CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

# SI-20

## Contamination

Juill. 2026

Votre gouvernement

Québec

# SI

## Intégrité des systèmes et des données

*System and Information Integrity*

# SI-20 — Contamination (Pc--)

**Énoncés :**

Intégrer les données ou les capacités dans les systèmes ou les composants de systèmes suivants pour déterminer si les données organisationnelles ont été exfiltrées ou ont été supprimées de façon inappropriée de : [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

**Responsable :** Aucun

**Discussion :**

Plusieurs cyberattaques ciblent l'information organisationnelle ou l'information que l'organisation conserve au nom d'autres entités (par exemple, les renseignements personnels), puis exfiltrent ces données. Par ailleurs, des attaques internes et des procédures effectuées par erreur par les utilisatrices ou utilisateurs peuvent supprimer l'information sur le système, ce qui va à l'encontre des stratégies organisationnelles. Les approches en matière de contamination peuvent être passives ou actives. Une approche passive à la contamination peut consister à ajouter de faux noms de courriel et de fausses adresses dans une base de données interne. Si l'organisation reçoit un courriel à l'une des fausses adresses, elle sait que la base de données a été compromise. De plus, comme l'organisation sait que le courriel a été envoyé par une entité non autorisée, elle sait que tous les paquets de données compris dans le courriel contiennent probablement du code malveillant et que l'entité non autorisée peut possiblement avoir obtenu une copie de la base de données. Une autre approche à la contamination peut comprendre l'intégration de fausses données ou de données stéganographiques dans les fichiers pour permettre aux données d'être repérées dans le cadre d'analyses de source ouverte. Pour finir, une approche active à la contamination peut comprendre l'intégration d'un logiciel dans les données, qui est capable d'envoyer des signaux « à la maison » pour alerter l'organisation de sa « capture » (et possiblement son emplacement), et de fournir le chemin par lequel il a été exfiltré ou supprimé.