CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AU-02

Journalisation d'événements

Juill. 2026

Votre gouvernement

Québec

AU

Journaux d'audit, traçabilité des actions

Audit and Accountability

AU-02 — Journalisation d'événements (PaF-) (Obligatoire)

Énoncés :

a. Déterminer les types d'événements que le système est en mesure de journaliser pour soutenir la fonction de vérification [Affectation : types d'événements définis par l'organisation que le système est en mesure de journaliser]
b. Coordonner la fonction de journalisation avec d'autres entités organisationnelles qui nécessitent de l'information en matière de vérification afin d'orienter et d'éclairer la sélection des critères pour les événements à journaliser
c. Préciser les types d'événements suivants pour la journalisation dans le système [Affectation : types d'événements définis par l'organisation (sous-ensemble de types d'événements défini dans le contrôle AU-02A) et fréquence de journalisation (ou la situation qui la justifie) de chaque type d'événement]
d. Expliquer pourquoi les types d'événements sélectionnés pour la journalisation sont jugés adéquats pour soutenir les enquêtes après coup des incidents
e. Vérifier et mettre à jour les types d'événements sélectionnés pour la journalisation tous les [Affectation : fréquence définie par l'organisation]

Paramètres :

a. : - événements liés à l'authentification, l'autorisation et l'accès - événements liés aux données structurées (BD) / non structurées (document) - événements liés aux systèmes d'exploitation - événements liés à l'infrastructure et au réseau - événements de sécurité et de détection - événements d'audit et de conformité
c. Voir le détail sur les événements à journaliser dans la discussion(Québec)
e. ans ou lors d'un changement majeur

Responsable : Partagée

Date limite de mise en oeuvre : 2024-12-14

Discussion :

On entend par événement tout fait observable dans un système. Les types d'événements pour lesquels une journalisation est requise sont liés à la sécurité des systèmes et à la protection de la vie privée. La journalisation d'événements appuie également des besoins particuliers en matière de surveillance et de vérification. Les types d'événements comprennent les changements de mots de passe, les ouvertures de session infructueuses, les accès infructueux aux systèmes, les changements apportés aux attributs de sécurité et de protection de la vie privée, l'accès ou la consultation de renseignements personnels, l'utilisation de privilèges d'administrateur, l'utilisation de justificatifs d'identité numériques, les changements liés aux actions de données, les paramètres de requêtes ou l'utilisation de justificatifs d'identité externes. En définissant l'ensemble des types d'événements pour lesquels une journalisation est requise, les organisations étudient la mise en place d'une vérification adaptée à chacun des contrôles. Par souci d'exhaustivité, la journalisation d'événements inclut tous les protocoles qui sont utilisés et pris en charge par le système. Dans le but d'établir un équilibre entre les besoins en matière de surveillance et de vérification et les autres besoins du système, la journalisation d'événements exige que soit déterminé le sous-ensemble des types d'événements qui seront journalisés à un moment précis. Par exemple, les organisations peuvent déterminer que les systèmes doivent pouvoir journaliser tous les accès aux fichiers, réussis ou non, mais ne pas activer cette capacité – sauf dans certaines circonstances – en raison de la charge potentielle qu'elle représente envers les performances du système. Les types d'événements que les organisations veulent journaliser peuvent changer. L'examen et la mise à jour de l'ensemble des événements journalisés sont nécessaires pour s'assurer que les événements sont toujours pertinents et continuent de soutenir les besoins de l'organisation. Les organisations devraient réfléchir à la façon dont les types d'événements de journalisation peuvent révéler de l'information au sujet des personnes, ce qui donnerait lieu à des risques d'atteinte à la vie privée, et comment atténuer de tels risques. Par exemple, il est possible que des renseignements personnels soient divulgués dans la piste de vérification, en particulier si l'événement de journalisation est basé sur des modèles ou le moment d'utilisation. D'autres contrôles et améliorations de contrôle peuvent faire référence aux besoins en matière de journalisation d'événements, dont le besoin de journaliser des types d'événements particuliers. Cela comprend les contrôles AC-02(04), AC-03(10), AC-06(09), AC-17(01), CM-03F, CM-05(01), IA-03(03)b, MA-04(01), MP-04(02), PE-03, PM-21, PT-07, RA-08, SC-07(09), SC-07(15), SI-03(08), SI-04(22), SI-07(08) et SI-10(01). Les organisations tiennent compte des types d'événements exigés en vertu des lois, des décrets, des directives, des politiques, de la réglementation, des normes et des lignes directrices applicables. Les dossiers de vérification peuvent être créés à différents niveaux, y compris au niveau des paquets lorsque l'information traverse le réseau. La sélection du niveau approprié de journalisation des événements est un élément important de la capacité de surveillance et de vérification dans la mesure où elle peut aider à relever les causes profondes d'un problème. Pour définir les types d'événements, les organisations doivent considérer la journalisation nécessaire pour couvrir les types d'événements connexes, comme les étapes dans les processus distribués basés sur une transaction et les actions qui surviennent dans les architectures orientées service.