Nous avons récemment subi une violation. Cyber Crucible peut-il être déployé dans un environnement potentiellement déjà compromis ?

Réponse courte : Oui. Cyber Crucible évalue ce que les programmes font en temps réel plutôt que de rechercher des fichiers connus comme malveillants ; il commence donc à bloquer les comportements malveillants dès son déploiement — y compris ceux d'un attaquant déjà présent dans l'environnement.

Pourquoi une compromission préalable ne l'aveugle pas

Comme la prévention repose sur l'intention comportementale au niveau du noyau, un attaquant déjà présent doit tout de même *agir* — accéder aux données d'identité, s'injecter dans des processus, commencer un chiffrement ou exfiltrer des données. Ce sont précisément ces actions qui déclenchent l'interception.

C'est ainsi que le déploiement dans le secteur des services financiers a révélé une intrusion active et en cours que la pile de sécurité existante n'avait jamais détectée. Cyber Crucible n'a pas été déployé pour enquêter sur une violation connue ; il a été déployé pour rechercher un angle mort, et il a découvert près de 10 000 processus malveillants déjà en cours.

À quoi s'attendre

Le déploiement dans un environnement compromis produit souvent une activité d'interception immédiate et de grande ampleur. C'est l'outil qui fonctionne comme prévu, et il s'agit fréquemment de la première preuve tangible pour une organisation qu'une activité malveillante était déjà en cours.

Revision #1
Created 2026-07-24 07:02:03 UTC by Dennis Underwood

Updated 2026-07-24 07:02:03 UTC by Dennis Underwood