Was zeigt die Seite „Prozessinjektionen“?

Prozessinjektionen sind eine softwaretechnische Fähigkeit, die in nicht-bösartigem Kontext auftreten kann oder direkt von einem Angreifer genutzt wird. Tatsächlich gehören Prozessinjektionen und die damit verbundenen Techniken zu den bevorzugten Methoden von Angreifern, aus einer Vielzahl von Gründen, die den Rahmen dieses Artikels sprengen würden (aber wenn Sie interessiert sind, können wir Sie auf entsprechende Schulungen verweisen).

Cyber Crucible macht Prozessinjektions-Ereignisse auf Kernel-Ebene sichtbar. Das bedeutet, Sie erhalten vollständige Transparenz über alle Prozesse und deren Informationen, unabhängig von den Berechtigungen dieses Prozesses. Wir haben festgestellt, dass viele der klassischen Telemetriequellen für Sicherheitstools verstummen, sobald Angreifer oder Software ein bestimmtes Berechtigungsniveau erreichen. Niemals wichtige Daten zu verpassen und niemals „stumm“ zu werden, ist ein wesentlicher Bestandteil unseres Zero-Trust-Produktdesigns.

Auf der Seite „Prozessinjektionen“ sehen Sie pro Ereignis die folgenden Angaben, wobei Filter zur Verfeinerung Ihrer Abfragen zur Verfügung stehen:

CC_Showing_All_Process_Injection_Columns.mp4
Im Rahmen einer Untersuchung werden Sie normalerweise feststellen, dass es zusätzliche Aktivitäten auf der Seite „Prozesserstellung“ gibt.

Revision #1
Created 2026-07-24 04:17:48 UTC by Dennis Underwood
Updated 2026-07-24 04:17:48 UTC by Dennis Underwood