CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-11(08)

Analyse dynamique du code

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-11(08) — Analyse dynamique du code (PcEE)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte utilise des outils d'analyse dynamique du code pour relever les défauts courants et documenter les résultats de l'analyse.

Responsable : COCD

Discussion :

L'analyse dynamique du code fournit une vérification d'exécution des programmes informatiques au moyen d'outils permettant de signaler l'occurrence de corruption de la mémoire, ainsi que les problèmes liés aux privilèges des utilisatrices et utilisateurs ou d'autres éventuels problèmes de sécurité. L'analyse dynamique du code met à profit des outils d'exécution pour vérifier si les fonctionnalités de sécurité s'exécutent comme prévu. Il existe un type d'analyse dynamique, que l'on nomme également test à données aléatoires, qui provoque des défaillances de programme en introduisant délibérément des données mal formatées ou aléatoires dans les programmes informatiques. Les stratégies des tests à données aléatoires se fondent sur l'utilisation prévue des applications et sur les spécifications de fonctions et de conception des applications. Pour comprendre la portée des analyses dynamiques du code et de l'assurance qu'elle fournit, les organisations peuvent également envisager de mener des analyses de couverture de code (par exemple, la vérification du degré auquel le code a été testé au moyen de mesures, comme le pourcentage des sous-routines testées ou le pourcentage des instructions de programme appelées pendant l'exécution de la suite de tests) et/ou des analyses de concordance (par exemple, le signalement des mots qui sont mal placés dans le code du logiciel, notamment les termes dérogatoires ou les mots qui ne sont pas de l'anglais ou du français).