CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SC-30

Dissimulation et détournement

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-30 — Dissimulation et détournement (PcEE)

Énoncés :

Employer les techniques de dissimulation et de détournement suivantes pour [Affectation : systèmes désignés par l'organisation] à [Affectation : périodes définies par l'organisation] : [Affectation : techniques de dissimulation et de détournement définies par l'organisation].

Responsable : Aucun

Discussion :

Les techniques de dissimulation et de détournement permettent de réduire considérablement la capacité de ciblage des adversaires (comme les créneaux et la surface d'attaque) qui préparent et lancent des cyberattaques. Par exemple, les techniques de virtualisation permettent aux organisations de dissimuler les systèmes et, éventuellement, de réduire la probabilité de réussite des attaques tout en évitant les coûts importants associés à la mise en place de plateformes multiples. L'usage accru des techniques de dissimulation et de détournement – notamment le facteur aléatoire, le facteur d'incertitude et la virtualisation – peut suffisamment confondre et désorienter les adversaires et, ultérieurement, accroître le risque de découverte ou d'exposition de leur savoir-faire. Les techniques de dissimulation et de détournement peuvent accroître le temps dont les organisations disposent pour effectuer les fonctions liées à la mission et aux activités de l'organisation. La mise en œuvre des techniques de dissimulation et de détournement sur un système peut ajouter en complexité et en charge de gestion.