CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SI-04(04)

Trafic de communications entrant et sortant

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-04(04) — Trafic de communications entrant et sortant (PaFF)

Énoncés :

a. Déterminer les critères à utiliser pour détecter les activités ou conditions inhabituelles ou non autorisées relatives au trafic de communications entrant et sortant
b. Surveiller le trafic de communications entrant et sortant [Affectation : fréquence définie par l'organisation] pour détecter toute [Affectation : activité ou condition inhabituelle ou non autorisée définie par l'organisation]

Paramètres :

b. en continu; toute action non autorisée (à définir par l'organisme selon le contexte) Informations additionnelles dans le contexte de l'administration publique du Québec : - configurations et politiques de prévention de la perte de données sensibles standardisées par le MCN

Responsable : Partagée

Discussion :

Les activités ou conditions inhabituelles ou non autorisées liées au trafic de communications entrant et sortant du système comprennent le trafic interne qui indique la présence de code malveillant ou l'utilisation non autorisée de code ou de justificatifs légitimes dans des systèmes organisationnels, ou la propagation sur des composants de système, le signalement de systèmes externes et l'exportation non autorisée de l'information. Les preuves du code malveillant ou de l'utilisation non autorisée de code ou de justificatifs légitimes permettent de détecter les systèmes ou les composants de systèmes potentiellement compromis.