kernel_driver
   ```

22. https ://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
23. https ://docs.microsoft.com/fr-fr/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus
24. https ://docs.microsoft.com/fr-fr/windows/security/threat-protection/auditing/event-4624
26. https ://docs.microsoft.com/fr-fr/windows/security/threat-protection/auditing/event-4735
25. Pour que cet évènement soit généré, la sous-catégorie « Suivi détaillé > Auditer la création du processus » doit être activée pour les « Succès ».
26. Attention : pour que cet évènement soit généré, il est nécessaire d'activer la sous-catégorie *Gestion du compte* > *Auditer la gestion des groupes de sécurité* pour les *Succès*.
27. https ://man7.org/linux/man-pages/man7/audit.rules.7.html

3. L'ouverture de session va générer des évènements dans divers journaux comme */var/log/auth.log*, */var/log/secure*, le journal *sshd*, etc. selon la distribution Linux utilisée et les éventuels paquets installés pour permettre son administration à distance ;

4. La modification d'un groupe sous Unix génère un évènement au moyen de règles *auditd* telles que :

   ```
   auditctl -w /etc/passwd -p wa -k user_change
   auditctl -w /etc/group -p wa -k group_change
   ```

C.3.1.3 Déclenchement d'alertes au niveau du SOC

Sachant que tous les évènements liés au scénario d'attaque sont désormais journalisés, un analyste du SOC configure une règle de corrélation associée à ce scénario : une alarme sera automatiquement générée lorsque certains évènements ou enchaînements d'évènements redoutés seront détectés sur le SI.

L'exemple présenté précédemment illustre la manière dont la configuration du système de journalisation est influencée par les scénarios d'attaque envisagés. Cette influence du système de détection sur le système de journalisation est représenté par la flèche « Influence détection -> journalisation » sur la figure 3.

C.3.1.4 Aller plus loin avec les scénarios d'attaque

Une source d'information intéressante pour élaborer des scénarios d'attaque est la matrice MITRE ATT&CK [28]. Elle permet d'inventorier les techniques d'attaques, potentiellement au moyen de signatures [29] complexes. Parmi ces signatures, certaines sont disponibles en source ouverte sous le format SIGMA [30].

Pour chaque scénario d'attaque à couvrir, il est recommandé de simuler au préalable l'attaque dans un environnement cloisonné et d'identifier les conséquences sur les journaux produits. À ce titre, le projet *DetectionLab* [31] permet de générer facilement un environnement de détection complet, tandis que le projet *Atomic Red Team* [32] permet la simulation de telles attaques. Une fois les effets de l'attaque visibles dans les journaux, les évènements correspondants doivent être collectés et les alertes idoines doivent être configurées.

C.3.2 Étape 3.2 : faire évoluer les capacités de détection en fonction de la connaissance du SI et de ses méthodes d'administration

Une autre bonne pratique consiste à mettre en place une stratégie de détection des incidents suivant un postulat de compromission (*assume breach*) : l'origine d'une compromission peut être aussi bien interne qu'externe au SI. Cela peut être réalisé en recherchant des signaux faibles d'attaques au cœur du SI (traces de latéralisation, de persistance, d'élévation de privilèges, etc). Pour rendre

28. Se reporter au site du projet pour plus d'informations : https ://attack.mitre.org.
29. Dans le contexte de ce guide, les termes *signature*, *marqueur* et *indicateurs de compromission* sont utilisés de manière interchangeables pour désigner des indices techniques susceptibles d'être révélateurs de la compromission d'un SI.
30. Se reporter au site du projet pour plus d'informations : https ://github.com/SigmaHQ/sigma.
31. Se reporter au site du projet pour plus d'informations : https ://github.com/clong/DetectionLab.
32. Se reporter au site du projet pour plus d'informations : https ://github.com/redcanaryco/atomic-red-team.

possible la détection de ces signaux faibles, le système de journalisation doit être configuré pour générer les évènements qui matérialiseront une ligne de base (*baseline*) censée représenter le comportement « normal » du SI, tandis que le système de détection doit être configuré de manière à lever des alertes lorsque des écarts de comportements sont détectés par rapport à cette ligne de base.

Tous ces écarts doivent donner lieu à des levées de doute, en particulier s'ils concernent des activités d'administration. En conséquence, plus les pratiques d'administration seront homogènes au sein du SI, plus la probabilité de détection des agissements des attaquants augmentera. Pour une détection des incidents pertinente, il est important qu'un travail d'urbanisation du SI et de rationalisation des pratiques d'administration ait été mené préalablement à la mise en œuvre d'un système de détection des incidents. Les analystes du SIEM doivent avoir la connaissance de ces pratiques d'administration et doivent adapter en permanence les règles de détection du SIEM au fur et à mesure de l'évolution de ces pratiques.

