CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

AU-06(05)

Analyse intégrée des enregistrements de vérification

Juill. 2026

Votre gouvernement

Québec

AU

Journaux d’audit, traçabilité des actions

Audit and Accountability

AU-06(05) — Analyse intégrée des enregistrements de vérification (PcE-)

Énoncés :

Intégrer l'analyse des enregistrements de vérification et l'analyse de [Sélection (un choix ou plus) : l'information liée au balayage des vulnérabilités; les données de rendement; l'information sur la surveillance du système d'information; {Affectation : données ou information recueillies par d'autres sources définies par l'organisation}] pour accroître sa capacité de détecter les activités inappropriées ou inhabituelles.

Responsable : Aucun

Discussion :

L'analyse intégrée des enregistrements de vérification n'est pas nécessaire pour le balayage des vulnérabilités, la génération de données de rendement et la surveillance du système. L'analyse intégrée nécessite plutôt que l'analyse d'information générée par balayage, surveillance ou autres activités de collecte de données soit intégrée à l'analyse de l'information d'enregistrement de vérification. Les outils de GIES peuvent faciliter le regroupement et la consolidation des enregistrements de vérification produits par les nombreux composants du système, de même que leur analyse et leur mise en corrélation. L'utilisation de scripts normalisés d'analyse des enregistrements de vérification développés par les organisations (complétés par des scripts localisés, au besoin) offre une approche plus rentable de l'analyse de l'information liée aux enregistrements de vérification recueillie. La corrélation entre l'information contenue dans les enregistrements de vérification et celle produite par le balayage des vulnérabilités est importante, car elle permet d'établir la justesse des balayages de vulnérabilités du système et d'établir des liens entre les événements de détection d'attaques et les résultats des balayages. Les liens avec les données de rendement peuvent permettre de détecter des attaques par déni de service ou d'autres types d'attaques qui entraînent l'utilisation non autorisée de ressources. Les associations avec l'information sur la surveillance du système peuvent contribuer à détecter des attaques et à établir un lien accru entre l'information de vérification et les situations opérationnelles.