¿Cómo ayuda Cyber Crucible a gestionar proveedores y resultados de ciberseguridad?

Respuesta breve: Cyber Crucible se encarga de la prevención automatizada en el endpoint, lo que le permite seleccionar y responsabilizar a su propio proveedor de monitoreo o respuesta, en lugar de quedar atado a un servicio empaquetado y difícil de evaluar, vinculado a un único proveedor de EDR o XDR.

El problema oculto de los servicios de seguridad empaquetados

Muchas organizaciones pagan sumas considerables por un centro de operaciones de seguridad alojado que viene junto con un producto particular de detección y respuesta en el endpoint o de detección y respuesta extendida. El problema es que este tipo de arreglo a menudo deja al cliente con poca visibilidad sobre qué tan atento o eficaz es realmente ese servicio de monitoreo. Es posible que no sepa con qué nivel de detalle se está vigilando su entorno, con qué rapidez se escalan los problemas, o si su cuenta es prioritaria para ese proveedor. Debido a que el monitoreo está vinculado a la tecnología subyacente, hay poco margen para negociar, medir o reemplazar el servicio si no cumple con las expectativas.

Separar la prevención del monitoreo restaura el control

Cyber Crucible se centra en la capa de prevención de la protección de endpoints, deteniendo automáticamente los intentos de ransomware, robo de datos y robo de identidad. Debido a que la prevención se gestiona de forma independiente, las organizaciones ya no están obligadas a aceptar un paquete único para detección y respuesta. En cambio, obtiene la libertad de elegir el socio de detección y respuesta gestionada (MDR) o de servicios de seguridad gestionados (MSSP) que mejor se adapte a sus necesidades, ya sea su propio personal interno, un MSSP especializado, u otro proveedor de MDR completamente distinto.

Por qué importa la elección

Esta separación le brinda la capacidad de definir sus propios acuerdos de nivel de servicio, medir la calidad y la capacidad de respuesta del equipo que monitorea su entorno, y responsabilizar a ese proveedor mediante una relación contractual real. En lugar de esperar que un proveedor empaquetado le esté prestando la atención adecuada, puede evaluar y hacer cumplir estándares de desempeño según sus propios términos. En definitiva, el enfoque de Cyber Crucible consiste en otorgar a las organizaciones un control genuino: control frente a los atacantes y, con igual importancia, control sobre las relaciones y contratos con los proveedores que respaldan su programa de seguridad.

https://player.vimeo.com/video/1046829518

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

Revision #1
Created 2026-07-24 02:12:13 UTC by Dennis Underwood
Updated 2026-07-24 02:12:13 UTC by Dennis Underwood