Exemples d'actions suspectes traduisant des écarts à la ligne de base

Un défaut de nommage d'une machine vis-à-vis des règles de nomenclature de l'entité, une tentative de connexion à Internet en contournement du serveur mandataire (ou *proxy*), l'administration d'une ressource via VNC [33] à la place de RDP [34] ou *PowerShell* peuvent trahir les activités d'un attaquant.

Comme nous venons de le voir, la capacité de détection des incidents est aussi influencée par la connaissance du SI et des méthodes d'administration. Or, la capacité à identifier une activité *normale* du SI est directement dépendante de la configuration du système de journalisation. Cette influence du système de journalisation sur le système de détection est représenté par la flèche « Influence journalisation -> détection » sur la figure 3.

C.4 Étape 4 : orienter les politiques de journalisation et de détection en améliorant la connaissance des menaces

Un entité soucieuse d'améliorer ses capacités de détection et de réaction aux incidents de sécurité doit chercher à faire évoluer la configuration de ses systèmes de journalisation et de détection en fonction de la connaissance des cyber menaces pesant sur le SI qu'elle cherche à protéger.

L'amélioration de la connaissance de la menace d'origine cyber passe par la capitalisation et l'analyse d'informations d'origines diverses. Ces informations sont désignées en anglais par le sigle CTI pour *Cyber threat intelligence*. L'influence que peut avoir la CTI sur les capacités de journalisation et de détection des incidents est symbolisée sur la figure 3 par la case « CTI » et les flèches pointant vers le système de journalisation et vers le système de détection.

Il est possible de distinguer trois types d'informations CTI :

33. *Virtual network computing.*
34. *Remote desktop protocol.*

- les informations **techniques** qui sont relatives aux indicateurs de compromission. Ces indicateurs peuvent être intégrés aux scénarios d'attaque mis en œuvre dans le système de détection ou faire l'objet de recherches d'antécédents dans les journaux collectés ;
- les informations **tactiques** qui visent à comprendre les capacités et les modes opératoires des attaquants (vecteur initial de compromission, familles de codes malveillants utilisés, techniques de persistance…) ;
- les informations **stratégiques** qui ont pour vocation de clarifier les motivations des attaquants et l'origine des attaques.

Le traitement de ces informations par les analystes SOC ou les analystes CSIRT [35] peut être industrialisé. À titre d'illustration, les informations de type indicateur et les données de contexte voire d'attribution d'une attaque peuvent être échangées de manière organisée grâce à certains standards (p. ex. le format STIX [36]).

Ces informations CTI peuvent être accessibles en source ouverte ou sur abonnement et être publiées par une autorité gouvernementale (p. ex. CERT-FR [37] en France) ou par un fournisseur privé.

Une bonne connaissance de la menace susceptible de cibler les systèmes supervisés permet d'améliorer les capacités de détection puis, en cas d'incident ou de suspicion d'incident, de guider les actions de réponse pour les rendre aussi pertinentes que possible.

35. *Computer security incident response team*.
36. Se reporter à ce site pour plus d'informations sur le format STIX (*Structured Threat Information eXpression*) : https ://oasis-open.github.io/cti-documentation/stix/intro.html.
37. Se reporter au site du CERT-FR pour plus d'informations : https ://www.cert.ssi.gouv.fr/.

Annexe D
Aspects juridiques et réglementaires

Les éléments juridiques et réglementaires sont structurants pour un système de journalisation. Ils doivent donc être pris en compte au plus tôt, lors de sa conception.

D.1 Intérêt de la journalisation

Un des principaux intérêts d'un système de journalisation est la capacité à détecter et analyser d'éventuels incidents, et, le cas échéant, d'identifier directement ou indirectement un profil ou un équipement concerné par celui-ci.

La mise en œuvre d'un système de journalisation est, d'ailleurs, au nombre des mesures de sécurité prévues par des réglementations, qu'il s'agisse de la protection des données à caractère personnel [38] ou de la protection des systèmes eux-mêmes.

