CISA والمركز الكندي للأمن السيبراني يصدران إرشادات لإدارة استهلاك رموز الذكاء الاصطناعي



أصدرت CISA والمركز الكندي للأمن السيبراني وشركاء آخرون إرشادات مشتركة لإدارة استهلاك الرموز في خدمات الذكاء الاصطناعي الخارجية، تتناول التكلفة والتوافر وهجمات استنزاف المحفظة.

- الإرشادات صادرة بشكل مشترك عن CISA والمركز الكندي للأمن السيبراني وشركاء آخرين.
- نماذج الاستخدام القائمة على الرموز في خدمات الذكاء الاصطناعي الخارجية قد تؤثر في التكلفة والأداء وإتاحة الخدمات الحيوية.
- غياب إدارة الاستهلاك قد يسبب تكاليف غير متوقعة وانخفاضاً في التوافر واستنفاد الرموز وهجمات حجب الرموز أو استنزاف المحفظة.
- تشمل الممارسات الموصى بها تحديد أولويات تخصيص الرموز، وكفاءة سير العمل، وتحسين صياغة الطلبات، والتخزين المؤقت، وتحسين البيانات، والمراقبة المستمرة.
- يُشجَّع مشغلو البنية التحتية الحرجة على تحديد الوظائف الحيوية المعتمدة على الذكاء الاصطناعي

> والتخطيط لانخفاض إتاحته.

أصدرت CISA والمركز الكندي للأمن السيبراني (Cyber Centre) مع شركاء آخرين إرشادات مشتركة بعنوان «إدارة استهلاك رموز الذكاء الاصطناعي لدعم المرونة التشغيلية»، تساعد المؤسسات على فهم استخدام الرموز وإدارته عند اعتماد خدمات ذكاء اصطناعي مقدمة من أطراف خارجية.

أهمية استهلاك الرموز

تعتمد خدمات كثيرة على الرموز في احتساب التكلفة وتحديد حدود الاستخدام. وتشير الإرشادات إلى أن ذلك قد يؤثر في التكلفة والأداء وإتاحة الخدمات الحيوية. وعند غياب الإدارة قد تواجه المؤسسات تكاليف متصاعدة وغير متوقعة، وانخفاضاً في توافر الخدمة، وتراجعاً في الأداء، واستنفاداً للرموز. كما تذكر الإرشادات هجمات حجب الرموز واستنزاف المحفظة بوصفها مخاطر محتملة.

ما توصي به الإرشادات

تعرض الوثيقة خطوات عملية في عدة مجالات:

- تحديد أولويات تخصيص الرموز.
- تصميم سير عمل فعّال.
- تحسين طريقة كتابة المستخدمين لطلباتهم.
- الاستفادة من التخزين المؤقت والسياق القابل لإعادة الاستخدام.
- تحسين البيانات قبل إرسالها.
- مراقبة استهلاك الرموز بمرور الوقت.

ويمكن لمالكي ومشغلي البنية التحتية الحرجة الاستفادة منها في تحديد الوظائف الحيوية المعتمدة على الذكاء الاصطناعي، وفهم الاعتماديات على مقدمي الخدمة والعمليات، والتخطيط لانخفاض إتاحة الذكاء الاصطناعي أثناء الانقطاعات أو الحوادث أو فترات الطلب المرتفع. ويمكن للمدافعين السيبرانيين كذلك الاستعانة بها في إدارة العمليات المعتمدة على الذكاء الاصطناعي.

الإرشادات ليست خاصة بقطاع أو بلد بعينه، لكن محاورها، ومنها رسم الاعتماديات والتوافر ومخاطر الأطراف الخارجية، ذات صلة بالمؤسسات المنظمة في المملكة التي تتبنى خدمات الذكاء الاصطناعي.

ما يجب فعله الآن

1. حصر الوظائف المعتمدة على خدمات الذكاء الاصطناعي الخارجية وتصنيف الحيوي منها.
2. مراجعة عقود مقدمي الخدمة والحدود التقنية المتعلقة بحصص الرموز ومعدلات الطلب ونماذج الفوترة.
3. وضع ميزانيات للرموز ومراقبة الاستهلاك وتنبيهات لرصد القفزات غير الطبيعية التي قد تدل على استنزاف المحفظة.
4. إدراج انخفاض إتاحة الذكاء الاصطناعي أو فقدانها في خطط استمرارية الأعمال والاستجابة للحوادث.

5. إصدار إرشادات داخلية حول صياغة الطلبات بكفاءة والتخزين المؤقت وتقليص البيانات قبل إرسالها.