¿Quién es el cliente ideal para la protección contra ransomware de Cyber Crucible?

Respuesta breve: Cyber Crucible es la opción más adecuada para las personas que piensan en términos de impacto empresarial, no solo de características técnicas. Esto incluye a líderes de TI con recursos limitados y a ejecutivos que comprenden lo que incluso una breve interrupción podría costarle a la empresa.

Por qué el pensamiento empresarial importa más que el cargo

No existe un único cargo que defina al cliente ideal de Cyber Crucible. Lo que importa es si la persona comprende las consecuencias reales de un incidente de ransomware o de robo de datos: pérdida de ingresos, interrupción de operaciones y el tipo de daño financiero que puede perdurar durante meses o años después. Alguien con esta mentalidad no necesita que lo convenzan de que la prevención automatizada vale la pena; ya entiende que evitar el tiempo de inactividad está directamente relacionado con proteger las ganancias y mantener el negocio en funcionamiento.

Esto es diferente de una conversación de ventas puramente técnica, en la que el valor de un producto queda enterrado bajo jerga que solo los especialistas pueden seguir. El enfoque de Cyber Crucible, impulsado por FortressAI, se diseñó en torno a un resultado sencillo y práctico para los clientes en primer lugar, con la tecnología subyacente construida para respaldar ese resultado. Debido a esto, las conversaciones más claras suelen darse con personas que se preocupan por lo que significa una falla de seguridad para el negocio, no solo por cómo funciona el software internamente.

Ejemplos de los interlocutores adecuados

Un director de TI que gestiona personal y presupuesto limitados, y que es personalmente responsable del tiempo de actividad y la fiabilidad del sistema, suele comprender el valor rápidamente, ya que el tiempo de inactividad afecta su carga de trabajo diaria y su desempeño.

Por otro lado, un CEO o un CFO puede impulsar la protección automatizada incluso cuando un equipo de seguridad se siente satisfecho con las medidas existentes, simplemente porque reconoce que una breve interrupción, a veces de tan solo una hora, puede generar un daño financiero que tarda más de un año en recuperarse.

El punto en común

Ya sea que la conversación comience con un líder de TI centrado en las operaciones o con un ejecutivo con mentalidad financiera, el ajuste más fuerte para Cyber Crucible es cualquier persona que evalúe la ciberseguridad a través del prisma de la continuidad del negocio y el riesgo financiero, en lugar de únicamente el detalle técnico.

https://player.vimeo.com/video/1046877762?texttrack=es

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

Revision #2
Created 2026-07-24 02:15:22 UTC by Dennis Underwood
Updated 2026-08-06 18:34:56 UTC by Dennis Underwood