CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

RA-10

Chasse aux cybermenaces

Juill. 2026

Votre gouvernement

Québec

RA

Évaluation des risques

Risk Assessment

RA-10 — Chasse aux cybermenaces (PaFF)

Énoncés :

a. Établir et maintenir une capacité de chasse aux cybermenaces de manière à :
- **1.** relever les indicateurs de compromission dans les systèmes organisationnels
- **2.** détecter, suivre et contrer les menaces qui visent les contrôles existants

b. Avoir recours à la capacité de chasse aux cybermenaces [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

La chasse aux cybermenaces est un moyen de cyberdéfense actif contrairement aux mesures de protection passives traditionnelles, comme les pare-feu, les systèmes de détection et de prévention des incidents, la mise en quarantaine du code malveillant dans des bacs à sable et les technologies et systèmes de GIES. La chasse aux cybermenaces porte sur la recherche proactive des systèmes, des réseaux et de l'infrastructure d'une organisation pour des menaces avancées. L'objectif consiste à suivre les cyberadversaires et à contrer leurs activités le plus tôt possible dans la séquence d'attaque afin d'accroître de façon mesurable la vitesse et l'exactitude des réponses de l'organisation. Les indicateurs de compromission comprennent le trafic réseau inhabituel, les changements inhabituels apportés aux fichiers et la présence de code malveillant. Les équipes de chasse aux cybermenaces tirent avantage du renseignement sur les menaces existant et peuvent en créer du nouveau, qu'elles échangent ensuite avec des organisations homologues, des organisations d'échange et d'analyse de l'information (ISAO pour Information Sharing and Analysis Organizations), des Centres d'échange et d'analyse de l'information (ISAC pour Information Sharing and Analysis Centers) et les ministères et organismes concernés du gouvernement.