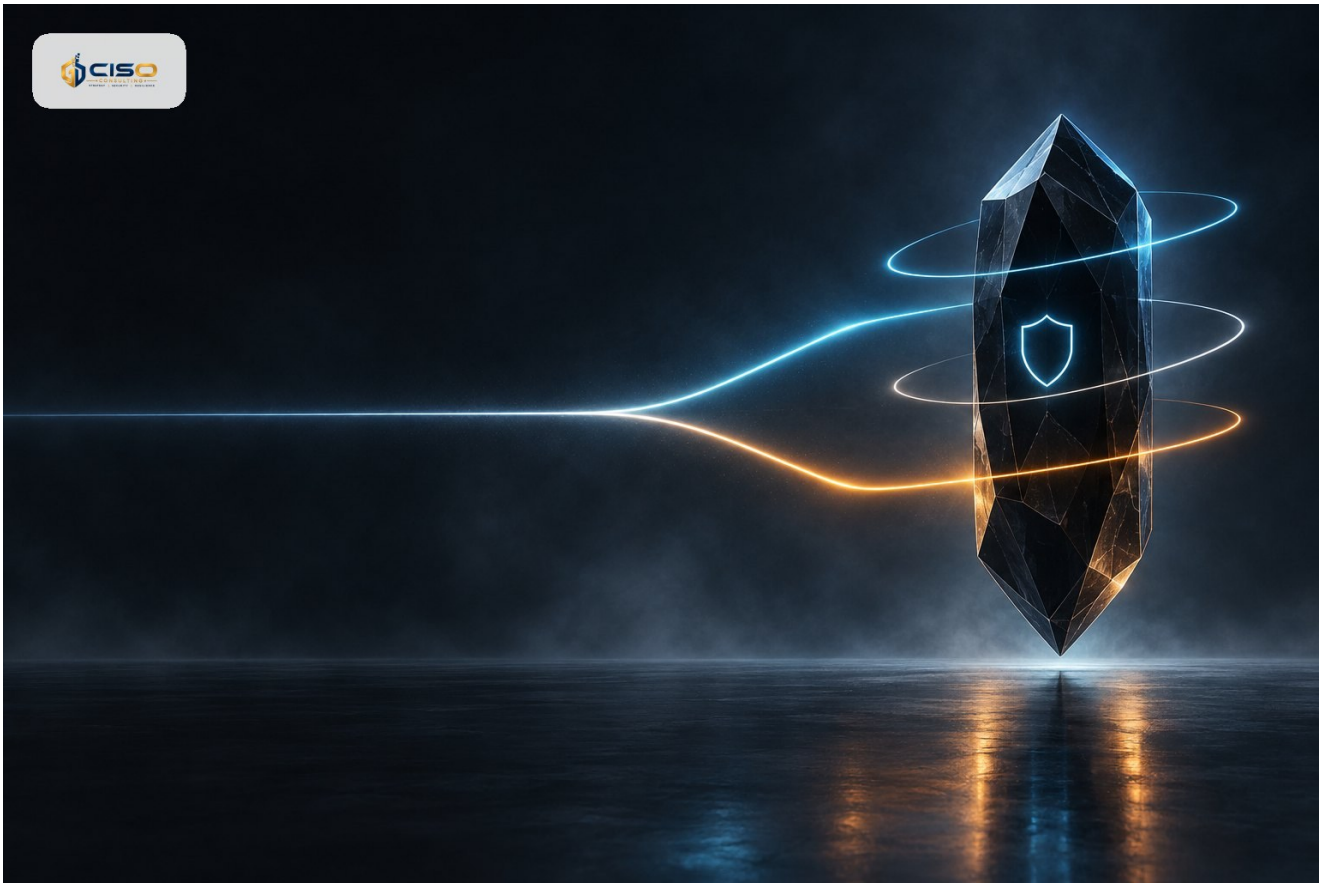
نماذج القرار بالذكاء الاصطناعي تصل إلى مراكز العمليات الأمنية: ما الذي ينبغي أن يزنه قادة الأمن



ظهرت خلال شهر فئة جديدة من نماذج القرار بالذكاء الاصطناعي من TypeSafe AI وOpenAI وCribl، وهي ذات صلة بمنصات مراكز العمليات الأمنية. المقتطف المتاح موجز وقليل التفاصيل.

