Cómo se compara Cyber Crucible

Respuestas directas a las preguntas de comparación y evaluación que hacen los compradores: frente a EDR, XDR, MDR, antivirus, DLP y recuperación basada en copias de seguridad.

¿Es Cyber Crucible un EDR, XDR, MDR? ¿O algo distinto, como Agentic AI?

Respuesta breve: Tiene elementos tanto de EDR como de XDR, pero la pregunta sobre la categoría no es la correcta. Lo que importa es *dónde se toma la decisión*. La lógica de respuesta de Cyber Crucible se ejecuta enteramente en el endpoint, utilizando únicamente la información disponible allí en el momento del ataque — porque los servidores analíticos remotos introducen dos debilidades fatales: la latencia y la fragilidad.

La respuesta honesta a la pregunta sobre la etiqueta

- **Como EDR:** si un EDR utiliza la telemetría del endpoint para tomar decisiones, entonces la respuesta automatizada de Cyber Crucible es un EDR. Frena el comportamiento de extorsión en milisegundos, utilizando únicamente información local.
- **Como XDR:** la telemetría también se envía a una base de datos (dispositivo del cliente o central) para correlación, threat hunting, trabajo de amenazas internas y auditorías de TI. Según la definición de marketing de XDR, eso también califica.

El equipo se siente cómodo con la expresión "EDR para defensa contra la extorsión", aunque el cómputo en el borde (edge computing) sea visto en algunos círculos como algo de generación anterior. El razonamiento que sigue explica por qué esa visión está equivocada.

Por qué la analítica remota se convirtió en un pasivo — la latencia

La "X" en XDR representa el traslado de la capacidad de cómputo analítico a servidores remotos. Eso otorga potencia, pero cuesta tiempo, y los atacantes construyeron sus técnicas alrededor de esa brecha:

- **Velocidad:** los ataques se aceleraron para que las acciones irreversibles se completen antes de que un servidor analítico pueda responder. Esto se observa especialmente con elementos pequeños y de alto valor, como las contraseñas.

- **Paralelismo:** muchas herramientas de endpoint inspeccionan un programa, esperan y luego pasan al siguiente. Los atacantes ejecutan múltiples programas de extorsión a la vez — 5.000 archivos accedidos en paralelo en lugar de 500.
- **Distribución:** la extorsión se ejecuta simultáneamente en muchas máquinas. Cyber Crucible ha observado aproximadamente 75 máquinas a la vez. Una herramienta se enfrenta entonces a 50 programas en 75 máquinas — 3.750 programas por inspeccionar.
- **Procesos comandantes:** algunos atacantes ejecutan un controlador local que vuelve a generar instantáneamente cualquier herramienta de extorsión que sea eliminada.

Las estrategias de detección y respuesta, por su propia naturaleza, esperan a que el ataque ya esté en curso. La analogía más adecuada es detener a los asaltantes de bancos en la puerta, en lugar de hacerlo después de que cierta cantidad de dinero ya haya salido de la caja fuerte.

Por qué la analítica remota se convirtió en un pasivo — la fragilidad

Alrededor del 80% de las soluciones EDR y XDR necesitan acceso a servidores analíticos remotos para funcionar de manera óptima, y apenas son funcionales sin ese "cerebro" en la nube.

Los atacantes explotan esto directamente: obtienen suficiente acceso para cambiar las reglas del firewall, bloquean la herramienta del endpoint para que no pueda comunicarse con sus servidores analíticos, y la herramienta pierde su capacidad de analizar o responder. Permanece sin ser explotada, instalada, en ejecución — y casi completamente ineficaz.

Lo que Cyber Crucible hace en cambio

Dado que la latencia y la fragilidad hacen insostenible la dependencia de la nube para la defensa contra la extorsión, Cyber Crucible inventó una capacidad de detección y respuesta cuya analítica de comportamiento utiliza **únicamente la información disponible en el endpoint en el momento del ataque**. La interdicción ocurre localmente, típicamente en menos de 200 milisegundos, sin ningún viaje de ida y vuelta a la nube en la ruta crítica.

