Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat

Canada

Guide sur la consignation d'événements

Publié : le 2020-08-07

© Sa Majesté la Reine du chef du Canada,
représentée par le président du Conseil du Trésor 2020,

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT39-52/2020F-PDF
ISBN : 978-0-660-36827-6

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Event Logging Guidance

Guide sur la consignation d’événements

Du Secrétariat du Conseil du Trésor du Canada

Sur cette page

1. Introduction
2. Références
Appendice A : Événements recommandés à consigner

1. Introduction

▶ **Dans cette section**

1.1 But et portée

Pour renforcer la sécurité et accroître la protection du réseau, il faut recueillir, surveiller et détecter les incidents de sécurité au moyen de l’analyse des données des journaux. Pour ce faire, la consignation des événements doit être activée sur tous les actifs de la technologie de l’information (TI) de l’organisation.

Le présent document fournit des conseils de haut niveau sur l’endroit où configurer la consignation des événements sur les actifs de la TI pour qu’elles soient transmises ultérieurement à un système centralisé de consignation des événements et des renseignements de sécurité approuvé par le gouvernement du Canada (GC).

1.2 Contexte

Compte tenu de l’environnement de menaces de plus en plus hostile et pour mieux réagir aux incidents qui découlent des attaques, les organisations du GC doivent recueillir, gérer et analyser des

journaux d'événements qui pourraient aider à la détection d'une attaque, à la détermination de sa portée, à la compréhension ou au rétablissement.

Selon le Computer Security Handling Guide du National Institute of Standards and Technology (NIST), « un événement est tout événement observable dans un système ou un réseau. » [1] Les événements sont saisis dans des journaux et d'autres données structurées et non structurées qui contiennent un enregistrement des événements qui se produisent dans un bien ou un réseau. Les données du journal peuvent fournir un moyen de responsabilisation individuelle, de reconstitution des événements, de détection et/ou de prévention des intrusions et de détermination des problèmes. Un ou plusieurs événements analysés dans un contexte de sécurité peuvent déclencher un incident de sécurité informatique. Le Plan de gestion des événements de cybersécurité du GC (PGEC GC) [2] définit un incident de sécurité informatique comme « tout événement (ou série d'événements), acte, omission ou situation qui entraîne une compromission. »

Pour réagir rapidement et efficacement aux attaques et pour appuyer la gestion des incidents, les journaux doivent contenir suffisamment de renseignements pour déterminer les événements qui se sont produits et qui ou ce qui les a provoqués. En l'absence d'un journal complet des événements, une attaque peut passer inaperçue indéfiniment et les dommages particuliers peuvent être irréversibles. Étant donné que, pour chaque système d'exploitation, chaque application et chaque périphérique réseau, on rédige des journaux d'événements, il est important de trouver un équilibre et un point de référence appropriés pour la consignation dans toute l'organisation.

1.3 Exigences

Les exigences suivantes sont déterminées à partir de diverses références du GC, comme le décrit le tableau ci-dessous.

Tableau 1-1 Exigences

Article	Exigences	Référence
1.	Les pratiques relatives la gestion des événements liés à la sécurité sont définies, documentées, mises en œuvre et tenues à jour afin d'assurer la surveillance, la réponse et le signalement des menaces, des vulnérabilités, des incidents et d'autres événements liés à la sécurité, et de veiller à ce que de telles activités soient coordonnées de façon efficace au sein du ministère, avec les partenaires et dans l'ensemble du gouvernement, ce qui permet de gérer les incidences possibles, d'appuyer la prise de décisions et de permettre la mettre en œuvre des mesures correctives.	*Politique sur la sécurité du gouvernement* [3], A.7
2.	Créer, protéger et conserver les journaux et les dossiers d'audit des systèmes d'information pour permettre la tenue d'activités de surveillance, d'établissement de rapports, d'analyse, d'enquêtes et de mise en œuvre de mesures correctives, selon les besoins de chaque système et conformément aux pratiques ministérielles.	*Directive sur la gestion de la sécurité* [4], B.2.3.8

