دراسة CREST: الذكاء الاصطناعي أصبح جزءًا معتادًا من اختبار الاختراق القائم على التهديدات



تُظهر دراسة CREST أن 81% من المزودين المشمولين يستخدمون الذكاء الاصطناعي في اختبار الاختراق القائم على التهديدات، بينما يظل التنفيذ الذاتي نادرًا، ويُتوقع تزايد متطلبات الإفصاح والموافقة.

- يستخدم 81% من 26 مزودًا شملتهم الدراسة الذكاء الاصطناعي في TLPT خارج نطاق التجريب، ويتوقع 65% أن يدعم 40% أو أكثر من المهام خلال 12 شهرًا.
- لا يسمح أي من مزودي TLPT الخاضعين للتنظيم الذين أجابوا (11 مزودًا) للذكاء الاصطناعي بتنفيذ الاختبار ذاتيًا.
- يرى 92% أن إرسال بيانات العميل إلى خدمات ذكاء اصطناعي خارجية أو سحابية يتطلب موافقة صريحة منه.
- يتوقع 85% زيادة متطلبات الشراء المتعلقة بالذكاء الاصطناعي، و81% زيادة طلبات الإفصاح عن

استخدامه.

نشرت CREST دراسة حول تأثير الذكاء الاصطناعي في اختبار الاختراق القائم على التهديدات (TLPT)، استندت إلى ردود 26 مزودًا وإلى طاولتين مستديرتين لخبراء القطاع، مع تركيز على الخدمات المالية.

أبرز النتائج

أصبح الذكاء الاصطناعي جزءًا من التنفيذ الفعلي، إذ يستخدمه 81% من المزودين المشمولين بما يتجاوز التجريب. وأكثر استخداماته شيوعًا إعداد التقارير والتقييم، يليه الاستطلاع والتحضير المبني على معلومات التهديد. ومن بين المزودين الذين يستخدمونه في محاكاة الجهات المهاجمة، أفاد 86% بتحسن الدقة والواقعية.

وتشير الدراسة إلى مخاطر أيضًا؛ فتحيّز النماذج وبيانات التدريب قد ينتج أنماطًا عامة تُضعف التمييز بين الجهات المهاجمة. أما انتحال الهوية بالذكاء الاصطناعي، كاستنساخ الصوت والفيديو الاصطناعي، فيتطلب مبررًا وتفويضًا وضمانات تتناسب مع الضرر المحتمل.

الضبط وحماية البيانات

التنفيذ الذاتي محدود؛ فلا يسمح أي من مزودي TLPT الخاضعين للتنظيم الذين أجابوا عن السؤال (11 مزودًا) للذكاء الاصطناعي بتنفيذ أنشطة الاختبار ذاتيًا. وصنّف 68% من المشاركين كلاًّ من النطاق والضبط التشغيلي، وبيانات العميل وسريتها، ضمن أبرز ثلاث مخاطر في التنفيذ.

وفي البيانات، يرى 92% أن إرسال معلومات العميل إلى خدمات ذكاء اصطناعي خارجية أو سحابية يستلزم موافقته الصريحة. ومن الاعتبارات: مواقع المعالجة والتخزين، والاحتفاظ بالبيانات، وممارسات تدريب النماذج، والمتعاقدون من الباطن، وصلاحيات الوصول. كما تلاحظ الدراسة أن خطوات الموافقة البشرية قد تبطئ الهجمات المحاكاة وتؤثر في الاستنتاجات حول الكشف والاستجابة، ولذلك يُنصح بتوثيق أي تغيير في ظروف الاختبار.

ما المتوقع

يتوقع المزودون استخدامًا أكبر لأدوات الهجوم المولّدة بالذكاء الاصطناعي، ويتوقع 85% منهم تشددًا أكبر في متطلبات الشراء المرتبطة به. وعلى الجهات التي تتعاقد على هذه الاختبارات أن تستعد لطرح أسئلة واضحة حول كيفية استخدامه وحوكمته.

ما يجب فعله الآن

1. اطلب من مزودي TLPT الإفصاح عن مواضع استخدام الذكاء الاصطناعي وكيفيته في أعمالكم، بما في ذلك أي خدمات خارجية أو سحابية.
2. اشترطوا موافقة كتابية صريحة قبل إرسال أي بيانات إلى خدمات ذكاء اصطناعي خارجية، وحدّدوا شروط التخزين والاحتفاظ وتدريب النماذج والمتعاقدين من الباطن.
3. ضعوا قواعد اشتباك تحدد ما إذا كان التنفيذ الذاتي للذكاء الاصطناعي مسموحًا، مع شروط إيقاف وسجلات للإجراءات الآلية والتدخلات البشرية.
4. اشترطوا التفويض والضمانات عند استخدام انتحال الهوية بالذكاء الاصطناعي في تمارين الهندسة

الاجتماعية.

5. أضيفوا بنودًا متعلقة بالذكاء الاصطناعي إلى عقود اختبار الاختراق، وراجعوا أثر تأخيرات الموافقة على استنتاجات الاختبار.