CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

# SI-04

## Surveillance des systèmes

Juill. 2026

Votre gouvernement

Québec

# SI

# Intégrité des systèmes et des données

*System and Information Integrity*

# SI-04 — Surveillance des systèmes (PaFF)

**Énoncés :**

**a.** Surveiller le système afin de détecter :
- **1.** des attaques et des signes indiquant de possibles attaques conformément aux objectifs de surveillance : [Affectation : objectifs de surveillance définis par l'organisation]
- **2.** des connexions locales, réseau ou à distance non autorisées

**b.** Détecter les utilisations non autorisées du système au moyen des techniques et des méthodes suivantes : [Affectation : techniques et méthodes définies par l'organisation]
**c.** Évoquer les capacités de surveillance interne ou déployer des dispositifs de surveillance :
- **1.** stratégiquement dans le système pour collecter l'information que l'organisation juge essentielle
- **2.** de manière aléatoire pour faire le suivi des types de transactions qui l'intéressent particulièrement

**d.** Analyser les anomalies et les événements détectés
**e.** Ajuster le niveau d'activité de la surveillance du système lorsqu'il y a un changement dans le risque associé aux activités et aux biens organisationnels, aux individus, à d'autres organisations ou au gouvernement
**f.** Obtenir un avis juridique concernant les activités de surveillance des systèmes
**g.** Fournir [Affectation : renseignements liés à la surveillance du système définis par l'organisation] à [Affectation : personnel ou rôles définis par l'organisation] [Sélection (un choix ou plus) : au besoin; {Affectation : fréquence définie par l'organisation}]

**Paramètres :**

a.
- **1.** tout événement de sécurité pouvant porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité (à définir par l'organisme); toutes menaces ou indicateurs de compromission (IOC) communiqués par le CERT-QC; les événements de sécurité d'intérêts communiqués par le chef gouvernemental de la sécurité de l'information (CGSI)

**b.** solution antivirus avec fonctionnalités d'Endpoint Detection and Response (EDR), solution de prévention de la perte de données, journalisation des événements de sécurité
**g.** à définir par l'organisme ou à la demande du chef gouvernemental de la sécurité de l'information (CGSI)

**Responsable :** OP

**Discussion :**

La surveillance du système est à la fois interne et externe. La surveillance externe comprend l'observation des événements qui surviennent dans les interfaces externes du système. La surveillance interne comprend l'observation des événements qui se produisent à l'intérieur du système. Les organisations surveillent le système en observant les activités liées à la vérification en temps réel ou en observant d'autres aspects du système, comme les tendances d'accès, les caractéristiques d'accès et d'autres opérations. Les objectifs de la surveillance orientent et éclairent la détermination des événements. La capacité de surveillance du système est possible grâce à une variété d'outils et de techniques, notamment les systèmes de détection et de prévention des intrusions, les logiciels de protection contre le code malveillant, les outils d'analyse, les logiciels de surveillance des enregistrements de vérification et les logiciels de surveillance des réseaux. Selon l'architecture de sécurité, la distribution et la configuration des dispositifs de surveillance peuvent avoir une incidence sur le débit aux principales frontières internes et externes, ainsi qu'à d'autres emplacements du réseau en raison de l'introduction de la latence du débit sur le réseau. S'il est nécessaire de gérer le débit, de tels dispositifs sont stratégiquement placés et déployés dans le cadre d'une infrastructure de sécurité panorganisationnelle établie. Les dispositifs de surveillance sont déployés à des emplacements stratégiques, notamment dans des emplacements du périmètre sélectionnés et près des principaux serveurs et des batteries de serveurs qui prennent en charge les applications essentielles. Les dispositifs de surveillance sont habituellement employés aux interfaces gérées associées aux contrôles SC-07 et AC-
- **17.** L'information collectée est déterminée par les objectifs de surveillance de l'organisation et la capacité des systèmes de prendre en charge de tels objectifs. Des types précis de transactions d'intérêt comprennent, par exemple, le trafic du protocole de transfert hypertexte (HTTP pour Hypertext Transfer Protocol) qui contourne les mandataires HTTP. La surveillance des systèmes fait partie intégrante des programmes de surveillance continue et d'intervention en cas d'incident de l'organisation et les résultats d'une telle surveillance servent de fondement à ces programmes. Les exigences en matière de surveillance du système, dont la surveillance selon le type de système, peuvent se trouver dans d'autres contrôles (par exemple, les contrôles AC-02G, AC-02(07), AC-02(12)a, AC-17(01), AU-13, AU-13(01), AU-13(02), CM-03F, CM-06D, MA-03A, MA-04A, SC-05(03)b, SC-07A, SC-07(24)b, SC-18B et SC-43B). Les ajustements apportés aux niveaux de surveillance du système sont basés sur des renseignements relatifs au maintien de l'ordre, du renseignement brut ou d'autres sources d'information. La légalité des activités de surveillance du système repose sur les lois, les décrets, les directives, la réglementation, les politiques, les normes et les lignes directrices applicables.