¿Qué muestra la página de Inyecciones de Procesos?

Las inyecciones de procesos son una capacidad de ingeniería de software que puede aparecer en un contexto no malicioso, o ser utilizada directamente por un atacante. De hecho, la inyección de procesos y las técnicas asociadas son una de las favoritas de los atacantes, por diversas razones que quedan fuera del alcance de este artículo (pero si nos lo pregunta, podemos orientarlo hacia capacitación al respecto).

Cyber Crucible expone los eventos de inyección de procesos a nivel del kernel. Esto significa que usted tiene visibilidad completa de todos los procesos y su información, independientemente de los permisos de ese proceso. Algo que hemos comprobado es que, una vez que los atacantes o el software alcanzan cierto nivel de permisos, muchas de las fuentes tradicionales de telemetría para las herramientas de seguridad dejan de reportar información. No perder nunca un dato importante, y no quedarse nunca en silencio, es una parte fundamental del diseño de nuestro producto basado en confianza cero (zero trust).

En la página de Inyecciones de Procesos, verá lo siguiente por cada evento, con filtros disponibles para refinar sus consultas:

CC_Showing_All_Process_Injection_Columns.mp4
Normalmente, en el transcurso de una investigación, encontrará que hay actividad adicional en la página de Creación de Procesos.

Revision #1
Created 2026-07-24 01:34:10 UTC by Dennis Underwood
Updated 2026-07-24 01:34:10 UTC by Dennis Underwood