Cyber Crucible réussit-il les tests de simulation de ransomware ?

La meilleure réponse est… cela dépend de la qualité et de la précision des simulations de ransomware, mais nous n’avons pas vu beaucoup de tests de grande qualité qui correspondent aux véritables outils et comportements d’attaque.

Cyber Crucible examine les schémas comportementaux sous-jacents dans l’accès aux fichiers, les comportements de la mémoire, les comportements des processus et les comportements cryptographiques afin d’identifier et de suspendre les activités d’extorsion de données en lien avec une attaque.

Certaines simulations de logiciels d’extorsion de données ont évolué au fil du temps pour devenir une représentation plus fidèle des attaques réelles.

Nous avons connu des simulations qui semblaient se concentrer sur la vérification des contre-mesures d’extorsion de données divulguées par certains fournisseurs, et non sur les techniques des outils d’extorsion et des attaquants eux-mêmes. On pourrait dire : « Tester la contre-mesure, pas l’attaque ».

En réponse, nous ne fuyons jamais les tests contre l’émulation d’attaquants, les tests d’intrusion ou les outils d’extorsion. Nous attaquons régulièrement notre propre logiciel, et rejouons les techniques d’attaquants dont nous avons entendu parler en ligne ou que nous avons trouvées (et stoppées) dans les environnements de nos clients.

Revision #1
Created 2026-07-24 07:02:17 UTC by Dennis Underwood
Updated 2026-07-24 07:02:18 UTC by Dennis Underwood