- أطلقت TypeSafe AI نموذج Jev في 15 سبتمبر ووصفته بأنه نموذج «النظام الأول»، في إشارة إلى التفكير السريع الحدسي.
- أعلنت OpenAI عن واجهة Decisions API في DevDay وفتحت نسخة تجريبية عامة في 6 أكتوبر.
- نشرت Cribl النموذج cribl-decision، وهو مهايئ LoRA مفتوح يمكن تشغيله محليًا.
- يربط المقال هذه الفئة الجديدة من النماذج بتصميم منصات مراكز العمليات الأمنية المعتمدة على الذكاء الاصطناعي.
- لا يتناول المقتطف المتاح الأداء أو التسعير أو اختبارات الأمان.

ما الذي ورد في الخبر

وفق موقع The Hacker News، انتقلت فئة جديدة من نماذج الذكاء الاصطناعي من العدم إلى الانتشار الواسع خلال نحو شهر. فقد أطلقت TypeSafe AI نموذج Jev في 15 سبتمبر ووصفته بأنه نموذج «النظام الأول»، مستعيرة مصطلح كانمان للتفكير السريع الحدسي. وأعلنت OpenAI عن واجهة Decisions API في DevDay، وفُتحت نسخة تجريبية عامة في 6 أكتوبر. ونشرت Cribl النموذج cribl-decision، وهو مهايئ LoRA مفتوح يمكن للمنظمات تشغيله محليًا. ويذكر المقال جهات أخرى، لكن المقتطف مقطوع.

أهمية الخبر لقادة مراكز العمليات الأمنية

يربط المقال هذه النماذج بمنصات مراكز العمليات الأمنية المعتمدة على الذكاء الاصطناعي، حيث أصبح الفرز الآلي واتخاذ القرار ميزة تسويقية. ولا يقدم المقتطف مقاييس أداء أو ادعاءات دقة أو تفاصيل عن دمج النماذج في المنتجات، ولذلك لا ينبغي استخلاص أحكام عن الجودة أو المخاطر منه وحده.

وبالنسبة للجهات المنظمة، يتعلق السؤال العملي بالحوكمة أكثر من سرعة الاعتماد. فالنموذج الذي يتخذ قرارات بشأن التنبيهات أو يوصي بها يحتاج إلى مالك واضح واختبار ورقابة، خاصة عند المقارنة بين واجهة مستضافة ومهايئ يعمل محليًا، إذ يختلف التعامل مع البيانات بينهما.

التوجه المقترح

يُنصح بمتابعة هذا التطور. اقرؤوا المقال كاملاً ووثائق المزوّدين قبل أي تقييم، وأبقوا أي تجربة محدودة وخاضعة للإشراف وقابلة للتراجع.

ما يجب فعله الآن

1. اقرؤوا المقال الأصلي ووثائق المزوّدين كاملة قبل استخلاص أي استنتاج.
2. اسألوا مزوّدي منصات مراكز العمليات الأمنية هل يستخدمون نماذج قرار، وهل هي مستضافة أم تعمل محليًا.
3. تأكدوا من مكان معالجة بيانات التنبيهات والسجلات وتخزينها قبل تفعيل أي ميزة قرار بالذكاء الاصطناعي.
4. اشترطوا مراجعة بشرية لقرارات الفرز الآلية أثناء أي تجربة.
5. وثّقوا القرارات المدعومة بالذكاء الاصطناعي في سجل المخاطر وراجعوها وفق متطلبات الضوابط الأساسية للأمن السيبراني (NCA ECC) وإطار الأمن السيبراني للقطاع المالي (SAMA CSF).