??? ???? Cyber Crucible ????? ????? ???????? ?? ???????

الإجابة المختصرة: تدعم Cyber Crucible وفاءك بالتزاماتك بموجب متطلب توطين البيانات في زامبيا. ويتطلب قانون حماية البيانات في زامبيا من مراقبي البيانات معالجة وتخزين البيانات الشخصية والبيانات الشخصية الحساسة في مركز بيانات أو خادم **داخل زامبيا**. يدعم نشر Cyber Crucible المحلي (on-premises) الوفاء بهذا المتطلب مباشرةً — إذ تعمل الواجهة الخلفية داخل بنيتك التحتية الخاصة، داخل البلد.

?? ?????? ???????

ينظم الجزء العاشر (Part X) من قانون حماية البيانات في زامبيا عمليات نقل البيانات عبر الحدود، وتُلزم المادة 70 مراقب البيانات بمعالجة وتخزين البيانات الشخصية والبيانات الشخصية الحساسة في مركز بيانات أو خادم يقع داخل زامبيا.

هذا **إلزام بموقع التخزين**، وليس اختباراً للضمانات. لا تفي الحماية التعاقدية بهذا المتطلب.

????? ?????? ??? ???? ????? ?????? ????????

لا يمكن لمزود يتطلب منتجه إرسال بيانات القياس عن بُعد (telemetry) الخاصة بنقاط النهاية إلى منطقة سحابية خارج زامبيا أن يلبي المادة 70 عبر تحسين عقوده أو تشفيره. فالمتطلب يتعلق □□□□□ □□□□□ □□□□□□□□ □□□□□□ .

????? ???? ??? ?????? ?????? ????????

- **واجهة خلفية محلية (on-premises)** — تعمل جميع برمجيات الإدارة على خوادم تتحكم بها أنت، داخل زامبيا.
- **تحليل محلي** — يجري تقييم التهديدات والتصدي لها على نقطة النهاية نفسها، بحيث لا تعتمد الحماية أبداً على خدمة خارج البلد.
- **انعدام البيانات الصادرة (zero outbound telemetry)** في التهيئة المعزولة عن الشبكة (air-gapped).

- **نطاق محدود للغاية** — لا يتم أبدًا جمع المفاتيح أو بيانات الاعتماد أو الرموز أو المحتوى، مما يجعل حجم البيانات الشخصية الخاضعة للمادة 70 صغيرًا من الأساس.

> الوضع وقت كتابة هذا المحتوى — يرجى التأكد من المستشار القانوني المحلي، بما في ذلك أي قواعد خاصة بالقطاع.

Revision #2
Created 2026-07-24 03:26:39 UTC by Dennis Underwood
Updated 2026-11-24 04:24:26 UTC by Dennis Underwood