Plus particulièrement, les arrêtés sectoriels pris en application des articles R. 1332-41-1 et L. 1332-6-1 du code de la défense imposent aux opérateurs d'importance vitale de mettre en œuvre « *un système de journalisation qui enregistre les évènements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité du SIIV ainsi qu'au fonctionnement du SIIV* » et précisent que « *Les évènements enregistrés par le système de journalisation sont horodatés au moyen de sources de temps synchronisées. Ils sont, pour chaque SIIV, centralisés et archivés pendant une durée d'au moins six mois* ». Le système de journalisation est accompagné d'un système de corrélation et d'analyse des journaux permettant la détection d'évènements susceptibles d'affecter la sécurité des systèmes d'information. Des règles identiques sont prévues à la charge des opérateurs de services essentiels et des fournisseurs de services numériques en vertu de l'arrêté du 14 septembre 2018 [39].

D'autres textes, dont la portée est fonction de leur champ d'application, contiennent également des règles relatives à la journalisation. Peuvent notamment être citées l'instruction générale interministérielle sur la protection du secret de la défense nationale [2], l'instruction interministérielle relative à la protection des systèmes d'information sensibles [15]. ou encore la Politique de sécurité des systèmes d'information de l'Etat (PSSIE). De manière générale, il est recommandé d'effectuer un état des lieux de la réglementation sectorielle applicable.

38. Art. 101 de la loi du 6 janvier 1978 modifiée. Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), tout comme la loi du 6 janvier 1978 modifiée, prévoient une obligation générale de sécurité des traitements de données à caractère personnel impliquant la mise en place de mesures techniques et organisationnelles appropriées.

39. Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

Afin d'être opposable en cas de contentieux, la mise en œuvre d'un système de journalisation doit respecter les règles relatives à l'administration de la preuve et les principes directeurs des procès civils et pénaux (loyauté, intégrité, licéité, etc.)

Attention

L'horodatage des journaux ainsi que l'utilisation de mécanismes permettant d'assurer leur intégrité (p. ex. l'utilisation de protocoles sécurisés lors de leurs transferts) permettent d'accroître leur valeur probatoire. Informer de l'existence du système de journalisation et recueillir le consentement des utilisateurs au travers de la charte informatique de l'entité permet d'en assurer l'opposabilité.

D.2 Application de la réglementation relative à la protection des données à caractère personnel

Les éléments de journalisation peuvent contenir des données à caractère personnel telles que définies par le Règlement général sur la protection des données (RGPD) et dans la loi du 6 janvier 1978 modifiée (loi informatique et liberté). À la différence des données exclusivement techniques (nom de machine, identifiant de processus, etc.), une adresse de courriel, une URL ou une adresse IP sont régulièrement considérées par la CNIL comme des données à caractère personnel.

Le besoin d'une journalisation découle principalement des obligations de sécurisation du traitement présent dans les dispositions du RGPD et de la loi informatique et liberté. Dans la mesure où le traitement des éléments de journalisation contient des données à caractère personnel, il doit respecter les dispositions de ces textes, dont :

- la mise en œuvre d'un niveau de sécurité adapté aux données traitées et aux finalités ;
- la gestion du cycle de vie des éléments de journalisation (processus de création, de conservation, de destruction, etc.) ;
- la garantie des droits de la personne (information, consentement préalable, droit d'accès, etc.)

La jurisprudence a posé plusieurs principes applicables à la gestion des éléments de journalisation par des personnes habilitées [40]. La CNIL a également formulé des recommandations afin de minimiser le risque de détournement des données collectées dans ce cadre, par exemple :

- seules des personnes spécifiquement habilitées peuvent accéder aux éléments de journalisation ;
- l'accès doit être strictement limité à la finalité poursuivie, de la manière la moins intrusive possible pour les données à caractère personnel ;
- le personnel habilité est soumis à des obligations de confidentialité particulières et ne doit divulguer une quelconque donnée à caractère personnel que dans des cas limités liés au fonctionnement technique ou à la sécurité des systèmes ou aux intérêts de l'entreprise ;
- la minimisation des données.

40. Le terme « habilité » est utilisé ici au sens juridique, c'est-à-dire « apte à accomplir un acte ».

Les éléments de journalisation ne peuvent être conservés que pour un temps limité. La CNIL recommande une durée comprise entre six mois et une année mais admet une durée plus longue justifiée dans certains cas précis (obligation légale, sensibilité particulière du traitement, poursuite d'une finalité spécifique, etc.). Dans tous les cas, la réglementation en matière de protection des données à caractère personnel impose aux responsables de traitement de fixer une durée de conservation proportionnée à la finalité poursuivie.

Attention

Les activités liées à la gestion des éléments de journalisation doivent être strictement limitées aux finalités identifiées par le responsable de traitement. Les procédures liées à la gestion des éléments de journalisation doivent être décrites dans des documents de référence, permettant ainsi de s'assurer que les données à caractère personnel ne sont pas conservées ou utilisées de manière illégitime.