La telemetría que sí fluye hacia la base de datos respalda la investigación, no la protección — threat hunting, detección de amenazas internas, auditorías de TI — y una API abierta permite alimentar plataformas XDR abiertas, herramientas SOAR o RPA. Ese trabajo es valioso, pero nunca es lo que se interpone entre usted y un ataque en curso.

¿Es Esta una Herramienta de Monitoreo Como Mis Otros Paneles de Seguridad?

La respuesta es que depende de cómo usted y su organización deseen utilizar la herramienta, pero probablemente "no".

Es importante señalar las estrategias de diseño de producto con Cyber Crucible:

1. La protección debe ser hiperautomatizada, y no debe requerir atención constante ni cuidado (atención a alertas), ni ajustes manuales (configuración) por parte de los usuarios.
2. Para los equipos de seguridad con más recursos, la telemetría valiosa debe estar disponible para ellos, para actividades avanzadas de búsqueda de amenazas, o para respaldar actividades de análisis forense y respuesta a incidentes.
3. La acción n.º 2 anterior no debe degradar de ninguna manera la protección implementada en la acción n.º 1.

El comentario más común que recibimos de la dirección de TI es que sus empleados no sabían que Cyber Crucible ya los había estado protegiendo durante semanas.

Tenemos muchos usuarios que aprovechan la herramienta en tres capacidades:

Configurar y Olvidar (Como sus Detectores de Humo)

Muchas organizaciones carecen de los recursos para tener cazadores de amenazas revisando la telemetría de Cyber Crucible (u otra herramienta), pero quieren que el riesgo de extorsión de datos "salga de su lista de preocupaciones". Eso está perfectamente bien, y la Prevención de Extorsión de Datos de Cyber Crucible está diseñada precisamente para eso.

Estos usuarios carecen de los recursos para dedicar tiempo a revisar los flujos de datos de Inyección de Procesos, Protección de Credenciales y Creación de Procesos.

Por lo tanto, encontramos que, a menos que estén respondiendo a una respuesta automatizada poco común por parte de Cyber Crucible, o estén realizando gestión de inventario, como cuando una nueva máquina necesita que se le despliegue Cyber Crucible...

...simplemente no inician sesión en el portal web de Cyber Crucible, y dejan que la automatización simplemente haga su trabajo.

¡Eso está perfectamente bien!

Búsqueda Avanzada de Amenazas + Protección Automatizada

Las capacidades de inyección de procesos, monitoreo de uso de credenciales y creación de procesos proporcionan un rico conjunto de datos, capturados mediante análisis de comportamiento a nivel de kernel, para realizar la búsqueda de amenazas.

La protección automatizada se activa una vez que comienza el robo de datos, el robo de credenciales (token, contraseña) o el cifrado de ransomware. Para todo lo demás, este es un excelente recurso.

El hallazgo más común hasta ahora son herramientas de gestión remota no gestionadas (al menos por los administradores de TI actuales) instaladas por los usuarios. Sí, a veces resultan en una protección automatizada contra la extorsión (es decir, la RMM no gestionada es utilizada por un actor malicioso), pero siempre es mejor conocer más sobre su entorno de antemano, ¡independientemente de eso!

Aquí hay un video rápido de un tipo de ataque que vimos en uso por atacantes, en múltiples entornos de clientes, que se utilizó para evadir con éxito las soluciones EDR de los clientes (no nos gusta mencionar nombres... había 3 productos en cuatro empresas).

rr-com-dll.mp4

Análisis Forense Posterior al Incidente y Remediación

Existen un par de tipos de casos de uso para los datos de Cyber Crucible.

El primero es para que una persona de seguridad en una empresa, o una persona de TI, pueda investigar la causa raíz de la suspensión de un programa. Para algunos clientes, que típicamente

instalan nuestro software y luego solo vuelven a iniciar sesión cuando hay nuevos empleados que incorporar, nunca han utilizado ninguna funcionalidad de Cyber Crucible excepto la página de Gestión de Agentes. Nos complace ayudarles a aprender sobre el análisis de causa raíz, que es sencillo e indoloro para usuarios técnicos y semitécnicos.

