Cybersécurité : Kaspersky lance sa sandbox sur site

L'éditeur russe de cybersécurité Kaspersky a confirmé la disponibilité de sa technologie sandbox pour une utilisation sur site (on-premise).

Le logiciel Kaspersky Research Sandbox « ne transfère rien hors de l'infrastructure [du client]. Si nécessaire, il peut tourner via Kaspersky Private Security Network, qui fonctionne en mode diode de données », a déclaré l'éditeur dans un billet de blog.

La solution Kaspersky Research Sandbox émule le système utilisé (Windows sur PC et Android sur smartphone, à ce jour) avec des paramètres aléatoires (nom d'utilisateur, de l'ordinateur, adresse IP, etc.) et imite un environnement utilisé activement.

Les équipes en charge de la sécurité IT peuvent ainsi « créer une copie isolée d'un poste de travail type utilisé par les employés, avec les logiciels spécifiques et les paramètres réseau associés. » De sorte que les logiciels malveillants ne puissent pas distinguer qu'ils fonctionnent sur une machine virtuelle, a précisé Kaspersky.

Détecter les menaces avancées

La solution intègre des fonctions d'analyse du comportement pour détecter les menaces avancées. Elle inclut également une interface de programmation (API) spécifique pour faciliter son intégration avec d'autres solutions de sécurité. Et fournit des rapports détaillés concernant l'exécution des différents fichiers au sein du réseau concerné.

Avec elle, Kaspersky s'adresse aux organisations dotées d'un centre des opérations de sécurité (SOC) ou d'un centre d'alerte et de réaction aux attaques informatiques (CERT) Autant d'organisations qui ont une « politique stricte en matière de partage de données », a commenté Veniamin Levtsov, VP Corporate Business chez Kaspersky.

Les entreprises qui ont besoin d'analyser des menaces complexes sans investissement additionnel pourront opter pour l'offre Kaspersky Cloud Sandbox, lancée en 2018.

(crédit photo © Shutterstock)