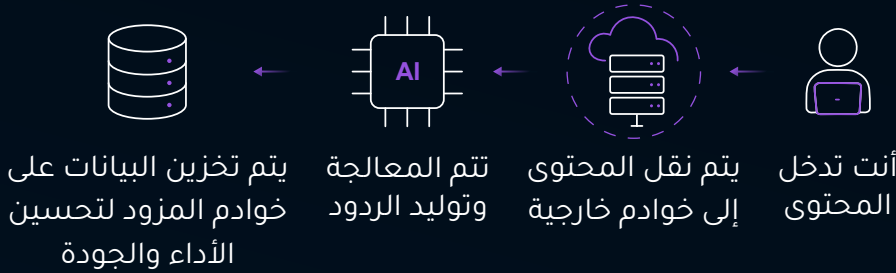


تسريب البيانات عبر الذكاء الاصطناعي

كيف تعمل أدوات الذكاء الاصطناعي مع البيانات؟



لذلك لا تبقى البيانات دائماً ضمن نطاق الاستخدام اللحظي، بل قد تتم معالجتها خارج سيطرة المؤسسة.

أصبحت أدوات الذكاء الاصطناعي جزءاً أساسياً من بيئة العمل، فهي تساعد في تسريع المهام وتنظيم الأفكار. لكن إدخال معلومات داخلية أو ملفات غير مخصصة للمشاركة في أدوات الذكاء الاصطناعي العامة قد يؤدي إلى تسريب البيانات وانتهائك الخصوصية.

مخاطر استخدام أدوات الذكاء الاصطناعي العامة في بيئة العمل

مشاركة مستندات غير مخصصة للنشر العام.

مخالفة سياسات أمن المعلومات والخصوصية.



تسريب البيانات الخاصة بالعمل من خلال رفع ملفات العمل الداخلية.



انتهاك الخصوصية.



كشف تفاصيل عن الأنظمة أو الإجراءات الداخلية.



قاعدة التحقق والبيانات عالية الحساسية

وتأكد من خلوها من **البيانات عالية الحساسية** التالية:

- ⊗ بيانات العملاء أو الموظفين
- ⊗ الأكواد البرمجية الداخلية
- ⊗ البيانات المالية والتشغيلية
- ⊗ كلمات المرور ومفاتيح الوصول
- ⊗ الخطط والاستراتيجيات غير المعلنة

قبل استخدام أي أداة ذكاء اصطناعي في العمل، يجب تطبيق **"قاعدة التحقق" اسأل نفسك:**

- ✓ هل هذه المعلومة مخصصة للاستخدام الداخلي فقط؟
- ✓ هل تم اعتماد الأداة رسمياً من جهة العمل؟
- ✓ هل يمكن مشاركة هذا المحتوى دون الإضرار بخصوصية المؤسسة؟

تهدف هذه القاعدة إلى منع مشاركة أي معلومات حساسة مع أدوات خارجية بشكل غير مقصود، حتى في حالات الاستخدام البسيط مثل التلخيص أو تحسين الصياغة.

هو استخدام أدوات الذكاء الاصطناعي داخل بيئة العمل دون اعتماد رسمي من المؤسسة أو إشراف من قسم تقنية المعلومات، مثل استخدام حسابات شخصية أو خدمات خارجية غير مصرح بها لإنجاز مهام وظيفية. خطورته تكمن في أنه يخلق تدفقاً غير مرئي للبيانات خارج إطار الحوكمة الأمنية، مما قد يؤدي إلى تسريب معلومات حساسة أو تخزينها في أنظمة لا تخضع لسياسات المؤسسة أو رقابتها.

ثقافة سيبرانية:



هل تعلم ما هو ال Shadow AI (الذكاء الاصطناعي الموازي)؟

الدرس؟



قامت الشركة بفرض قيود على استخدام أدوات الذكاء الاصطناعي العامة داخل بيئة العمل.



يمكنكم الاطلاع على تفاصيل الحادثة عبر مسح الكود

حادثة واقعية:



في عام 2023، سجلت شركة Samsung Electronics حوادث داخلية تتعلق باستخدام أدوات الذكاء الاصطناعي العامة مثل ChatGPT في بيئة العمل. قام بعض المهندسين بإدخال أكواد برمجية داخلية ومحتوى من اجتماعات عمل بهدف تحسين الكود أو تلخيص النصوص، لكن هذه البيانات تم إرسالها إلى منصات خارجية لمعالجتها، مما أدى إلى مخاوف أمنية تتعلق بخروج معلومات حساسة خارج بيئة المؤسسة.

تدابير سيبرانية عند استخدام أدوات الذكاء الاصطناعي في العمل

استخدام الأدوات المعتمدة من جهة العمل فقط.



التأكد من سياسة الخصوصية قبل استخدام أي أداة خارجية.



الإبلاغ عن أي مشاركة غير مقصودة لبيانات حساسة لفريق تقنية المعلومات.



استخدام الذكاء الاصطناعي للمهام العامة فقط مثل الصياغة، التلخيص، والترجمة غير الحساسة.



عدم إدخال أي بيانات داخلية أو معلومات يمكن ربطها بالمؤسسة أو تحديدها بشكل مباشر.



استبدال البيانات الحساسة بمعلومات عامة أو رمزية عند الحاجة.



الذكاء الاصطناعي أداة فعالة لزيادة الإنتاجية في العمل، غير أن الاستخدام غير الواعي قد يعرض بيانات العمل الحساسة لخطر التسريب.



استخدم الذكاء الاصطناعي بذكاء... ولا تدخل بيانات المؤسسة خارج بيئة العمل الآمنة.