CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

IR-04(11)

Équipe intégrée d'intervention en cas d'incident

Juill. 2026

Votre gouvernement

Québec

IR

Gestion des incidents de cybersécurité

Incident Response

IR-04(11) — Équipe intégrée d’intervention en cas d’incident (PbMM)

Énoncés :

Établir et maintenir une équipe intégrée d’intervention en cas d’incident qui peut être déployée à tout endroit identifié par l’organisation dans [Affectation : délais définis par l’organisation].

Responsable : Aucun

Discussion :

Une équipe intégrée d’intervention en cas d’incident est une équipe d’expertes et experts qui évalue, documente et intervient en cas d’incidents de manière à ce que les systèmes organisationnels et les réseaux puissent récupérer rapidement et mettre en oeuvre les contrôles nécessaires pour éviter d’éventuels incidents. Le personnel de l’équipe d’intervention en cas d’incident comprend des analystes d’informatique judiciaire et de programmes malveillants, des développeuses et développeurs d’outils, les architectes ou ingénieures et ingénieurs de système, les praticiennes et praticiens de la protection de la vie privée et les membres du personnel affectés aux opérations en temps réel. La capacité de traitement des incidents comprend l’exécution rapide de la préservation de la preuve criminalistique et de l’analyse et de l’intervention face aux intrusions. Pour certaines organisations, l’équipe d’intervention en cas d’incident peut être une entité interorganisationnelle. Une équipe intégrée d’intervention en cas d’incident facilite l’échange d’information et permet au personnel de l’organisation (par exemple, les développeuses et développeurs, les personnes chargées de la mise en application et les opératrices et opérateurs) de tirer profit des connaissances de l’équipe concernant la menace afin de mettre en oeuvre des mesures de défense qui permettront aux organisations de décourager plus efficacement les intrusions. De plus, les équipes intégrées facilitent la détection rapide d’intrusions, l’élaboration de mesures d’atténuation appropriées et le déploiement de mesures de défense efficaces. Par exemple, dès qu’une intrusion est détectée, l’équipe intégrée peut rapidement développer des mesures que les opérateurs peuvent mettre en oeuvre, corréler le nouvel incident à l’information liée aux intrusions précédentes et élargir le développement du renseignement sur la cybersécurité en cours. Les équipes intégrées d’intervention en cas d’incident sont mieux en mesure d’identifier les tactiques, techniques et procédures liées aux opérations ou à des fonctions opérationnelles et de mission et définir les mesures d’intervention à prendre qui ne perturberont pas les fonctions liées à la mission et aux activités de l’organisation. Les équipes d’intervention en cas d’incident peuvent être réparties dans les organisations pour assurer une meilleure résilience.