D.3 Régimes particuliers relatifs à la conservation des éléments de journalisation

La réglementation encadre plusieurs hypothèses dans lesquelles certains opérateurs, en fonction de leur nature ou de leurs activités, sont astreints à une obligation de production et de conservation des éléments de journalisation, notamment aux fins de répondre aux demandes de services habilités (autorité judiciaire, ANSSI, etc.). Le cas échéant, ces régimes sont cumulatifs.

D.3.1 Conservation des éléments de journalisation par les fournisseurs d'accès à Internet (FAI) ou d'hébergement

Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication au public en ligne (c.-à-d. les FAI) ainsi que celles qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services (c.-à-d. les hébergeurs) détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires [41].

Sont en particulier concernés les fournisseurs d'accès et hébergeurs professionnels, les entreprises et administrations qui donnent accès à Internet à leurs personnels dans le cadre de leur activité professionnelle, les entreprises et administrations offrant un service en ligne qui stocke des données fournies par leurs usagers, les fournisseurs de point d'accès au public (hôtels, restaurants, etc.), les cybercafés, les fournisseurs de services en ligne (blogs, réseaux sociaux, etc.).

41. Décret nº 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Attention

Les fournisseurs d'accès à Internet et les hébergeurs sont tenus de conserver certaines données de leurs journaux pendant une durée fixée par les textes [42].

La non-conservation de ces données par les fournisseurs d'accès à Internet et les hébergeurs est sanctionnée pénalement par une peine d'emprisonnement d'un an et de 250 000 euros d'amende pour les personnes physiques et d'une amende de 1 250 000 euros pour les personnes morales [43].

D.3.2 Conservation des éléments de journalisation des opérateurs de communications électroniques

Les opérateurs de communications électroniques, c'est-à-dire les personnes qui au titre d'une activité professionnelle principale ou accessoire offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, ont l'obligation de conserver certaines données de leurs abonnés [44] mais uniquement lorsqu'ils les collectent dans le cadre de la fourniture du service. Ces opérateurs peuvent être similaires à ceux visés à la section D.3.1 (cybercafés, fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne Wi-Fi que ce soit à titre payant ou non) mais les éléments de journalisation faisant l'objet d'une conservation diffèrent.

Les catégories de données concernées sont les données utiles :

- dans le cadre de la facturation et du paiement des prestations de communications électroniques ;
- pour différentes finalités définies à l'article L. 34-1 du code des postes et des communications électroniques (notamment besoins des procédures pénales, prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale, besoins de la lutte contre la criminalité et la délinquance graves) ;
- dans le cadre de la protection des systèmes d'information de l'opérateur de communications électroniques.

Les types de données concernés par ces catégories sont précisés par les articles R. 10-12 et suivants du code des postes et des communications électroniques.

Attention

La durée minimale de conservation diffère selon le type de donnée concerné, allant de trois mois à un an, voire cinq ans à compter de la fin de validité de son contrat, pour les informations relatives à l'identité civile de l'utilisateur.

La non-conservation, le non-respect de la durée minimale de conservation et de l'anonymisation des données sont sanctionnés pénalement par une peine d'emprisonnement d'un an et de 75 000 euros d'amende [45].

42. Art. L. 34-1 du code des postes et des communications électroniques.
43. LCEN, art. 6 VI, al. 1).
44. Art. L. 34-1 du code des postes et des communications électroniques.
45. Art. L. 39-3 du code des postes et télécommunications électroniques.

Annexe E
Évolutions du guide

E.1 Nouvelles recommandations

Les recommandations suivantes font leur apparition dans la version 2.0 du guide :

R2, R4, R6, R7, R12, R14-, R15, R23+, R26+, R27, R28, R29, R30, R31

E.2 Mises à jour entre les versions 1.0 et 2.0

Outre les mises à jour de forme, le guide a fait l'objet de mises à jour de fond entre les versions 1.0 et 2.0 dont les principales sont énumérées ci-après :

- ajout de la section 3.5 relative à l'externalisation de tout ou partie du SI et aux conséquences de cette externalisation pour le système de journalisation ;
- ajout de la section 3.6 qui donne une recommandation concernant la journalisation des postes en situation de nomadisme ;
- refonte de l'annexe A relative au catégories d'évènements qu'il convient de journaliser pour constituer un *socle minimal de journalisation* ;
- création d'une nouvelle annexe C qui introduit le sujet de la détection des incidents de sécurité ;
- mise à jour de l'annexe C « Aspects juridiques et réglementaires » dans la version 1.0 du guide qui devint l'annexe D dans cette version 2.0.

