

Wer ist der ideale Kunde für den Ransomware-Schutz von Cyber Crucible?

Kurze Antwort: Cyber Crucible eignet sich am besten für Menschen, die in geschäftlichen Auswirkungen denken, nicht nur in technischen Merkmalen. Dazu gehören IT-Verantwortliche mit knappen Ressourcen ebenso wie Führungskräfte, die verstehen, was selbst ein kurzer Ausfall das Unternehmen kosten könnte.

Warum unternehmerisches Denken wichtiger ist als der Jobtitel

Es gibt keinen einzelnen Jobtitel, der den idealen Cyber Crucible-Kunden definiert. Entscheidend ist, ob die Person die realen Konsequenzen eines Ransomware- oder Datendiebstahls versteht: entgangene Umsätze, gestörte Abläufe und die Art von finanziellem Schaden, der sich über Monate oder Jahre hinziehen kann. Jemand mit dieser Denkweise muss nicht davon überzeugt werden, dass automatisierte Prävention sinnvoll ist – er versteht bereits, dass die Vermeidung von Ausfallzeiten direkt mit dem Schutz des Gewinns und der Aufrechterhaltung des Geschäftsbetriebs zusammenhängt.

Das unterscheidet sich von einem rein technischen Verkaufsgespräch, bei dem der Wert eines Produkts in Fachjargon untergeht, dem nur Spezialisten folgen können. Der Ansatz von Cyber Crucible, angetrieben von FortressAI, wurde zunächst um ein einfaches, praktisches Ergebnis für die Kunden herum gestaltet, wobei die zugrunde liegende Technologie entwickelt wurde, um dieses Ergebnis zu unterstützen. Aus diesem Grund entstehen die klarsten Gespräche in der Regel mit Menschen, denen wichtig ist, was ein Sicherheitsvorfall für das Unternehmen bedeutet – nicht nur, wie die Software im Detail funktioniert.

Beispiele für die richtigen Gesprächspartner

Ein IT-Leiter, der mit begrenztem Personal und Budget arbeitet und persönlich für Betriebszeit und Systemzuverlässigkeit verantwortlich ist, erkennt den Nutzen oft schnell, da Ausfallzeiten seinen

täglichen Arbeitsaufwand und seine Leistung beeinträchtigen. Auf der anderen Seite drängt ein CEO oder CFO möglicherweise auf automatisierten Schutz, selbst wenn ein Sicherheitsteam mit den bestehenden Maßnahmen zufrieden ist – einfach weil sie erkennen, dass eine kurze Unterbrechung, manchmal nur eine Stunde lang, einen finanziellen Schaden verursachen kann, von dem man sich erst nach weit über einem Jahr wieder erholt.

Der gemeinsame Nenner

Ob das Gespräch mit einem betriebsorientierten IT-Leiter oder einer finanziell denkenden Führungskraft beginnt – der stärkste Fit für Cyber Crucible ist jeder, der Cybersicherheit aus der Perspektive von Geschäftskontinuität und finanziellem Risiko bewertet, statt allein aus technischer Sicht.

<https://player.vimeo.com/video/1046877762?texttrack=de>

[Auf Vimeo ansehen](#) · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Revision #2

Created 2026-07-24 05:06:12 UTC by Dennis Underwood

Updated 2026-08-06 18:37:05 UTC by Dennis Underwood