CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-05(03)

Détection et surveillance

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-05(03) — Détection et surveillance (--M)

Énoncés :

a. Utiliser les outils de surveillance suivants pour détecter les indicateurs d'attaques par déni de service visant le système ou lancées à partir de celui-ci : [Affectation : outils de surveillance définis par l'organisation]
b. Surveiller les ressources système suivantes pour déterminer si elles sont suffisantes pour prévenir les attaques par déni de service fructueuses : [Affectation : ressources du système définies par l'organisation]

Responsable : Aucun

Discussion :

Les organisations examinent l'utilisation et l'importance des ressources de systèmes, lorsqu'elles gèrent les risques liés à des attaques par déni de service pouvant résulter d'attaques malveillantes. Les attaques par déni de service peuvent provenir de sources internes ou externes. Les ressources sensibles aux attaques par déni de service sont les fonctions de stockage sur disque matériel, la mémoire et les cycles des unités centrales de traitement (UCT). Au nombre des techniques qui permettent de prévenir les attaques par déni de service visant les fonctions et la capacité de stockage, on retrouve l'imposition d'une limite pour les disques, une configuration des systèmes qui permet d'alerter automatiquement les administratrices et administrateurs lorsque la limite d'une capacité de stockage est atteinte, l'utilisation de technologies de compression de fichiers dans le but de maximiser l'espace de stockage, et l'imposition de partitions distinctes pour les données système et les données d'utilisateur.