CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SI-07(17)

Autoprotection des applications d'exécution

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-07(17) — Autoprotection des applications d'exécution (-M-)

Énoncés :

Mettre en œuvre [Affectation : contrôles définis par l'organisation] pour assurer l'autoprotection des applications d'exécution.

Responsable : Aucun

Discussion :

L'autoprotection des applications d'exécution fait appel à l'instrumentation du moteur d'exécution pour détecter et bloquer l'exploitation des vulnérabilités logicielles en tirant avantage de l'information tirée du logiciel en cours d'exécution. La prévention de l'exploitation du moteur d'exécution diffère des mesures de protection traditionnelles basées sur le périmètre dans la mesure où les mécanismes de protection et les pare-feu ne peuvent détecter et bloquer les attaques qu'au moyen de l'information réseau, sans connaître le contexte. La technologie d'autoprotection des applications d'exécution peut faire en sorte que les logiciels soient moins susceptibles aux attaques en surveillant ses intrants et en bloquant ceux qui pourraient donner lieu à des attaques. Elle peut également aider à protéger l'environnement d'exécution contre les changements indésirables et le trafiquage. Lorsqu'une menace est détectée, la technologie d'autoprotection des applications d'exécution peut prévenir l'exploitation et prendre d'autres mesures (par exemple, envoyer un message d'avertissement à l'utilisatrice ou utilisateur, mettre fin à la session de l'utilisatrice ou utilisateur, arrêter l'application ou envoyer une alerte au personnel de l'organisation). Les technologies d'autoprotection des applications d'exécution peuvent être déployées en mode surveillance ou en mode protection.