¿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.

Revision #1
Created 2026-07-24 01:45:13 UTC by Dennis Underwood
Updated 2026-07-24 01:45:13 UTC by Dennis Underwood