CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

IR-04(14)

Centre des opérations de sécurité

Juill. 2026

Votre gouvernement

Québec

IR

Gestion des incidents de cybersécurité

Incident Response

IR-04(14) — Centre des opérations de sécurité (PaFF)

Énoncés :

Établir et tenir à jour un centre des opérations de sécurité.

Responsable : Aucun

Discussion :

Un centre des opérations de sécurité (SOC pour Security Operations Centre) est le centre névralgique pour les opérations de sécurité et la défense des réseaux informatiques d'une organisation. L'objectif du centre des opérations de sécurité est de défendre et de surveiller en permanence les systèmes et les réseaux d'une organisation (c'est-à-dire la cyberinfrastructure). Le Centre des opérations de sécurité est aussi chargé de détecter, d'analyser et d'intervenir en temps opportun lors d'incidents de cybersécurité. L'organisation dote en personnel technique et opérationnel le centre des opérations de sécurité (par exemple, des analystes de la sécurité, du personnel chargé des interventions en cas d'incident, des ingénieures et ingénieurs en sécurité des systèmes) et met en oeuvre une série de contrôles techniques, procéduraux ou opérationnels (y compris ceux qui touchent la surveillance, l'analyse et les outils de criminalistique) pour surveiller, fusionner, mettre en correspondance, analyser et intervenir en fonction de données d'événements de menace et d'événements touchant la sécurité provenant de diverses sources. Ces sources comprennent les défenses du périmètre, les périphériques réseau (par exemple, routeurs et commutateurs) et des sources de données d'agents d'extrémité. Le centre des opérations de sécurité offre une capacité globale en matière de connaissance de la situation pour aider les organisations à déterminer la posture de sécurité du système et de l'organisation. Une capacité de centre des opérations de sécurité peut être obtenue de plusieurs façons. Les plus grandes organisations peuvent mettre en place un centre des opérations de sécurité dédié alors que des organisations plus petites peuvent faire appel à des organisations tierces pour fournir une telle capacité. Si un incident de sécurité venait à impliquer la compromission de renseignements personnels, le personnel du centre des opérations de sécurité devrait faire appel à des professionnelles et professionnels de la protection de la vie privée dans des organisations. En ce qui a trait aux organisations détenant un nombre important de renseignements personnels, il convient pour celles-ci d'avoir des représentantes et représentants dotés d'une expertise en matière de protection de la vie privée au sein de leur centre des opérations de sécurité parmi leur personnel technique et opérationnel.