Authentification : BlackBerry Cylance lance sa solution dopée à l'IA

Blackberry Cylance, l'unité née du rachat pour 1,4 Md$ de la firme californienne Cylance par le canadien BlackBerry Limited, confirme la mise sur le marché de CylancePersona.

Une solution d'analyse comportementale et biométrique, dopée à l'intelligence artificielle (IA). Avec elle, Blackberry Cylance promeut « une surveillance continue du comportement des utilisateurs [de terminaux] et de leurs données biométriques ». Pour « identifier en temps réel les utilisateurs suspects », en fonction de différentes actions.

Il s'agit de limiter la marge de manoeuvre d'initiés ou d'éléments externes à l'entreprise prêts à exploiter les identifiants d'utilisateurs légitimes pour lancer une cyberattaque.

Comment ? « En réunissant des éléments comme l'authentification initiale, l'analyse biométrique centrée sur l'utilisateur, la surveillance comportementale basée sur l'IA et des réponses actives automatisées », a déclaré Eric Cornelius, directeur produit chez BlackBerry Cylance, cité dans un communiqué.

Authentification en continu

La firme précise que CylancePersona détecte en temps réel des actions « suspectes » de l'utilisateur, du clavier et de la souris. Autant d'actions qui peuvent trahir une usurpation d'identifiants ou une tentative de prise de contrôle à distance d'un dispositif.

Par ailleurs, la solution scrute « les activités de connexion précédentes des utilisateurs, dont l'emplacement, l'heure ou le mode d'authentification ».

Il s'agit de valider ou non des tentatives de connexion en cours. Pour ce faire, CylancePersona surveille l'activité des utilisateurs et détermine un « score de confiance » Cylance. Si ce score est inférieur à un seuil donné en fonction des attentes du client, une action d'authentification renforcée ou une suspension peut être automatiquement déclenchée. Tout en limitant « les faux positifs », selon les promoteurs de l'offre.

Destinée à l'industrie de la cybersécurité, CylancePersona vient enrichir les capacités de prévention, détection et réponse aux menaces de la plateforme d'IA du fournisseur nord-américain. Plus largement, une interface de programmation (API) cloud permet d'intégrer la fonctionnalité « zero-trust » dans des produits tiers.