CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-30(02)

Facteur aléatoire

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-30(02) — Facteur aléatoire (PcEE)

Énoncés :

Employer [Affectation : techniques définies par l'organisation] pour introduire le facteur aléatoire dans la gestion des activités et des biens organisationnels.

Responsable : Aucun

Discussion :

Le facteur aléatoire introduit un niveau accru d'incertitude dans l'esprit des adversaires relativement aux mesures que les organisations prennent pour protéger leurs systèmes contre les attaques. En effet, de telles mesures peuvent freiner la capacité des adversaires à cibler correctement les ressources informationnelles des organisations qui assurent le soutien de fonctions essentielles liées à leurs missions et à leurs activités. L'incertitude peut également faire hésiter les adversaires avant de lancer ou de poursuivre des cyberattaques. Les techniques de détournement qui recourent au facteur aléatoire comprennent la prise de mesures de routine à divers moments de la journée, l'emploi de diverses technologies de l'information, le recours à différents fournisseurs et la rotation des rôles et des responsabilités au sein du personnel organisationnel.