

¿Cómo debemos ejecutar una prueba de concepto para una herramienta de prevención?

Respuesta breve: impleméntela junto a su stack existente en un entorno de producción real y compare lo que detecta cada herramienta. El resultado más informativo no es una prueba de laboratorio: es la diferencia entre lo que sus herramientas actuales alertan y lo que realmente se intercepta.

Por qué implementarla en paralelo funciona mejor

La empresa de servicios financieros de nuestro caso mejor documentado hizo exactamente esto. No eliminaron nada. Añadieron Cyber Crucible específicamente para descubrir qué se le estaba escapando a su inversión existente, y obtuvieron una respuesta definitiva en un plazo de 60 días.

Qué medir

- **Intercepciones sobre las que su stack actual nunca alertó.** Esta es la señal principal.
- **Tiempo hasta la decisión.** La prevención debe completarse antes de que se produzca el daño, no antes de que se cierre un ticket.
- **Interrupción del negocio.** Cuente el tiempo de inactividad, los reinicios y las interrupciones provocadas por falsos positivos.
- **Horas de analista consumidas.** La prevención autónoma debe reducir la carga de trabajo, no añadir una cola.

Una advertencia sobre las pruebas de laboratorio

Probar con muestras extraídas de bases de datos de malware a menudo mide muy poco, porque los atacantes diseñan el malware para que permanezca inactivo a menos que reciba una señal de validación de un servidor de mando y control en vivo que ellos aún operan. Una muestra que no

hace nada en su laboratorio no demuestra nada sobre un ataque real.

Revision #1

Created 2026-07-24 01:54:01 UTC by Dennis Underwood

Updated 2026-07-24 01:54:01 UTC by Dennis Underwood