

¿Cyber Crucible detiene toda inyección de procesos?

¡No!

Existe una variedad de actividades que ocurren en los sistemas que constituyen inyección de procesos, pero que no son necesariamente maliciosas.

Cyber Crucible hace visibles todas estas actividades de inyección de procesos para la caza de amenazas y el análisis de causa raíz, pero no detiene la actividad a menos que comiencen las actividades de extorsión de datos, ya sea robo de datos o cifrado por ransomware.

A continuación se muestra un ejemplo de inyección de procesos realizada por el software de seguridad de endpoints PC Matic, denominado PCPitStop. Es probable que se trate de un comportamiento que llevan a cabo para inspeccionar los procesos en ejecución.

5373968.png?width=680

Gracias al análisis de comportamiento a nivel de kernel de Cyber Crucible, usted cuenta con visibilidad completa de todas las actividades, independientemente del nivel de permisos del software (incluyendo software con altos privilegios de Microsoft o de proveedores de antivirus).

Si se realiza una respuesta automatizada, esta página y la página de Creaciones de Procesos pueden consultarse para obtener resultados de investigación rápidos.

Además, los equipos de caza de amenazas pueden aprovechar la API REST para consultar indicadores de posibles técnicas maliciosas en memoria.

Revision #1

Created 2026-07-24 01:47:28 UTC by Dennis Underwood

Updated 2026-07-24 01:47:28 UTC by Dennis Underwood