# ¿Qué sucede si uno de mis productos de seguridad tiene un conflicto con Cyber Crucible?

Cyber Crucible actualmente coexiste con todos los principales proveedores de seguridad, si utilizamos los informes del Cuadrante Mágico de Gartner como métrica de los actores establecidos de la industria.

El software de endpoint de Cyber Crucible es de forma fiable más resiliente que otros software, y eso incluye otras herramientas de seguridad de endpoint. Además, el otro software de seguridad normalmente ni siquiera tiene visibilidad completa del software de Cyber Crucible.

# Otra herramienta de seguridad intenta desactivar Cyber Crucible

## Resumen:

La otra herramienta intenta desactivar parte de Cyber Crucible. No pueden. La herramienta del otro proveedor no ha probado qué sucede cuando otra herramienta (es decir, Cyber Crucible) dice: “no, no me voy a desactivar”. La otra herramienta se bloquea o entra en un estado de error.

## La respuesta de Cyber Crucible:

La respuesta puede ser doble. La primera es incluir el software de Cyber Crucible en la lista blanca del otro proveedor. Esto hará que la otra herramienta ignore el software de Cyber Crucible, lo cual (con suerte) evitará que la otra herramienta entre en un estado de error.

Si eso no funciona, corresponde a nuestro equipo idear una solución. Hemos aprendido que otros proveedores actúan mucho más lentamente (varios meses o nunca) para corregir un error de su

parte.

Históricamente, en las pocas ocasiones en que esto ha ocurrido, básicamente hemos creado un entorno en el que la otra herramienta cree que tuvo éxito. Una analogía no técnica sería dejar que un familiar joven o un hijo le gane a usted en las damas.

# Otra herramienta de seguridad intenta ejecutar código haciéndose pasar por Cyber Crucible

## Resumen:

Esto ocurre muy rara vez, pero ha habido casos en los que una herramienta de seguridad intenta inyectar su código en el programa en ejecución de Cyber Crucible, y ejecutar código haciéndose pasar por nosotros.

Esto no es diferente a que un hacker se haga pasar por una herramienta de seguridad, y no hay manera de diferenciar si un hacker se ha apoderado del programa de seguridad “de confianza” (o de cualquier otro programa de seguridad).

## La respuesta de Cyber Crucible:

No existe un escenario en el que Cyber Crucible permita que otra empresa (o un hacker) ejecute código haciéndose pasar por nuestro producto. La única solución en este momento sería incluir el software de Cyber Crucible en la lista blanca de la herramienta del otro proveedor. No hay mitigación que Cyber Crucible pueda proporcionar para esto, a fin de evitar que la otra herramienta intente este comportamiento.

Afortunadamente, este es un evento muy poco frecuente.

# Cyber Crucible es deshabilitado por otra herramienta

Hubo varios casos en los que herramientas de seguridad con accesos altamente privilegiados intentaban repetidamente deshabilitar el software de Cyber Crucible. Esto incluyó intentos repetidos de eliminar nuestro controlador, o de detener nuestro servicio una y otra vez.

Si bien esos problemas nunca afectaron la defensa contra extorsión, sí impactaron negativamente la experiencia del usuario y el rendimiento del sistema.

Todo eso es histórico.

Si otra herramienta tiene la capacidad, legítima o no, de interrumpir Cyber Crucible, entonces un hacker también podría hacerlo.

Si sospecha u observa que el software de Cyber Crucible se ha visto disminuido de alguna manera, independientemente del software que lo haya causado, por favor contáctenos de inmediato.

Generalmente somos la última herramienta que queda entre un extorsionista y sus datos críticos. No hay lugar para debilidades en esa circunstancia.

Revision #1
Created 2026-07-24 01:46:09 UTC by Dennis Underwood
Updated 2026-07-24 01:46:09 UTC by Dennis Underwood