CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SI-04(11)

Analyse des anomalies du trafic de communications

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-04(11) — Analyse des anomalies du trafic de communications (PaFF)

Énoncés :

Analyser le trafic de communications sortant des interfaces externes au système et [Affectation : points internes dans le système définis par l'organisation] afin de relever les anomalies.

Responsable : Aucun

Discussion :

Les points internes définis par l'organisation comprennent les sous-réseaux et les sous-systèmes. Les anomalies dans les systèmes organisationnels comprennent les transferts de fichiers volumineux, les connexions permanentes à long terme, les tentatives d'accès à l'information depuis des emplacements inattendus, l'utilisation de protocoles et de ports inhabituels, l'utilisation de protocoles réseau non surveillés (par exemple, l'utilisation du protocole IPv6 lors d'une transition au protocole IPv4) et les tentatives de communication avec des adresses externes présumées malveillantes.