El segundo tipo de cliente para el análisis forense posterior al incidente son las firmas de DFIR que son convocadas para investigar un problema en un cliente, a veces a solicitud de la compañía de seguros cibernéticos, y Cyber Crucible se instala después de un incidente. (Oigan, no siempre podemos estar ahí antes que el atacante, por mucho que queramos... ¡de lo contrario, todas las empresas del mundo nos tendrían, y la extorsión sería cosa del pasado!)

La mejor manera de describir una implementación después de un ataque de extorsión es "desordenada". No porque seamos difíciles de instalar o de comenzar a proteger. ¡Todo lo contrario! En ese caso, los atacantes normalmente se han movido por el sistema, y están incrustados en los sistemas operativos, el equipo de red, Active Directory, y están operando en memoria. Múltiples máquinas terminan teniendo procesos suspendidos, y a veces los atacantes incluso intentan recuperar el control. Es un poco como tomar una medicina que al principio te hace sentir mal, pero que necesitas para llegar a mejorar.

Los clientes que ya están estresados a veces reaccionan emocionalmente ante "más" ruido, a medida que los atacantes finalmente son erradicados y derrotados. Hay mucha educación en cuanto a por qué o cómo sus pilas de seguridad existentes no encontraron a los atacantes. Al final, sin embargo, la empresa recupera el control sobre su infraestructura de TI. No se convertirán en una de las 80-90% de las empresas que son re-extorsionadas un año o dos después, en lo que llamamos "la economía de suscripción a la extorsión".

El tercer tipo de cliente que tenemos es un MSSP que, a menudo es socio de Cyber Crucible, y que está respondiendo a una protección automatizada de Cyber Crucible. Necesitan descubrir la manera en que el atacante logró un punto de apoyo temporal, y cerrar cualquier brecha en la seguridad. La buena noticia es que HIPAA u otros informes de cumplimiento normalmente reportan poca o ninguna violación de confidencialidad, debido a la velocidad de la respuesta automatizada. Muchas veces, el MSSP informa "nada que reportar", lo cual hace felices a todos los involucrados. Bueno, excepto al criminal.

¿Cyber Crucible coexiste con otros productos de seguridad?

¡Sí!

Cyber Crucible está actualmente implementado y coexiste con todos los proveedores de seguridad del Cuadrante Mágico de Gartner.

Nuestro software se descubre y configura automáticamente para tener conocimiento de las actividades de las demás herramientas de seguridad.

En el raro caso de que exista un posible conflicto, consulte este artículo de la base de conocimientos.

¿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.

¿En qué se diferencia Cyber Crucible de EDR, XDR y MDR?

Respuesta breve: EDR, XDR y MDR son herramientas de detección y respuesta: observan un ataque, generan una alerta y dependen de una persona o de un servicio en la nube para decidir qué hacer. Cyber Crucible es una herramienta de prevención: decide de forma autónoma en el endpoint y detiene el proceso malicioso en menos de 200 milisegundos, antes de que se produzca ningún daño.

Las diferencias prácticas

	EDR / XDR / MDR	Cyber Crucible
Tiempo de respuesta	De minutos a horas	Menos de 200 milisegundos
Método de detección	Firmas y datos históricos	Intención conductual, sin firmas
Cobertura de día cero	Parcial	Diseñado para amenazas desconocidas
Dependencia humana	Alta — analistas y SOC	Ninguna — totalmente autónomo
Dónde se toman las decisiones	Análisis en la nube	Localmente, en el kernel

Por qué importa esta diferencia

Las herramientas de detección se diseñaron para una época en la que los ataques se desarrollaban a lo largo de horas o días. Los ataques automatizados ahora se completan en segundos. Una herramienta que genera una alerta precisa después de que los datos ya han sido exfiltrados ha documentado la pérdida, no la ha evitado.

Esto no significa que la detección carezca de valor — la informática forense y la investigación son importantes. Significa que la detección por sí sola no puede detener un ataque a la velocidad de una máquina.

¿Cyber Crucible reemplaza mi EDR, o funciona junto a él?