3.	Analyser les journaux et les dossiers d'audit des systèmes d'information. Examiner les résultats de la surveillance du système, des évaluations de la sécurité, des essais et de l'analyse post-événement. Prendre des mesures préventives, réactives et correctives pour corriger certaines lacunes et veiller à ce que les pratiques et les mesures de sécurité de la TI continuent de répondre aux besoins du ministère.	*Directive sur la gestion de la sécurité, B.2.7.1, B.2.7.2, B.2.7.3, B.2.7.4*
4.	La surveillance continue des événements et du rendement du système et l'inclusion d'une fonction de dossiers d'audit en matière de sécurité dans tous les systèmes d'information permettent de détecter les incidents à l'appui de la prestation continue des services. Il est essentiel qu'un niveau adéquat de consignation et d'établissement de rapports soit configuré aux fins de la portée des services d'informatique en nuage qui relèvent de la responsabilité du GC. Ces documents aideront à ce qui suit : • permettre la détection rapide des activités suspectes; • faciliter les enquêtes et les interventions en cas d'incident de sécurité; • prendre en charge le processus d'audit. Ces mesures s'étendent également aux fournisseurs de services d'informatique en nuage (FSIN) qui doivent surveiller en permanence les composantes de services d'informatique en nuage relevant de leur compétence. Les politiques de conservation de la fonction de journal d'audit doivent être définies conformément aux règles suivantes : • Outil d'évaluation générique de Bibliothèque et Archives Canada pour la technologie de l'information; • autres exigences et normes ministérielles.	Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) 2017-01 [5], Section 6.3.1 Surveillance des systèmes d'information
5.	La détection des événements de cybersécurité potentiels, y compris les incidents de cybersécurité confirmés, par le contrôle des diverses sources d'information (ce qui comprend les solutions logicielles et le matériel des ministères et du reste du gouvernement) et par l'établissement de rapports par les ministères et organismes concernés fait partie de la phase de détection et d'évaluation.	PGEC GC [2]
6.	Pour éviter toute compromission des actifs et des infrastructures reliés à Internet, désactiver tous les ports et services non essentiels et supprimer les comptes inutiles. Un audit au niveau de l'organisation et une solution antivirus sont des éléments clés de toute configuration sécurisée.	Centre canadien pour la cybersécurité (CCCS) – Les 10 principales mesures de sécurité des TI, n° 4 [6]
7.	La surveillance des alertes du système de prévention des intrusions au niveau de l'hôte et la consignation des renseignements permettront de repérer rapidement les intrusions.	Les 10 principales mesures de sécurité des TI du CCCS, n° 8 [6]

1.4 Mesures de sécurité connexes

Voici les mesures de sécurité connexes du document du cadre de gestion des risques liés à la sécurité de la TI CSTI-33 du CCCS [7] : qui dépendent de la consignation et de la surveillance.

Tableau 1 -2 Mesures de sécurité connexes

Mesure de sécurité	Nom
AC-3	Mesure de contrôle d’accès
AC-4	Contrôle du circuit des renseignements
AC-5	Répartition des tâches
AC-8	Avis de l’utilisation du système
AC-17	Accès à distance
AU-2	Événements vérifiables
AU-3	Contenu des dossiers d’audit
AU-4	Capacité de stockage des données d’audit
AU-05	Réponses aux échecs de traitement de vérification
AU-6	Examen, analyse et établissement de rapports de vérification
AU-7	Réduction de la vérification et génération de rapports de vérification
AU-8	Estampilles temporelles
AU-9	Protection des renseignements de vérification
AU-11	Conservation des données d’audit
AU-12	Génération de l’audit
AU-14	Audit de séance
CA-7	Surveillance continue
IR-4	Traitement des incidents
IR-5	Surveillance des incidents
PE-3	Mesure de contrôle d’accès physique
PE-6	Surveillance de l’accès physique
RA-3	Évaluation du risque
RA-5	Balayage de la vulnérabilité
SC-7	Protection des limites des réseaux
SC-26	Pots de miel

SI-4	Surveillance des systèmes d'information
SC-35	Clients leurres
SI-3	Protection des codes malveillants
SI-7	Intégrité des logiciels, des micrologiciels et des renseignements

1.5 Directives de mise en œuvre

On doit tenir compte des directives de mise en œuvre suivantes :

1.5.1 Stratégie de consignation et de surveillance

Le fondement d'une gestion efficace des journaux consiste en une stratégie de consignation et de surveillance organisationnelles définie, telle qu'elle est présentée dans la famille des mesures de la surveillance du système d'information CSTI-33 (SI-4) :

A. L'organisation surveille les systèmes d'information pour détecter ce qui suit :
   1. attaques et indicateurs d'attaques éventuelles, conformément à [Affectation : Objectifs de surveillance définis par l'organisation];
   2. connexions locales, en réseau et à distance non autorisées.
B. L'organisation détermine l'utilisation non autorisée du système d'information par [Affectation : techniques et méthodes définies par l'organisation].
C. Les organisations déploient des appareils de surveillance :
   1. dans le cadre stratégique du système d'information, afin de recueillir des renseignements essentiels déterminés par l'organisation;
   2. dans des emplacements spéciaux du système pour suivre des types particuliers d'opérations présentant un intérêt pour l'organisation;
D. L'organisation protège les renseignements obtenus à partir d'outils de surveillance des intrusions contre tout accès, toute modification ou suppression non autorisé.

La surveillance des systèmes d'information est une exigence de base pour les mesures connexes, en particulier les familles et les mesures identifiées dans le **tableau 1-2 Mesures de sécurité connexes**.

