CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SI-04(16)

Corrélations entre les résultats des activités de surveillance

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-04(16) — Corrélations entre les résultats des activités de surveillance (PaFF)

Énoncés :

Établir des corrélations entre les outils et les mécanismes de surveillance employés dans l'ensemble du système.

Responsable : Aucun

Discussion :

Établir des corrélations entre les résultats des différents outils et mécanismes de surveillance des systèmes peut fournir une vue d'ensemble plus complète des activités se déroulant dans le système. Établir des corrélations entre les outils et les mécanismes de surveillance qui travaillent habituellement de manière isolée – notamment, les logiciels de protection contre les programmes malveillants, la surveillance des hôtes et la surveillance des réseaux – peut fournir une vue d'ensemble de l'organisation et révéler des modèles d'attaques qui seraient autrement restés inaperçus. Comprendre les capacités et les limites de différents outils et mécanismes de surveillance et savoir comment maximiser l'utilisation des renseignements générés par ces outils et mécanismes peut aider l'organisation à mettre sur pied, exploiter et maintenir des programmes de surveillance efficaces. La corrélation de l'information sur la surveillance est particulièrement importante lorsque les organisations passent des anciennes aux nouvelles technologies (par exemple, la transition des protocoles réseau IPv4 à IPv6).