CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SI-04(24)

Indicateurs de compromission

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-04(24) — Indicateurs de compromission (PaFF)

Énoncés :

Découvrir, collecter et distribuer à [Affectation : personnel ou rôles définis par l'organisation] les indicateurs de compromission fournis par [Affectation : sources définies par l'organisation].

Responsable : Partagée

Discussion :

Les indicateurs de compromissions sont des artéfacts judiciaires des intrusions qui ont été relevées dans le système de l'organisation au niveau de l'hôte ou du réseau. Ils fournissent de l'information précieuse sur les systèmes qui ont été compromis. Les indicateurs de compromission peuvent comprendre la création de valeurs de clés de Registre. Les indicateurs de compromission du trafic réseau comprennent des éléments du localisateur de ressources uniformes (URL pour Universal Resource Locator) ou du protocole qui indiquent que les serveurs ont reçu des instructions de commande et de contrôle (C2) d'un programme malveillant. L'adoption et la distribution rapides des indicateurs de compromission peuvent améliorer la sécurité de l'information en réduisant le laps de temps pendant lequel les systèmes et les organisations sont vulnérables aux mêmes exploits ou attaques. Les indicateurs de menace, les tactiques, les techniques, les procédures et les autres indicateurs de compromission peuvent être accessibles dans le cadre de coopérations gouvernementales et non gouvernementales, comme le Forum of Incident Response and Security Teams (FIRST), l'Échange canadien de menaces cybernétiques (ECMC) et le ministère de la Cybersécurité et du Numérique (MCN) en tant qu'équipe d'intervention en cas d'urgence informatique (CERT-QC).