Complément à ces exigences générales, l '**annexe A : Les événements recommandés aux fins de consignation** fournissent une liste d'événements provenant de sources d'événements informatiques communs qui devraient être consignés par les organisations du GC.

Les instruments de politique et de directive du GC mentionnés dans le **tableau 1-1 Exigences** concernent la consignation et l'audit, mais ne fournissent aucun renseignement sur la façon d'établir une stratégie fondamentale de consignation et de surveillance qui satisfait aux exigences des mesures de la norme CSTI-33 précisées ci-dessus. Il est donc recommandé d'examiner les ressources externes suivantes :

- Orientations détaillées du NIST sur l'élaboration d'une capacité de gestion des journaux, y compris des éléments de politique [8].
- Le modèle de l'Institut SysAdmin, Audit, Network, Security (SANS) pour la création d'une politique et la définition des exigences en matière de consignation, ainsi que des rôles et des responsabilités [9]. Ce modèle pose des questions auxquelles il faut répondre dans une politique typique de consignation et de surveillance.

1.5.2 Conservation et préservation des journaux

Bibliothèque et Archives Canada recommande une période de conservation de deux ans après la dernière utilisation administrative en ce qui concerne les renseignements ayant une valeur opérationnelle dans les processus de la TI ou de sécurité [10]. Le bulletin AU-11 du CSTI-33 stipule que les périodes de conservation et de préservation des documents de vérification (c'est-à-dire, les enregistrements de journaux relatifs aux événements vérifiables) sont « définies par l'organisation »; toutefois, le profil des mesures de sécurité de l'informatique en nuage du gouvernement du Canada [11] établit pour ces documents les exigences de conservation suivantes :

- FSIN : Période = [**au moins 90 jours**]
- GC : Période = [**événements et journaux au moins trois mois en ligne et au moins six mois en stockage; événements et journaux associés à un incident de sécurité pendant au moins deux ans**]

Les exigences ci-dessus, propres aux systèmes Protégé B/Intégrité moyenne/Disponibilité moyenne hébergés dans le nuage, peuvent être appliquées de la même façon aux systèmes Protégé B/Intégrité moyenne/Disponibilité moyenne hébergés sur place, y compris l'enregistrement de sécurité pour les systèmes énumérés à **l'annexe A : Événements recommandés pour la connexion**.

Les exigences en matière de conservation et de préservation des journaux pour les autres données sur les événements recueillies auprès des systèmes informatiques du GC au-dessus ou au-dessous du système Protégé B/Intégrité moyenne/Disponibilité moyenne, y compris celles énumérées dans l'annexe, devraient être définies dans les instruments de politique organisationnelle et les profils des mesures de sécurité de la TI et d'autres types de normes. La politique devrait établir un équilibre entre les exigences de réduction des risques et les incidences opérationnelles, telles que les coûts d'immobilisations et les besoins en ressources.

1.5.3 Protection les renseignements figurant au journal

Les installations de consignation et les renseignements sur les journaux doivent être protégés contre toute effraction et tout accès non autorisés, car, quelle que soit l'ampleur de la consignation effectuée par une organisation, ces journaux ne valent rien si leur intégrité ne peut être vérifiée. Les journaux de l'administrateur et de l'exploitant sont souvent des cibles pour effacer les pistes d'activités et les preuves de la présence d'un attaquant.

Les mesures communes de protection des informations sur les journaux sont les suivantes :

- Vérification de l'activation de la consignation des événements pour les composants du système.
- Veiller à ce que seules les personnes ayant des besoins pour l'exercice de leurs fonctions puissent consulter les fichiers journaux.
- Confirmer que les fichiers journaux actuels sont protégés contre les modifications non autorisées par des mécanismes des mesures de contrôle d'accès, la ségrégation physique et/ou la ségrégation du réseau.
- Veiller à ce que les fichiers journaux actuels soient rapidement sauvegardés sur un serveur de journaux centralisé ou sur un support non effaçable.
- Utilisation de mécanismes de vérification de l'intégrité des fichiers pour détecter les modifications non autorisées apportées aux fichiers de configuration de consignation des événements et aux fichiers journaux.

