

Wir wurden kürzlich kompromittiert. Kann Cyber Crucible in einer möglicherweise bereits kompromittierten Umgebung bereitgestellt werden?

Kurze Antwort: Ja. Cyber Crucible bewertet, was Programme gerade tun, anstatt nach bekannten schädlichen Dateien zu suchen, und beginnt daher bereits bei der Bereitstellung, böses Verhalten zu stoppen — auch das eines Angreifers, der bereits Fuß gefasst hat.

Warum eine vorherige Kompromittierung keine Rolle spielt

Da die Prävention auf der verhaltensbasierten Absicht auf Kernel-Ebene beruht, muss ein bereits vorhandener Angreifer dennoch *handeln* — auf Identitätsdaten zugreifen, sich in Prozesse einschleusen, mit der Verschlüsselung beginnen oder Daten verschieben. Genau diese Aktionen lösen die Unterbrechung aus.

Auf diese Weise brachte die Bereitstellung im Finanzdienstleistungssektor eine aktive, andauernde Eindringung ans Licht, auf die der bestehende Sicherheits-Stack nie reagiert hatte. Cyber Crucible wurde nicht zur Untersuchung einer bekannten Sicherheitsverletzung eingesetzt, sondern um einen blinden Fleck aufzudecken — und fand dabei fast 10.000 bereits laufende böse Prozesse.

Was zu erwarten ist

Die Bereitstellung in einer kompromittierten Umgebung führt häufig zu sofortiger, umfangreicher Interceptionsaktivität. Das ist das Werkzeug, das wie beabsichtigt funktioniert, und es ist oft der erste eindeutige Beweis, den eine Organisation dafür erhält, dass bereits etwas im Gange war.

Revision #1

Created 2026-07-24 04:39:39 UTC by Dennis Underwood

Updated 2026-07-24 04:39:39 UTC by Dennis Underwood