CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

RA-03(04)

Cybernanalyse prédictive

Juill. 2026

Votre gouvernement

Québec

RA

Évaluation des risques

Risk Assessment

RA-03(04) — Cybernanalyse prédictive (PbMM)

Énoncés :

Faire appel aux capacités d'automatisation et d'analyse avancées suivantes pour prédire et identifier les risques qui pèsent sur [Affectation : systèmes ou composants de systèmes désignés par l'organisation] : [Affectation : capacités d'automatisation et d'analyse avancées définies par l'organisation].

Responsable : Aucun

Discussion :

Un COS doté des ressources appropriées ou une équipe d'intervention en cas d'incidents informatiques (CIRT pour Computer Incident Response Team) pourrait être dépassé par le volume d'information généré par la prolifération des outils et des appliances de sécurité, à moins qu'il n'ait recours à l'automatisation et à l'analyse évoluées pour analyser les données. Les capacités d'automatisation et d'analyse évoluées sont généralement prises en charge par les concepts d'intelligence artificielle (IA), dont l'apprentissage automatique (AA). Les exemples comprennent la découverte de menaces et l'intervention automatisées (ce qui inclut les capacités de collecte à grande échelle, d'analyse basée sur le contexte et d'intervention adaptative), les opérations de flux de travail automatisées et les outils de prise de décision assistée par ordinateur. Il convient de remarquer que les adversaires dotés de moyens sophistiqués pourraient être en mesure d'extraire l'information relative aux paramètres d'analyse et d'entraîner l'AA de nouveau pour classifier une activité malveillante comme étant anodine. Par conséquent, l'AA devrait faire l'objet d'une surveillance humaine pour veiller à ce que ces adversaires dotés de moyens sophistiqués ne puissent pas camoufler leurs activités.