1.6 Directives supplémentaires

1.6.1 Windows

Des instructions supplémentaires pour les environnements Windows sont disponibles dans les documents suivants :

- **La National Security Agency repère son adversaire grâce à la surveillance du journal des événements de Windows (août 2015)** [12]**.** Cet article fournit une introduction à la collecte des journaux d'événements importants des postes de travail Windows et à leur stockage dans un emplacement central pour faciliter la recherche et la surveillance de l'état du réseau**.** Le document aide les administrateurs à configurer la collection centrale de journaux d'événements. On recommande un ensemble d'événements de base à collecter sur un réseau intégré à l'aide de la stratégie de groupe et des outils intégrés déjà disponibles dans le système d'exploitation Microsoft Windows.
- **Pratiques exemplaires de Microsoft pour sécuriser Active Directory** [13] [14] : Cet article traite de plusieurs sujets, allant de la défense contre différentes attaques sur les installations Active Directory à la recommandation d'une liste exhaustive d'événements à surveiller dans un domaine donné.
- **Présentation du Centre national de cybersécurité sur la consignation à des fins de sécurité** [15] : Cette orientation aidera à concevoir une approche de la consignation qui permettra de répondre à certaines des questions typiques posées lors d'un incident cybernétique, comme les suivantes :
  - Que s'est-il passé?
  - Quelles sont les incidences?
  - Que devrions-nous faire ensuite?

- Y a-t-il eu des mesures correctives efficaces après l'incident?
- Nos mesures de sécurité fonctionnent-elles?

1.6.2 Nuage

Les approches de surveillance de la sécurité des actifs d'informatique en nuage publics présentent des similitudes et des différences par rapport à celles des environnements informatiques traditionnels. Il existe des menaces propres au nuage, mais les entreprises sont plus susceptibles d'être confrontées aux menaces traditionnelles qui touchent leur environnement d'informatique en nuage et aux menaces provenant du nuage qui touchent leur environnement informatique traditionnel.

La surveillance des événements dans un nuage nécessite une combinaison d'outils traditionnels, tels que des outils de renseignements sur la sécurité et de gestion des événements ou de prévention de la perte de données, et des outils d'origine nuageuse, tels que les courtiers en accès d'informatique en nuage sécuritaire, la gestion de la posture de la sécurité du nuage ou plateformes de protection de la charge de travail dans le nuage, afin de répondre aux besoins en matière de détection. Les principaux FSIN offrent tous des options de consignation et de gestion des journaux des événements d'origine nuageuse, dont la pertinence devra être évaluée par chaque organisation en fonction de ses besoins et de ses contraintes. On recommande d'activer et d'exploiter ces fonctions de consignation et de surveillance au sein de chaque plateforme. Toutefois, les organisations du GC devraient tenir compte des incidences financières et logistiques.

Les documents suivants renferment des conseils supplémentaires pour trois environnements d'informatique en nuage communs :

- **Consignation et audit Azure** [16] **:** Azure offre un large éventail d'options de consignation et d'audit de sécurité configurables pour vous aider à cibler les lacunes de vos stratégies et mécanismes de sécurité. Cet article traite de la génération, de la collecte et de l'analyse de journaux de sécurité à partir de services hébergés sur Azure.
- **Amazon Web Services (AWS)** [17] [18] : Les journaux d'Amazon CloudWatch sont utilisés pour surveiller et stocker les fichiers journaux et y accéder à partir des instances Elastic Compute Cloud (EC2) d'Amazon (Amazon EC2), CloudTrail des services d'informatique en nuage d'Amazon (AWS), Route 53 et d'autres sources.
- **Plateforme d'informatique en nuage de Google** [19] : Les journaux d'audit du nuage aident les équipes de sécurité à maintenir les pistes d'audit dans la plateforme d'informatique en nuage de Google. Grâce à cet outil, les entreprises peuvent atteindre le même niveau de transparence en matière d'activités administratives et d'accès aux données sur la plateforme d'informatique en nuage de Google que dans les environnements locaux. Chaque activité administrative est enregistrée sur une piste d'audit renforcée et permanente, qui ne peut être désactivée par aucun acteur malveillant.

2. Références

Notes en bas de page

1 National Institute of Standards and Technology, « Computer Security Handling Guide », 2012. [En ligne]. Disponible à : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

2 Secrétariat du Conseil du Trésor du Canada, « Plan de gestion des événements de cybersécurité du Canada », [en ligne]. Disponible à : https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html.

3 Gouvernement du Canada, « Politique sur la sécurité du gouvernement », juillet 2019.

4 Gouvernement du Canada, « Directive sur la gestion de la sécurité », juillet 2019.

5 Secrétariat du Conseil du Trésor du Canada, « Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité, novembre 2017.

6 Centre canadien pour la cybersécurité, « 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada du Centre de la sécurité des télécommunications », novembre 2014.

7 Centre canadien pour la cybersécurité, « La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie » (CSTI-33), 2012.

8 National Institute of Standards and Technology, « Guide pour la gestion des journaux de sécurité informatique », [en ligne]. Disponible à : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

9 SANS Institute, Norme de consignation des renseignements SANS, [En ligne]. Disponible à : https://www.sans.org/security-resources/policies/server-security/pdf/information-logging-standard.

10 Bibliothèque et Archives Canada, « Gestion de l'information » [en ligne]. Disponible à : http://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-gouvernement/lignes-directrices/outils-generiques-evaluation/Pages/gestion-de-linformation.aspx.