Respuesta breve: Cualquiera de las dos opciones. Cyber Crucible está diseñado para funcionar junto a herramientas EDR, XDR y MDR existentes sin conflictos, y muchos clientes lo implementan de esa manera. También funciona como una capa de prevención independiente si decide reducir su conjunto de herramientas.

Funcionamiento junto a su conjunto de herramientas actual

Cyber Crucible no requiere que elimine nada. Añade prevención autónoma por debajo de la capa de detección que ya posee, y funciona con o sin la presencia de EDR y MDR.

Los clientes con frecuencia comienzan de esta manera de forma deliberada: implementan Cyber Crucible para descubrir qué le falta a su conjunto de herramientas existente. En una implementación del sector de servicios financieros, esa respuesta llegó en 60 días: casi 10,000 procesos maliciosos interceptados que tres EDR y un SOC subcontratado nunca detectaron.

Reducción del conjunto de herramientas

Una vez que los equipos ven con qué frecuencia sus herramientas de detección no actúan, algunos optan por consolidar. No existe dependencia de proveedor ni integraciones forzadas: puede reemplazar su EDR por completo o simplemente reducir el gasto donde no esté justificando su costo.

¿Es Cyber Crucible un antivirus?

Respuesta breve: No. Los antivirus identifican archivos maliciosos conocidos mediante firmas. Cyber Crucible no utiliza firmas en absoluto: evalúa lo que un programa en ejecución realmente está haciendo y detiene el comportamiento malicioso, incluidas las amenazas que nadie ha visto antes.

Por qué las firmas ya no son suficientes

Una firma solo puede describir un ataque que alguien ya ha analizado. Ese modelo falla en dos situaciones comunes:

- **Ataques de día cero (zero-day)**, en los que aún no existe ninguna firma.
- **Ataques sin archivos (fileless)**, en los que no hay ningún archivo con el cual comparar una firma.

La detección basada en firmas también requiere actualizaciones constantes provenientes de fuentes de inteligencia de amenazas, lo que significa que su protección siempre va por detrás del atacante.

Qué lo reemplaza

Cyber Crucible modela el comportamiento —actividad de memoria, actividad de procesos y acceso a archivos— y evalúa la intención en tiempo real. Por eso ha detenido ataques de día cero en redes de clientes hasta 90 días antes de que cualquier otro proveedor los reportara o respondiera públicamente a ellos.

¿Por qué la copia de seguridad y recuperación no es suficiente para hacer frente al ransomware?

Respuesta breve: Las copias de seguridad abordan solo la etapa final de un ataque de ransomware: el cifrado. Para cuando comienza el cifrado, los atacantes generalmente ya han robado credenciales y extraído sus datos. Restaurar desde una copia de seguridad recupera sus archivos; no hace nada respecto a los datos que ya están en manos del atacante.

El ransomware es el último paso, no el primero

Una intrusión típica se desarrolla en tres etapas:

1. **Robo de identidad** — se comprometen credenciales para obtener acceso.
2. **Robo de datos** — se exfiltran propiedad intelectual, registros de clientes y otros datos sensibles.
3. **Cifrado** — los archivos se bloquean y se exige un rescate.

Las estrategias de recuperación entran en juego solo en la tercera etapa. La violación de confidencialidad y la pérdida de control operativo ya han ocurrido.

El costo real

El mayor riesgo empresarial del ransomware generalmente no es el rescate en sí, sino los ingresos perdidos por una interrupción prolongada y el daño reputacional que le sigue. Prevenir el compromiso inicial protege ambos aspectos, razón por la cual la prevención debe preceder a la planificación de recuperación, en lugar de reemplazarla.

¿Por qué capturar las claves de cifrado del ransomware ya no es una defensa válida?

Respuesta breve: La captura de claves dejó de ser técnicamente fiable en 2021. El ransomware moderno evita las bibliotecas de cifrado estándar del sistema operativo, por lo que no existen claves que una herramienta defensiva pueda interceptar; e incluso cuando se obtienen claves, muchas veces no se pueden aplicar.

