CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-35

Identification des programmes malveillants externes

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-35 — Identification des programmes malveillants externes (PbMM)

Énoncés :

Inclure les composants de systèmes qui tentent proactivement d'identifier les programmes malveillants en provenance du réseau ou les sites Web malveillants.

Responsable : Aucun

Discussion :

L'identification des programmes malveillants externes diffère des leurres mentionnés dans le contrôle SC-26 dans la mesure où les composants analysent activement les réseaux, y compris Internet, à la recherche de code malveillant contenu sur les sites Web externes. Comme pour les leurres, le recours à des techniques d'identification des programmes malveillants externes exige la prise de mesures d'isolation pour s'assurer que tout code malveillant découvert lors de la recherche et exécuté par la suite n'a aucune incidence sur les systèmes organisationnels. La virtualisation est une technique courante qui permet de réaliser une telle isolation.