11 Gouvernement du Canada, « Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage » [en ligne]. Disponible à : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-

numerique/technologiques-modernes-nouveaux/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html.

12 La National Security Agency repère son adversaire grâce à la surveillance du journal des événements de Windows (version 2), 2015. [En ligne]. Disponible à : https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm.

13 Pratiques exemplaires de Microsoft pour sécuriser Active Directory », [en ligne]. Disponible à : https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory.

14 « Monitoring Active Directory for Signs of Compromise », [Online]. Available: Microsoft, Monitoring Active Directory for Signs of Compromise, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise.

15 Centre national de la cybersécurité, « Introduction à la consignation à des fins de sécurité », juillet 2018. [En ligne]. Disponible à : https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

16 Microsoft, « Consignation et audit Azure », janvier 2019. [en ligne]. Disponible à : https://docs.microsoft.com/en-us/azure/security/azure-log-audit.

17 Services Web d'Amazon, « Que sont les journaux CloudWatch d'Amazon? » [en ligne]. Disponible à : https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html.

18 Amazon, « Renseignements généraux en matière de consignation d'AWS » [en ligne]. Disponible à : https://aws.amazon.com/answers/logging/.

19 Google, « Journaux d'audit lié à l'informatique en nuage » [en ligne]. Disponible à : https://cloud.google.com/audit-logs/.

20 Gouvernement australien, « Lignes directrices en matière de surveillance des systèmes » [en ligne]. Disponible à : https://www.cyber.gov.au/ism.

Appendice A : Événements recommandés à consigner

Le **tableau A-1, Configuration et rendement du système** , reflète les directives pour la collecte des données en matière de configuration et de rendement dans les systèmes d'information.

Tableau A-1 Configuration et rendement du système

Données recommandées	Format	Priorité

État du système (utilisation des ressources, rendement.)	Journal Interroger la base de données Script	MOYENNE
Mises à jour des logiciels Agent utilisateur dans le cas des mises à jour logicielles du périphérique ou de l'hôte	Journal Interroger la base de données Script	MOYENNE
Configuration – Renseignements recueillis régulièrement	Interroger la base de données Script	ÉLEVÉE
Modifications de la configuration Succès et échec	Consignation après un plan d'action de gestion ou une ouverture de séance administrative	MOYENNE

Tableau A-2 Authentification et autorisation

Données recommandées	Format	Priorité
1. Manuel de sécurité de l'information 2019 du gouvernement australien – Alertes et défaillances du système liées à la sécurité. 2. Ajout, suppression et modification des autorisations d'accès aux utilisateurs et aux groupes. 3. Tentatives d'accès non autorisées aux systèmes et fichiers essentiels. 4. Ouvertures de séances d'authentification réussies 5. Les tentatives d'ouverture de séance d'authentification ont échoué. 6. Fermetures de séance d'authentification.	Journal	MOYENNE
Authentification administrative 1. Ouvertures de séances d'authentification réussies. 2. Les tentatives d'ouverture de séance d'authentification ont échoué. 3. Fermetures de séance d'authentification. 4. Hausse des privilèges – Réussite. 5. Hausse des privilèges – Échec.	Journal	ÉLEVÉE
Autorisation Toutes les opérations privilégiées, y compris « sudo », activation de l'accès à l'interface de lignes de commande (CLI), commandes d'administration des systèmes, PowerShell.	Journal	ÉLEVÉE

Tableau A-3 Filtrage de courriels, pourriels et hameçonnage.

Données recommandées	Format	Priorité
Données brutes et métadonnées – Filtrage des événements 1. Date et heure 2. Envoyé par l'expéditeur, par l'expéditeur. 3. Destinataire 4. Objet	Journal Saisie des paquets	MOYENNE

5. En-têtes de courriel 6. Règle déclenchée : journal des politiques comportant les valeurs réelles, y compris, sans toutefois s'y limiter, les dossiers du serveur DNS, l'identificateur de la campagne d'hameçonnage et l'URL du domaine.	Pièces jointes des courriels	
Mises à jour de la politique sur le filtrage de contenu.	Journal	MOYENNE
Modifications du dictionnaire de pourriels.	Journal	MOYENNE
Adresse IP et réputation du domaine (tel qu'il est indiqué au moyen de la connexion au serveur de messagerie).	Journal	FAIBLE

Tableau A-4 Antivirus et protection contre les comportements malveillants

Données recommandées	Format	Priorité
1. Date et heure. 2. Nom d'hôte, adresse IP et nom de port de la source. 3. Nom d'hôte, adresse IP et nom de port de la destination. 4. Description du code malveillant ou de la mesure et gravité. 5. Identité ou (hachage) identificateur du ou des fichiers. 6. Description de la mesure prise – nettoyage, quarantaine, suppression. 7. Mises à jour de la signature.	Journal Pièces jointes	MOYENNE
Indication de l'hôte qui s'est connecté à une URL particulière. • Adresse IP et réputation du domaine • URL • Catégorisation	Journal	ÉLEVÉE

