

¿Por qué los MSP y revendedores se asocian con Cyber Crucible?

Respuesta breve: Porque la prevención autónoma permite que un socio conserve el margen, la relación con el cliente y el SLA, en lugar de revender un SOC alojado por el proveedor y asumir la culpa cuando ese SOC no detecta un ataque a velocidad de máquina.

La trampa de revender detección

La industria empujó a los socios a revender servicios de MDR y SOC alojados por proveedores. Cuando el monitoreo impulsado por humanos inevitablemente pasa por alto un ataque automatizado, el proveedor pasa por alto la brecha, y el cliente no despiden al proveedor. Despiden al socio.

Qué cambia a nivel operativo

- Las amenazas se neutralizan de inmediato, antes de que los analistas reciban una alerta.
- El volumen de alertas se reduce drásticamente respecto a las más de 100 por endpoint al día que provocan fatiga de alertas.
- No hay ajuste de reglas YARA ni búsqueda manual de amenazas.
- Los socios capturan el flujo de ingresos en lugar de conformarse con comisiones de proveedor.

Y en cuanto al riesgo

Un socio cuya oferta de seguridad previene ataques en lugar de documentarlos mantiene una conversación fundamentalmente distinta con los clientes sobre resultados y responsabilidad.

Revision #1

Created 2026-07-24 01:52:42 UTC by Dennis Underwood

Updated 2026-07-24 01:52:42 UTC by Dennis Underwood