Sécurité applicative : difficile de trouver le juste prix

Complexe, élevé… ou les deux : peut mieux faire sur le *pricing*. Tous les « leaders » du Magic Quadrant de l'AST (tests de sécurité des applications) ont droit à la remarque.

Ces « leaders » sont au nombre de cinq. Deux américains (Synopsys et Veracode), un britannique (Micro Focus), un indien (HCL Software) et un israélien (Checkmarx).

Sur ce marché se distinguent trois typologies de solutions :

- SAST (analyse statique, portant sur les fichiers sources)
- DAST (analyse dynamique, lors de l'exécution des applications)
- IAST (analyse « interactive », qui combine les deux autres approches)

Pour l'édition 2021 de ce Magic Quadrant, Gartner a élargi son périmètre d'analyse. Il y a notamment inclus l'IaC, les conteneurs, le *fuzz testing* et les API.

L'AST s'ouvre aux microservices…

Du côté de **Checkmarx**, on bénéficie de bons points sur les outils CxSCA (analyse de composition logicielle) et CxIAST (IAST passif). Gartner fait notamment remarquer la capacité de fonctionnement autonome du premier. Et la capacité de **visualisation des environnements de microservices** dans le second. Il salue aussi la qualité de l'**accompagnement des développeurs** dans l'évaluation et la remédiation des failles.
Les remarques ne sont pas aussi positives sur le volet DAST. En la matière, l'offre de Checkmarx n'est disponible que sous forme de service managé et basé sur les technologies d'un autre fournisseur. Apparaît aussi une tendance de certains clients à se tourner, en cas d'option pour un déploiement SaaS, vers des offres concurrentes. Quant à la tarification, les coûts se révèlent élevés, malgré une simplification du modèle de licence (au nombre d'utilisateurs pour la plupart des produits).

Chez **HCL Software**, la question du *pricing* est plutôt une affaire de complexité. Gartner attribue aussi de mauvais points pour l'UI et pour la qualité du support technique sur des usages avancés.

Au contraire, il distingue positivement les capacités d'**automatisation des analyses SAST** et d'activation des données qui en résultent. Tout en soulignant que HCL bénéficie d'une « bonne réputation » sur la partie DAST – ainsi que sur le IAST, qui fait l'objet d'une offre autonome depuis l'an dernier.

Pour **Micro Focus**, la conclusion est plutôt flatteuse : l'entreprise fournit « **une des offres AST les plus complètes** ». Elle se distingue par ailleurs sur le SAST au sein des environnements de développement et sur l'analyse des prédictions IA. *A contrario*, Gartner regrette, au-delà d'un *pricing* à la fois élevé et complexe, l'absence de *fuzzing* et d'IAST autonomes. Ainsi que la complexité des résultats produits pour les clients qui ne mènent pas ensuite des analyses contextuelles.

… à degrés variables

Concernant **Synopsys**, c'est l'intégration avec l'existant (pratiques de développement et de maintenance) qui pose problème. Gartner se montre plus partagé à propos de l'offre Intelligent Orchestration : son architecture en microservices apporte un **haut niveau de flexibilité**, avec des tests orientés événements ; mais elle manque de maturité. Sur le *pricing*, deux éléments sont pointés. D'une part, un manque d'adéquation au *mid-market*. De l'autre, un processus de contractualisation compliqué.
L'IAST est quand à lui un point positif, pour sa capacité à analyser les microservices. Gartner salue aussi le *plug-in* Code Sight, qui renforce l'intégration des composantes SAST et SCA dans les *process* DevOps.

Veracode, au contraire, a encore ses limites dans la prise en charge de ces *process*, déplore Gartner. Il lui manque notamment l'IaC. Quant à l'analyse des conteneurs, elle se limite aux images Docker et n'est implémentée que dans la brique SCA. Le *pricing*, lui, se révèle élevé, surtout pour les renouvellements.
Les bons points au crédit du fournisseur américain se trouvent sur le DAST (avec l'adjonction d'un service de découverte d'applications), le SCA (associé à un moteur NLP qui étend l'analyse aux *logs* et aux rapports de bugs) et aux **capacité d'analyse au sein des IDE**.

Illustration principale © Shahadat Rahman – Unsplash