Tableau A-5 Prévention des pertes de données

Données recommandées	Format	Priorité
1. Date et heure. 2. Nom d'hôte, adresse IP et nom de port de la source. 3. Nom d'hôte, adresse IP et nom de port de la destination. 4. Description du code malveillant ou de la mesure et gravité. 5. Identité ou identificateur du ou des fichiers. 6. Description de la mesure prise – nettoyage, quarantaine, suppression. 7. Mises à jour de la signature.	Journal Pièces jointes	FAIBLE

Tableau A-6 Infrastructure de périphériques réseau

L'infrastructure des périphériques réseau devrait inclure DNS, DHCP et WiFi.

Données recommandées	Format	Priorité
Renseignements sur la location du DHCP y compris l'adresse MAC, l'adresse IP.	Journa Saisie des paquets	DE FAIBLE À MOYENNE

DNS – adresse IP et nom de port de la source, adresse IP et nom de port de la destination. 1. Contenu de la requête, de la réponse et des erreurs – tous les types d'enregistrement. 2. Demande de transfert de zone et réponse (journal d'audit). 3. Demande de transfert de zone et réponse (contenu).	Saisie des paquets préférés, sinon inscription au journal.	ÉLEVÉE en ce qui concerne l'analyse DNS, la protection contre les attaques DNS, la protection contre l'exfiltration et l'atténuation contre les domaines malveillants.
1. Journaux d'infrastructure pris en charge au moyen du Wi-Fi, y compris les journaux de sécurité au niveau INFO. 2. Événements du système de détection d'intrusion de réseau et du système de prévention d'intrusion de réseau (IDS/IPS) Wi-Fi. 3. Alertes IDS/IPS Wi-Fi. 4. Journaux d'authentification de périphérique avec l'agent utilisateur. 5. Journaux de navigation des URL + méthodes HTTP (p. ex., POST, GET, etc.). 6. Journaux d'authentification utilisateur. 7. Renseignements sur la location du DHCP y compris l'adresse MAC, l'adresse IP. 8. Journaux de pare-feu affichant l'adresse IP de NAT (Traduction des adresses réseau). 9. Journaux d'itinérance. 10. Horodatages.	Journal Saisie des paquets Données du SNMP, y compris WALK, GET, TRAP	ÉLEVÉE
Mappage du tableau de conversion d'une adresse réseau statique et transfert de ports. 1. Protocole. 2. Port. 3. Adresse IP et nom de port à l'échelle locale et mondiale (intérieur du tunnel). 4. Adresse IP et nom de port à l'échelle locale et mondiale (extérieur du tunnel). 5. Horodatages.	Journal Interroger la base de données Script Dossier Configuration SNMP	LA PLUS ÉLEVÉE

Tableau A-7 Infrastructure de périphériques de réseau

D'autres infrastructures des périphériques de réseau comprendraient des routeurs, des commutateurs, des données de substitution, des pare-feux, des IDS/IPS, des périphériques de passerelle de RPV.

Pour les périphériques comportant plusieurs interfaces, il est souhaitable d'obtenir l'interface MAC – si elle peut être corrélée aux adresses IP et de NAT.

