الذكاء الاصطناعي يكشف فجوات قديمة في الكشف عن المخاطر ومعالجتها



ركزت النقاشات في Cyber Week 2026 على أن الذكاء الاصطناعي يقلّص الوقت المتاح لفرق الأمن للاستجابة، ويكشف نقاط ضعف في طريقة اكتشاف المخاطر ومعالجتها.

- تمحورت نقاشات Cyber Week 2026 حول أثر الذكاء الاصطناعي في عمليات الأمن.
- الذكاء الاصطناعي يقلّص الوقت المتاح لفرق الأمن للاستجابة للتهديدات.
- كما يكشف فجوات في كيفية اكتشاف المؤسسات للمخاطر ومعالجتها.
- المشكلات المطروحة قديمة عاشها قطاع الأمن لسنوات، وليست جديدة.

ما الذي نوقش

وفق ما نقلته Dark Reading عن Cyber Week 2026، دار جانب كبير من النقاش حول تغيّر إيقاع العمل الأمني

بفعل الذكاء الاصطناعي. والفكرة المحورية أن الوقت المتاح للفرق للاستجابة للتهديدات أصبح أقل من السابق.

وأشارت النقاشات نفسها إلى أن الذكاء الاصطناعي لا يصنع نقاط ضعف جديدة بقدر ما يكشف القائمة منها، أي الفجوات في طريقة اكتشاف المؤسسات للمخاطر وفي طريقة معالجتها.

أهمية ذلك للجهات المنظَّمة

المصدر موجز ولا يذكر أرقامًا أو حالات أو أدوات محددة. ومع ذلك فرسالته مفيدة لقادة المخاطر والالتزام: إذا كانت مهلة الاستجابة تضيق، فإن بطء الكشف والمعالجة أو تجزؤهما يصبح أوضح وأكثر كلفة.

وبالنسبة للمؤسسات في المملكة، فهي دعوة لاختبار مدى فاعلية عمليات المراقبة والفرز والمعالجة الحالية عمليًا، بدل الاكتفاء بوجود إجراءات موثقة.

استجابة متزنة

لا يصف المصدر حالة طارئة جديدة ولا يطلب إجراءً عاجلاً. ومن الخطوات المعقولة مراجعة هادئة لأداء الكشف والمعالجة، مع قياس صريح للزمن الذي تستغرقه كل مرحلة، ثم رفع النتائج عبر أطر الحوكمة والتقارير القائمة إلى الإدارة.

ما يجب فعله الآن

1. قياس الزمن الحالي من الكشف إلى الفرز إلى المعالجة في الحوادث والثغرات الأخيرة.
2. تحديد المراحل التي تعتمد على تسليم يدوي في الكشف أو المعالجة وإعطاؤها أولوية للتبسيط.
3. اختبار إجراءات الاستجابة للحوادث بتمرين مكتبي يفترض مهلة استجابة أقصر.
4. رفع النتائج والفجوات إلى الإدارة العليا عبر حوكمة المخاطر القائمة.