CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SI-04(12)

Alertes automatisées générées par l'organisation

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-04(12) — Alertes automatisées générées par l'organisation (PaFF)

Énoncés :

Alerter [Affectation : personnel ou rôles définis par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation] lors de répercussions potentielles des activités inhabituelles ou inappropriées suivantes sur la sécurité ou la protection de la vie privée : [Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes].

Paramètres :

détenteurs, administrateurs/pilote de l'actif et tout autre personne jugée d'intérêt; à définir par l'organisme (ex.: courriel, message texte, notification tableau de bord, signals auditifs/visuels, etc.); à définir par l'organisme (ex.: accès inhabituel à des fichiers sensibles, utilisation d'outils non autorisés, utilisation abusive d'un compte privilégié, envoi de données sensibles par courrier électronique à une adresse électronique personnelle, etc.)

Responsable : OP

Discussion :

Le personnel organisationnel sur la liste de notification des alertes comprend les administratrices et administrateurs de système, les propriétaires responsables de la mission ou des activités, les propriétaires de système, les hauts fonctionnaires du ministère responsables de la sécurité de l'information, les hauts fonctionnaires ou cadres supérieures ou supérieurs en matière de protection de la vie privée, les responsables de la sécurité des systèmes ou les responsables de la protection de la vie privée. Par alertes automatisées générées par l'organisation, on entend les alertes de sécurité générées par les organisations et celles diffusées par l'intermédiaire de moyens automatisés. Les sources des alertes générées par l'organisation mettent l'accent sur les autres entités, comme les rapports des activités suspectes et les rapports sur les menaces internes potentielles. Contrairement aux alertes générées par l'organisation, les alertes générées par le système dans le contrôle SI-04(05) mettent l'accent sur les sources d'information qui sont internes aux systèmes, comme les enregistrements de vérification.