Données recommandées	Format	Priorité
Routeurs et commutateurs	Script	MOYENNE

• Tableaux d'acheminement • Modifications de routage (consignation de toutes les commandes ILC, Protocole de passerelle frontière) • Schéma de l'adresse IP et mise en œuvre	Dossier Configuration	
Hachage du binaire ou des binaires exécuté sur le périphérique	Script	ÉLEVÉE
Pare-feu Tous les événements du pare-feu. Au minimum, si les listes de mesures d'accès sont activées et que le périphérique filtre l'achalandage : 1. Permis d'action, mises à nu, fermetures, refus et abandons. 2. Interface. 3. Nom d'hôte, adresse IP et nom de port, adresse MAC de la source. 4. Nom d'hôte, adresse IP et nom de port, adresse MAC de la destination. 5. Type de protocole. 6. Nom et numéro de la règle appliquée. 7. URL, le cas échéant, utilisateur et agent d'utilisateur associés.	Journal	ÉLEVÉE
Toutes les alertes et tous les événements IDS/IPS 1. Nom d'hôte, adresse IP et nom de port, adresse MAC de la source. 2. Nom d'hôte, adresse IP et nom de port, adresse MAC de la destination. 3. Signature déclenchée et détails associés, y compris la signature, l'anomalie, le seuil de taux. 4. Nom du périphérique. 5. Type d'événement et catégorie. 6. Dans le cas du système de prévention des intrusions réseau Fortinet, le contexte de l'attaque. 7. Agent utilisateur (Web/périphérique), s'il est disponible.	Journal Saisie des paquets	ÉLEVÉE
Passerelle de RPV – tous les événements À tout le moins, pour les acceptations, les mises à nu, les fermetures, les refus et les abandons : 1. Date et heure. 2. Nom d'hôte, adresse IP et nom de port, adresse MAC de la source. 3. Nom d'hôte, adresse IP et nom de port, adresse MAC de la destination. 4. Adresse IP et nom de port, adresse MAC de la source (intérieur du tunnel). 5. Adresse IP et nom de port, adresse MAC de la destination (intérieur du tunnel). 6. Renseignements d'authentification – succès ou échec à l'aide du nom d'utilisateur et du périphérique avec l'agent utilisateur. 7. Changement d'état des connexions ou du tunnel. 8. Validation de l'état du certificat RPV.	Journal	ÉLEVÉE
Filtres des données de substitution et du contenu Web Fournit une adresse IP NAT d'utilisateur et de passerelle pour fournir des rapports améliorés sur les domaines et les adresses IP malveillants. Dans le cas du Web, on utilise le format W3C. 1. Date et heure. 2. Nom d'hôte, adresse IP et nom de port, adresse MAC de la source.	Journal Saisie des paquets	LA PLUS ÉLEVÉE

3. Nom d'hôte, adresse IP et nom de port, adresse MAC de la destination. 4. Méthodes, agent utilisateur, en-têtes décodés de l'URL du site Web. 5. Catégories d'URL. 6. ADRESSE URL. 7. Autorisé, restreint.		
Filtres des données de substitution et du contenu Web 1. Mises à jour de la politique. 2. Mises à jour des logiciels.	Journal	LA PLUS ÉLEVÉE

Tableau A-8 Infrastructure à clés publiques du GC

Données recommandées	Format	Priorité
Tous les événements liés à ce qui suit : • Génération • Révocation • Accès • Mise à jour • Expiration • Récupérer • Réussites de l'authentification • Échec de l'authentification • Journaux du Protocole allégé d'accès annuaire (LDAP)	Journal	ÉLEVÉE

Tableau A-9 Évaluation des vulnérabilités

Données recommandées	Format	Priorité
1. Date et heure. 2. Nom d'hôte, adresse IP et version du système d'exploitation. 3. Ports ouverts. 4. Applications installées. 5. Vulnérabilités répertoriées dans les applications installées. 6. Source de la vulnérabilité et gravité.	Journal	MOYENNE À ÉLEVÉE Corrélation avec la saisie de paquets pour la cyberdéfense et la connaissance de la situation

Tableau A-10 Systèmes d'exploitation

Données recommandées	Format	Priorité
Infrastructure Windows et systèmes d'exploitation. • Pratiques exemplaires de Microsoft pour sécuriser Active Directory [12]. • La National Security Agency repère son adversaire grâce à la surveillance du journal des événements de Windows (août 2015) [11]. • Présentation du Centre national de cybersécurité sur la consignation à des fins de sécurité [14]. • Consignation et transfert d'événements Windows [20].	Journal	ÉLEVÉE

1. Accès des utilisateurs et des administrateurs aux composants et applications du système d'exploitation : a. Accès aux fichiers et aux objets b. Accès au journal d'audit (réussite et échec) c. Accès au système (échec) 2. Rendement du système et caractéristiques opérationnelles : a. Utilisation des ressources, état du processus b. Événements système c. Modifications de l'état du service (p. ex., démarrage, arrêt) d. Échec du service et redémarrage 3. Configuration du système : a. Modifications de la configuration de la sécurité (réussite et échec) b. Journal d'audit effacé c. Changements apportés aux comptes d. Gestion d'utilisateurs ou de groupes 4. Accès aux fichiers : a. Transfert de données vers un média externe 5. Commandes d'exécution Powershell		

Tableau A-11 Niveau des bases de données

Données recommandées	Format	Priorité
1. Ajout de nouveaux utilisateurs, en particulier les utilisateurs privilégiés. 2. Requête, réponse et suivi a. méthode b. commentaires ou variables c. requêtes intégrées multiples d. alertes ou échecs de la base de données 3. Tentatives d'augmentation des privilèges – réussite ou échec. 4. Modifications apportées à la structure de la base de données. 5. Modifications des rôles utilisateur ou des autorisations de la base de données. 6. Mesures de l'administrateur de la base de données. 7. Ouverture de séance et fermeture de séance de la base de données; échec des ouvertures de séance. 8. Utilisation de commandes exécutables. 9. Commandes ILC sur la base de données. 10. Configuration et version de la base de données. 11. Accès à des renseignements de nature délicate dans la base de données, telle que les clés, les mots de passe et les données liées à la confidentialité.	Journal	ÉLEVÉE

