CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SI-03(08)

Détection des commandes non autorisées

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-03(08) — Détection des commandes non autorisées (-F-)

Énoncés :

a. Détecter les commandes non autorisées du système d'exploitation dans l'interface de programmation d'application du noyau de [Affectation : composants matériels des systèmes désignés par l'organisation] : [Affectation : commandes non autorisées du système d'exploitation définies par l'organisation]
b. [Sélection (un choix ou plus) : Émettre un avertissement; vérifier l'exécution de la commande; empêcher l'exécution de la commande]

Paramètres :

a. à définir par l'organisme: à définir par l'organisme
b. à définir par l'organisme selon le contexte Informations additionnelles dans le contexte de l'administration publique du Québec : - exigences du ministère de la Cybersécurité et du Numérique (MCN)

Responsable : Partagée

Discussion :

La détection des commandes non autorisées peut être appliquée aux interfaces essentielles autres que les interfaces axées sur le noyau, y compris les interfaces avec machines virtuelles et applications privilégiées. Les commandes non autorisées des systèmes d'exploitation comprennent les commandes pour des fonctions du noyau provenant de processus du système auxquels on n'accorde pas la confiance nécessaire pour initialiser de telles commandes, ainsi que les commandes pour des fonctions du noyau qui semblent suspectes, mêmes si les commandes de ce type pourraient vraisemblablement être initialisées par ces processus. L'organisation peut faire en sorte que la détection des commandes malveillantes soit effectuée à partir d'une combinaison de types de commandes, de classes de commandes ou d'occurrences précises de commandes. L'organisation peut également définir les composants matériels à partir de types de composants, de composants, de leur emplacement dans le réseau ou d'une combinaison de ces éléments. L'organisation peut choisir entre différentes mesures en fonction du type, de la classe ou de l'occurrence des commandes malveillantes.