Cloud : AWS renforce Amazon Inspector pour sécuriser EC2

Amazon Web Services (AWS) a dévoilé de nouvelles fonctionnalités d'Amazon Inspector, son service automatisé d'évaluation de sécurité. Avec l'objectif de renforcer la protection d'applications exécutées sur Amazon Elastic Compute Cloud (Amazon EC2). Le service qui fournit des capacités de calcul redimensionnables aux développeurs.

Il s'agit de simplifier le processus d'évaluation du réseau. Les clients doivent ainsi pouvoir « configurer ces évaluations en quelques clics sur la page de démarrage d'AWS ».

« Le nouveau package de règles d'accessibilité réseau analyse votre configuration Amazon Virtual Private Cloud (VPC). Pour déterminer si vos instances EC2 peuvent être atteintes à partir de réseaux externes tels qu'Internet, une passerelle privée virtuelle, AWS Direct Connect ou un VPC tiers », a expliqué AWS dans un billet de blog.

En d'autres termes, l'outil informe le client d'un éventuel accès externe à ses hôtes.

Rationaliser l'évaluation réseau

AWS déclare fournir aux utilisateurs les moyens de trouver plus rapidement les ports accessibles et, éventuellement, d'en restreindre l'accès. Pour faciliter l'alerte lorsque des ports critiques sont exposés. Et mieux appréhender les vulnérabilités du réseau.

« Le paysage des menaces devient de plus en plus volatile et les exigences de conformité augmentent. Les évaluations de réseau sont donc plus importantes que jamais pour nos clients », a déclaré Ian Massingham, responsable technique EMEA chez AWS.

Avec la technologie de raisonnement automatisé d'Amazon Inspector, la multinationale ambitionne donc de donner aux utilisateurs les moyens de rationaliser l'évaluation réseau.

AWS a précisé que les résultats de sécurité d'Amazon Inspector incluent les : ID d'Amazon Machine Image (AMI), balises d'instance, groupe Auto Scaling, nom d'hôte, adresses IP, noms DNS et ID de sous-réseau de l'instance Amazon EC2 vulnérable.