Tableau A-12 Niveau d'application

Données recommandées	Format	Priorité
Applications Web • ADRESSE URL • En-têtes • Méthodes HTTP – Demande avec le corps des données • Réponse HTTP avec le corps des données	Journal Saisie des paquets Non chiffré	ÉLEVÉE

Requêtes et réponses de la base de données d'application Web.	Journal	ÉLEVÉE
Panne d'une application Web – Processus ou applications.	Journal	ÉLEVÉE
Configuration et version des applications Web, configuration et version de l'intergiciel.	Journal	ÉLEVÉE
Applications commerciales prêtes à l'emploi standards et personnalisées. 1. Authentification de l'utilisateur (réussite et échec). 2. Utilisation des applications de l'utilisateur et de l'administrateur : a. Accès aux fichiers et aux objets b. Accès au journal d'audit (réussite et échec) c. Accès au système (échec) d. Transactions d'application (visites de pages Web, courriels envoyés ou reçus, transfert de fichiers terminé.) 3. Journaux de transactions. 4. Rendement du système et caractéristiques opérationnelles : a. Utilisation des ressources b. État du processus c. Erreurs (validation d'entrée, opérations non autorisées) d. Événements système e. Modifications de l'état du service (p. ex., démarrage, arrêt.) 5. Configuration et version de l'application.	Journal Tableaux de bord de surveillance des applications	MOYENNE
1. Authentification de l'utilisateur (réussite et échec). 2. Accès de l'utilisateur aux composants de l'application : a. Accès aux fichiers et aux objets b. Accès au journal d'audit (réussite et échec) c. Accès au système (échec) d. Transactions d'application 3. Journaux de transactions. 4. Rendement du système et caractéristiques opérationnelles : a. Utilisation des ressources b. Erreurs (validation d'entrée, opérations non autorisées) et codes de sortie c. État du processus d. Modifications de l'état du service (p. ex., démarrage, arrêt) 5. Configuration et version des applications, configuration et version de l'intergiciel. 6. Renseignements sur l'utilisation, le cas échéant. 7. Événements de demande et de réponse de l'utilisateur, le cas échéant.	Journal	ÉLEVÉE

Tableau A-13 Système de virtualisation

Données recommandées	Format	Priorité
1. Authentification des utilisateurs : a. Ouverture de séance (réussite et échec) b. Tentatives d'accès privilégié (réussite et échec)	Journal	ÉLEVÉE

2. Accès de l'utilisateur et de l'administrateur ou accès racine et actions des composants et des applications : a. Accès aux fichiers et aux objets b. Accès au journal d'audit (réussite et échec) c. Accès au système (échec) 3. Rendement du système et caractéristiques opérationnelles : a. Utilisation des ressources, état du processus b. Événements système c. Modifications de l'état du service (p. ex., démarrage, arrêt.) 4. Configuration du système : a. Modifications de la configuration de la sécurité (réussite et échec) b. Modifications apportées à l'hyperviseur c. odifications apportées aux machines virtuelles d. Modifications apportées au sein des machines virtuelles e. Journal d'audit effacé 5. Création et déploiement des machines virtuelles. 6. Migration des machines virtuelles (p. ex., systèmes source et cible, durée, autorisation). 7. Création et suppression d'objets au niveau du système.		

Tableau A-14 Environnements de nuage

Données recommandées	Format	Priorité
Presque toutes les attaques réussies sur les services d'informatique en nuage résultaient d'erreurs de configuration des clients. Compte tenu de cela, la consignation et la surveillance devraient être axées sur ce qui suit : 1. Toute activité sur le ou les comptes Break Glass (qui ne devraient jamais être utilisés). 2. Modifications de la Politique sur l'accessibilité conditionnelle. 3. Modifications des politiques d'environnement (p. ex., abonnement Azure, services AWS, solutions Google, etc.) dans les journaux de gestion. 4. Changements de rôle privilégiés. 5. Changements au réseau virtuel (RéseauVirtuel). 6. Suppression de la fonction Supprimer les verrous. 7. Modifications des politiques de consignation. 8. Modifications de la gestion de l'identité privilégiée et de la protection de l'identité. 9. Modifications des règles d'alerte (audit de l'auditeur). 10. Voûte pour clés/modifications apportées à la gestion des clés. 11. Journaux de l'API. 12. Journaux d'accès aux fichiers de stockage, fichiers, hachages de fichiers. 13. Écarts par rapport au niveau de référence pour les niveaux d'application de production. 14. Écarts par rapport au niveau de référence pour les niveaux de données de production.	Journal	LA PLUS ÉLEVÉE

▶ Signaler un problème ou une erreur sur cette page

Partagez cette page

Date de modification : 2020-08-05