E.3 Matrice de rétrocompatibilité depuis la version 1.0 vers les versions ultérieures

Afin de permettre aux lecteurs ayant déjà travaillé sur la base de la première version du guide [6], dénommée v1.0 dans la suite du texte, il est proposé une matrice de rétrocompatibilité permettant de trouver les ajouts, suppressions ou équivalences de recommandations.

Attention

Cette matrice est un outil pour faciliter la lecture mais n'a pas vocation à établir une équivalence stricte entre les différentes versions du guide. La lecture détaillée des recommandations actualisées est fortement conseillée.

Référence v1.0	**Référence actuelle**	**Référence v1.0**	**Référence actuelle**
R1	R1	Inexistante	R19
Inexistante	R2 Activer la journalisation sur un nombre important d'équipements du SI	R14	R20
R2	R3	R15	R20-
Inexistante	R4 Homogénéiser les paramètres d'horodatage	R16	R21
R3	R5	R17	R23
Inexistante	R6 Identifier la granularité de journalisation des équipements	Inexistante	R23+ Privilégier le stockage des journaux dans une base de données indexée
Inexistante	R7 Journaliser les empreintes des fichiers potentiellement malveillants	R18	R24
R4	R8	R19	R25
R5	R9-	R20	R26
R6	R9	Inexistante	R26+ Restreindre au strict besoin opérationnel les droits de suppression des journaux
R7	R10	Inexistante	R27 Restreindre au strict besoin opérationnel les droits d'accès en lecture aux journaux
R8	R11	R21	Supprimée
Inexistante	R12 Contrôler régulièrement la couverture de la chaîne de collecte des évènements	R22	Supprimée
R9	R14	R23	Supprimée
Inexistante	R14- Adopter un transfert des journaux en temps différé	R24	R22
Inexistante	R15 Faire une analyse de risque pour déterminer le mode de transfert des journaux	Inexistante	R28 Étudier l'alternative d'un ou plusieurs systèmes de journalisation en cas d'externalisation
R10	R13	Inexistante	R29 Récupérer les journaux relatifs aux interconnexions en cas d'externalisation
R11	R16	Inexistante	R30 Recourir à un PDIS en cas d'externalisation du stockage ou de la corrélation
R12	R17	Inexistante	R31 Collecter les journaux des postes en situation de nomadisme
R13	R18		

Liste des recommandations

Bibliographie

[1] *Norme internationale IS0 8601-1 :2019*.
Référentiel, ISO, 2019.
https://www.iso.org/standard/70907.html.

[2] *Instruction générale interministérielle n°1300*.
Référentiel, SGDSN, août 2021.
https://www.ssi.gouv.fr/igi1300.

[3] *Recommandation relative à la journalisation*.
Technical Report Délibération n° 2021-122, CNIL, novembre 2021.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044272396.

[4] *Recommandations pour un usage sécurisé d'(Open)SSH*.
Note technique DAT-NT-007/ANSSI/SDE/NP v1.2, ANSSI, août 2015.
https://www.ssi.gouv.fr/nt-ssh.

[5] *Recommandations de configuration d'un système GNU/Linux*.
Guide ANSSI-BP-028 v1.2, ANSSI, février 2019.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[6] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[7] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[8] *Maîtrise du risque numérique - l'atout confiance*.
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance.

[9] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://www.ssi.gouv.fr/nt-tls.

[10] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.
https://www.ssi.gouv.fr/passerelle-interconnexion.

[11] *Guide de sélection d'algorithmes cryptographiques*.
Guide ANSSI-PA-079 v1.0, ANSSI, mars 2021.
https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques.

[12] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://www.ssi.gouv.fr/securisation-admin-si.

[13] *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory*.
Guide ANSSI-PB-090 v1.0, ANSSI, janvier 2022.
https://www.ssi.gouv.fr/journalisation-windows.

[14] *Expression des besoins et identification des objectifs de sécurité*.
Guide Version 1.1, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/ebios.

[15] *Instruction interministérielle n°901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://www.ssi.gouv.fr/ii901.

[16] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences*.
Référentiel Version 2.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf.

[17] *Les serveurs de temps NTP français*.
Page web, GIP RENATER.
https://services.renater.fr/ntp/serveurs_francais.

[18] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

Version 2.0 - 28/01/2022 - ANSSI-PA-012/ANSSI/SDE
Licence ouverte / Open Licence (Étalab - v2.0)
ISBN : 978-2-11-167114-0 (papier)
ISBN : 978-2-11-167115-7 (numérique)
Dépôt légal : janvier 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN