CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

IR-04(12)

Programme malveillant et analyse criminalistique

Juill. 2026

Votre gouvernement

Québec

IR

Gestion des incidents de cybersécurité

Incident Response

IR-04(12) — Programme malveillant et analyse criminalistique (PbMM)

Énoncés :

Analyser un programme malveillant ou d'autres artéfacts qui restent dans le système après l'incident.

Responsable : Aucun

Discussion :

Lorsqu'elle est effectuée avec soin dans un environnement isolé, l'analyse d'un programme malveillant et d'autres artéfacts résiduels d'un incident ou d'une brèche de sécurité peut procurer à l'organisation une connaissance approfondie sur les tactiques, les techniques et les procédures utilisées par les adversaires. Elle permet aussi d'indiquer l'identité ou certaines caractéristiques définies de l'adversaire. De plus, l'analyse des programmes malveillants peut aider l'organisation à élaborer des interventions en vue d'éventuels incidents.