Verhindert Cyber Crucible jede Prozessinjektion?

Nein!

Es gibt eine Vielzahl von Aktivitäten auf Systemen, die eine Prozessinjektion darstellen, aber nicht zwangsläufig bösartig sind.

Cyber Crucible macht all diese Prozessinjektionsaktivitäten für die Bedrohungssuche und Ursachenanalyse sichtbar, stoppt die Aktivität jedoch nicht, es sei denn, es beginnen Datenexfiltrations-Aktivitäten wie Datendiebstahl oder Ransomware-Verschlüsselung.

Nachfolgend ein Beispiel für eine Prozessinjektion, die von der Endpoint-Security-Software PC Matic namens PCPitStop durchgeführt wird. Es handelt sich wahrscheinlich um ein Verhalten, das sie zur Überprüfung laufender Prozesse ausführen.

5373968.png?width=680
Dank der kernelbasierten Verhaltensanalyse von Cyber Crucible haben Sie vollständige Sichtbarkeit auf alle Aktivitäten, unabhängig von der Berechtigungsstufe der Software (einschließlich hochprivilegierter Microsoft- oder Antivirus-Anbieter-Software).

Falls eine automatisierte Reaktion durchgeführt wird, können diese Seite sowie die Seite „Prozesserstellungen“ durchsucht werden, um schnelle Untersuchungsergebnisse zu liefern.

Zusätzlich kann die REST-API von Threat-Hunting-Teams genutzt werden, um nach Indikatoren für mögliches bösartiges In-Memory-Tradecraft zu suchen.

Revision #1
Created 2026-07-24 04:33:16 UTC by Dennis Underwood
Updated 2026-07-24 04:33:16 UTC by Dennis Underwood