Warum arbeiten MSPs und Reseller mit Cyber Crucible zusammen?

Kurze Antwort: Weil autonome Prävention es einem Partner ermöglicht, die Marge, die Kundenbeziehung und das SLA selbst zu kontrollieren – anstatt ein vom Anbieter gehostetes SOC weiterzuverkaufen und die Schuld zu tragen, wenn dieses SOC einen Angriff mit Maschinengeschwindigkeit übersieht.

Die Falle beim Weiterverkauf von Detection

Die Branche hat Partner dazu gedrängt, vom Anbieter gehostete MDR- und SOC-Dienste weiterzuverkaufen. Wenn die menschengesteuerte Überwachung zwangsläufig einen automatisierten Angriff übersieht, verpasst der Anbieter den Vorfall – und der Kunde entlässt nicht den Anbieter. Er entlässt den Partner.

Was sich operativ ändert

- Bedrohungen werden sofort neutralisiert, bevor Analysten überhaupt eine Warnmeldung erhalten.
- Das Alarmvolumen sinkt drastisch gegenüber den 100+ Warnmeldungen pro Endpunkt und Tag, die zu Alarmmüdigkeit führen.
- Kein Feintuning von YARA-Regeln und keine manuelle Bedrohungssuche.
- Partner erschließen sich den Umsatzstrom selbst, anstatt sich mit Anbieterprovisionen zu begnügen.

Und in Bezug auf das Risiko

Ein Partner, dessen Sicherheitsangebot Angriffe verhindert, anstatt sie lediglich zu dokumentieren, führt mit seinen Kunden ein grundlegend anderes Gespräch über Ergebnisse und Verantwortlichkeit.

Revision #1
Created 2026-07-24 04:39:30 UTC by Dennis Underwood
Updated 2026-07-24 04:39:30 UTC by Dennis Underwood