Wie nutzt Cyber Crucible Speicheranalysen?

Die Kernel-Analysen von Cyber Crucible verfolgen den Zustand des Arbeitsspeichers eines Programms während seines gesamten Lebenszyklus, vom Programmstart bis zum Programmende. Zudem wird der Zustand der Interaktionen im Arbeitsspeicher mit anderen Programmen erfasst.

Die Verhaltensüberwachung prüft auf unsichere Zustände im Arbeitsspeicher des Programms. Dies kann auf einen Exploit, einen Softwarefehler oder bekannte speicherbasierte (sogenannte „dateilose“) Angriffe hinweisen.

Diese Überwachung erfolgt live an den Programmen auf äußerst effiziente Weise, um sicherzustellen, dass der Systembetrieb und die Abläufe des Kunden durch die Analyse von Cyber Crucible nicht beeinträchtigt werden.

Sobald ein mögliches Angreiferverhalten zum Zweck von Identitäts- oder Datendiebstahl oder Erpressung erkannt wird, fließt diese Verhaltensverfolgung und -analyse des Arbeitsspeichers gemeinsam mit anderen erfassten Telemetriedaten in die Entscheidung ein, ob ein Programm beendet werden sollte.

Revision #1
Created 2026-07-24 04:33:45 UTC by Dennis Underwood
Updated 2026-07-24 04:33:45 UTC by Dennis Underwood