CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-11(01)

Analyse statique du code

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-11(01) — Analyse statique du code (PbMM)

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 statique du code pour identifier les défauts courants et documenter les résultats de l'analyse.

Paramètres :

-

Responsable : OP

Discussion :

L'analyse statique du code dicte la technologie et la méthodologie employées pour les examens de sécurité et comprend une vérification des lacunes dans le code, ainsi que l'intégration de code ou de bibliothèques qui contiennent des vulnérabilités connues ou qui sont désuets et non pris en charge. L'analyse statique du code peut être utilisée pour relever les vulnérabilités et imposer l'adoption des pratiques de codage sécurisé. Elle est particulièrement efficace lorsqu'elle est utilisée dans les premières phases du processus de développement, au moment où les changements de code peuvent être automatiquement analysés dans le but de trouver les lacunes. L'analyse statique du code peut fournir des conseils clairs en matière de correction et relever les défauts à corriger par les développeuses et développeurs. Les preuves d'une mise en oeuvre adéquate de l'analyse statique peuvent comprendre l'agrégation de la densité des défauts pour les types de défauts critiques, la preuve que les défauts ont été inspectés par les développeuses, les développeurs ou les spécialistes de la sécurité et les preuves que les défauts ont été corrigés. Une forte densité de résultats ignorés (couramment appelés de faux positifs) pourrait être le symptôme d'un problème lié au processus ou à l'outil d'analyse. Dans de tels cas, les organisations établissent la validité des preuves en les comparant à celles obtenues d'autres sources.