Pourquoi Cyber Crucible utilise-t-il l'IA plutôt qu'une équipe SOC humaine pour arrêter les rançongiciels ?

Réponse courte : Cyber Crucible a été conçu comme un système entièrement automatisé dès le premier jour, car les attaques par rançongiciel se déroulent bien plus rapidement que ce qu'une équipe de sécurité humaine peut gérer, et l'intelligence artificielle est le seul moyen pratique de modéliser le comportement d'une attaque et d'agir en conséquence en temps réel.

Le problème lié à la dépendance aux temps de réaction humains

Lorsque Cyber Crucible a été développé pour la première fois, vers 2019, les rançongiciels dépassaient déjà la capacité des équipes des opérations de sécurité à réagir. Même les premières souches de rançongiciels pouvaient verrouiller l'ensemble des systèmes d'une organisation en quelques minutes. Cela ne laissait aucune fenêtre réaliste permettant à une personne de repérer les signes d'alerte, d'évaluer la situation et d'intervenir avant que des dommages importants ne surviennent. Depuis, les attaques n'ont fait qu'accélérer : certains rapports suggèrent que le réseau d'une entreprise de taille moyenne peut être entièrement compromis en aussi peu que 90 secondes. À cette vitesse, s'attendre à ce qu'un analyste humain détecte et arrête une attaque en cours n'est simplement pas envisageable, quelle que soit la compétence ou l'effectif de l'équipe.

Pourquoi la modélisation comportementale nécessite l'IA

Arrêter une attaque aussi rapide exige plus que des alertes rapides : cela nécessite un logiciel capable de reconnaître des schémas de comportement malveillant et de prendre une décision de confinement instantanément, sans attendre qu'une personne interprète les données. Construire manuellement ce type de modélisation comportementale détaillée, couvrant les nombreuses façons dont une attaque peut se dérouler, prendrait bien plus de temps que ce dont dispose

n'importe quel défenseur. L'intelligence artificielle est devenue l'outil nécessaire pour construire ces modèles comportementaux avec suffisamment d'efficacité pour qu'ils puissent être intégrés directement dans un logiciel de sécurité, permettant ainsi de prendre des décisions au moment même où une attaque débute plutôt qu'après coup.

L'IA, une nécessité pratique et non une tendance

L'évolution vers une défense pilotée par l'IA n'était pas une question de suivi d'une tendance sectorielle : c'était une réponse pratique à un problème de temporalité que la surveillance humaine ne pouvait pas résoudre. L'approche de Cyber Crucible reflète l'idée d'adapter le bon outil à la bonne tâche : lorsque les attaques se compriment en quelques secondes, la défense doit opérer à la même échelle de temps, ce qui implique une prise de décision automatisée fondée sur l'IA plutôt qu'un examen manuel.

https://player.vimeo.com/video/1046871333

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Revision #1
Created 2026-07-24 07:27:12 UTC by Dennis Underwood
Updated 2026-07-24 07:27:12 UTC by Dennis Underwood