¿Cyber Crucible tiene falsos positivos? ¿Cuál es la tasa de falsos positivos?

Cyber Crucible se esfuerza por lograr un entorno de producto con 0 falsos positivos. Dicho esto, en ocasiones ocurren falsos positivos. Analicemos de dónde provienen.

Actualmente, la tasa de falsos positivos es de aproximadamente 1 respuesta por mes, por cada 1800 implementaciones/agentes, con total trazabilidad sobre por qué ocurren esas respuestas.

Programa Corrupto Realizando Operaciones Rápidas de Archivos

Ya sea a propósito o debido a una mala programación, a veces los programas se corrompen a sí mismos, o son corrompidos por otros programas mientras se ejecutan. Vemos esto con frecuencia en nuevas funciones de suites de programas grandes, como Microsoft Office, o software personalizado de propiedad exclusiva.

Lo que sucede es que la memoria del programa se corrompe, lo que aumenta el nivel de inspección del programa. Si eso va seguido de un comportamiento de acceso a archivos similar al de una extorsión, Cyber Crucible se ve obligado a suspender el programa. Cada vez somos mejores identificando errores conocidos, y usted al menos podrá ejecutar su programa hasta que falle (algunos se reinician automáticamente, otros no).

En un mundo donde los atacantes no usan el sistema de archivos, y en su lugar secuestran la memoria de los programas en ejecución, debemos actuar con precaución.

Cyber Crucible ahora tiene la capacidad de crear un permiso, en el que, si el Programa A, con los Argumentos A, causa una corrupción en el Programa B, con los Argumentos B, podemos crear una exclusión temporal para:

(Programa A + Argumentos A) abre (Programa B + Argumentos B)

De esa manera no se asume un riesgo adicional de que un atacante esté involucrado, a menos que este utilice exactamente los mismos argumentos.

Un excelente ejemplo de esto fue cuando Microsoft introdujo por primera vez la apertura de documentos de Office desde dentro de su software de chat de escritorio. Corrompía el programa de Office…todas…y…cada…una de las veces…luego el programa de Office comenzaba a escanear todos los Documentos en la máquina aproximadamente el 25% de las veces. Eso… necesitaba una exclusión.

Si experimenta un fallo, use el botón de soporte, y le ayudaremos a crear una exclusión, hasta que el proveedor solucione el problema.

Programas de Seguridad

Cyber Crucible convive muy bien con programas de seguridad. Contrario a lo que la mayoría de los nuevos clientes piensan, las herramientas de seguridad más avanzadas suelen usar interacciones con el sistema más avanzadas que los programas antivirus que utilizan tecnologías más antiguas. De hecho, algunas herramientas de seguridad gratuitas o económicas ejecutan una variedad de scripts de Powershell inseguros como parte clave de su protección, en lugar de programas reales.

Como una herramienta de seguridad altamente resiliente basada en el kernel, es mejor considerar a Cyber Crucible como “más baja”, o “más cercana” al hardware que la mayoría de las demás herramientas. Cyber Crucible identifica automáticamente otras herramientas de seguridad y las agrega a los modelos de comportamiento. Mientras las herramientas de seguridad no muestren señales de estar comprometidas, se les permite operar normalmente.

Ocasionalmente, una herramienta de seguridad provocará inestabilidad en el sistema, cuando sus intentos de desactivar o interferir con el software de Cyber Crucible fallan. En esos casos, es mejor incluir en la lista blanca a Cyber Crucible en la otra herramienta de seguridad, para evitar que intente (sin éxito) deshabilitar o interferir con Cyber Crucible.

No dude en abrir un ticket de soporte con Cyber Crucible, a través del portal web, para discutir el asunto.

Herramientas Administrativas o de Copia de Seguridad

En algunas circunstancias, se debe crear un comportamiento personalizado para una herramienta administrativa o de copia de seguridad, mientras el equipo de Cyber Crucible desarrolla un modelo

de comportamiento mejorado. En este caso, el equipo de Cyber Crucible ayudará en la creación de una excepción en el modelo de comportamiento, que aislará el programa junto con sus argumentos, para una ventana de oportunidad extremadamente pequeña ante un posible ataque.

Revision #1
Created 2026-07-24 01:53:27 UTC by Dennis Underwood
Updated 2026-07-24 01:53:27 UTC by Dennis Underwood