Cómo el ransomware moderno elude la captura de claves

- **Bibliotecas personalizadas:** el código de cifrado se compila directamente en el malware en lugar de invocar bibliotecas del sistema operativo, de modo que las claves se generan y se utilizan enteramente dentro del propio proceso del atacante, invisibles para las herramientas que vigilan las llamadas estándar.
- **Implementaciones únicas:** algunas variantes utilizan cifrado no estándar y distinto en cada ejecución. Incluso una clave capturada no se puede aplicar, porque el propio algoritmo es a medida.
- **Cifrados de flujo (streaming ciphers):** se basan en un concepto fundamentalmente distinto al de AES y son simplemente inmunes a la captura de claves AES.

Cyber Crucible desarrolló y patentó originalmente la tecnología de captura de claves, y luego presentó el criptoanálisis que demostraba sus límites en BSides Pittsburgh en 2021. Avanzamos hacia otra dirección porque la evidencia así lo indicaba.

El problema de cumplimiento normativo

La captura de claves requiere almacenar las claves de cifrado de forma centralizada, lo que crea un único punto de fallo y un objetivo de alto valor. Un gobierno también podría obligar a acceder a ellas mediante una citación clasificada o una carta de seguridad nacional, sin su conocimiento. Se trata de un riesgo grave de soberanía de datos, sumado a una defensa que ya no funciona.

¿Por qué las herramientas de seguridad de tipo "recolector en la nube" tienen dificultades frente a los ataques modernos?

Respuesta breve: Un recolector en la nube es un agente ligero para endpoints que realiza poco análisis local y, en su lugar, envía telemetría en bruto a una plataforma en la nube para su procesamiento. Ese trayecto de ida y vuelta añade una demora que un ataque automatizado no le concede, y el agente depende de los mismos componentes del sistema operativo que los atacantes comprometen hoy en día.

Por qué la industria lo construyó de esta manera

La ingeniería a nivel de kernel es difícil y costosa. Enviar la telemetría a la nube permitió a los proveedores desarrollar software para endpoints más económico, monetizar el almacenamiento en la nube y comercializar capacidades de "IA en la nube". El modelo se optimizó para facilitar el desarrollo, no para la defensa.

Los dos modos de fallo

1. **Demasiado lento.** Los ataques automatizados de "entrar y arrasar" (smash-and-grab) se completan en milisegundos. La analítica en la nube no puede emitir una respuesta a tiempo.
2. **Ciego justo cuando más importa.** Dado que estos agentes dependen de bibliotecas nativas del sistema operativo para funcionar y recopilar datos, un atacante que comprometa dichas bibliotecas puede silenciar al agente. Este sigue ejecutándose y no reporta nada: un panel de control que indica que todo está bien mientras los datos salen de la organización.

Cyber Crucible procesa localmente en el kernel y toma sus propias decisiones, por lo que no existe un trayecto de ida y vuelta a la nube ni dependencia de un sistema operativo potencialmente comprometido.

¿Cyber Crucible ralentiza mis sistemas?

Respuesta breve: No. El uso típico de CPU es de alrededor del 1 % o menos, y la arquitectura evita deliberadamente la técnica que provoca la mayoría de las ralentizaciones causadas por agentes de endpoint: insertar hooks en las bibliotecas del sistema de Windows.

Por qué otros agentes provocan lentitud

Las herramientas de seguridad heredadas insertan "hooks" en bibliotecas del sistema altamente optimizadas para vigilar comportamientos maliciosos. Esas bibliotecas nunca fueron diseñadas para modificarse sobre la marcha. Cuando una herramienta de seguridad y un atacante manipulan esas bibliotecas al mismo tiempo, el resultado es una degradación significativa del sistema.

El patrón que sigue es predecible: el usuario culpa a la herramienta de seguridad por la lentitud y la elimina. El proveedor no puede reproducir el problema en un laboratorio, sin saber que un adversario con privilegios de nivel raíz está manipulando el sistema. Los atacantes han aprendido a explotar esto deliberadamente, degradando el rendimiento hasta que las víctimas desactivan sus propias defensas.

Un enfoque diferente

Cyber Crucible opera a través de subsistemas independientes dentro del kernel en lugar de insertar hooks en componentes frágiles de Windows, por lo que no compite con el sistema operativo —ni con un atacante— por las mismas rutas de código frágiles.