CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

CM-08(03)

Détection automatisée de composants non autorisés

Juill. 2026

Votre gouvernement

Québec

CM

Gestion sécurisée des configurations système

Configuration Management

CM-08(03) — Détection automatisée de composants non autorisés (-F-)

Énoncés :

a. Détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système au moyen de [Affectation : mécanismes automatisés définis par l'organisation] [Affectation : fréquence définie par l'organisation]
b. Prendre les mesures suivantes lorsque des composants non autorisés sont détectés : [Sélection (un choix ou plus) : désactiver l'accès réseau de ces composants; isoler les composants; aviser {Affectation : personnel ou rôles définis par l'organisation}]

Paramètres :

a. solution moderne contre les logiciels malveillants; en continu avec un délai de détection maximal de 5 minutes
b. isoler le composant, alerter ou notifier les détenteurs, administrateurs/pilotes de l'actif et tout autre personne jugée d'intérêt

Responsable : OP

Discussion :

La détection automatisée de composants non autorisés est appliquée en plus de surveiller les connexions à distance et les appareils mobiles non autorisés. La surveillance des composants de systèmes non autorisés peut être effectuée de façon continue ou lors d'analyses périodiques des systèmes menées à cette fin. Les mécanismes automatisés peuvent également être utilisés de façon à empêcher la connexion de composants non autorisés (voir le contrôle CM-07(09)). Des mécanismes automatisés peuvent être mis en place dans les systèmes ou dans des composants de système distincts. Lors de l'acquisition et de la mise en oeuvre de mécanismes automatisés, les organisations doivent déterminer si de tels mécanismes dépendent de la capacité des composants du système à prendre en charge un agent ou du programme demandeur à détecter étant donné que certains composants n'ont pas d'agents ou ne peuvent pas en prendre en charge (par exemple, des dispositifs de l'Internet des objets ou des capteurs). On peut isoler les composants de système non autorisés en les plaçant dans des domaines ou des sous-réseaux séparés ou en les mettant en quarantaine. On appelle souvent ce type d'isolation le principe du bac à sable.