الذكاء الاصطناعي الوكيل وتأثيره على الأمن السيبراني

م. أبرار يوسف الدخيل

يشهد مجال الحوسبة والأمن السيبراني في السنوات الأخيرة تحولًا كبيرًا مع ظهور ما يُعرف بالذكاء الاصطناعي (Agentic AI) الوكيل وهو جيل متقدم من أنظمة الذكاء الاصطناعي التي لا تكتفي بتحليل البيانات أو تقديم التوصيات ، بل تمتلك القدرة على اتخاذ قرارات وتنفيذ مهام بشكل مستقل داخل الأنظمة الرقمية .هذا النوع من الذكاء يمثل نقلة نوعية في طريقة عمل الأنظمة، حيث أصبح بإمكانه التفاعل مع بيئات متعددة، وربط أنظمة مختلفة، وتنفيذ أوامر دون تدخل بشري مباشر، مما يعزز الكفاءة والسرعة في العمليات، لكنه في المقابل يفتح الباب أمام تحديات أمنية جديدة ومعقدة.

إن دمج الذكاء الاصطناعي في الأنظمة الرقمية أدى إلى توسّع ما يُعرف بسطح الهجوم ،(Attack Surface) حيث أصبحت هناك نقاط ضعف إضافية يمكن استغلالها من قبل المهاجمين .فعندما يكون النظام قادرًا على تنفيذ أوامر حساسة بشكل تلقائي، فإن أي خلل في الإعدادات أو إساءة استخدام للصلاحيات قد يؤدي إلى اختراقات واسعة النطاق.

في المقابل، لم يعد المهاجمون يعتمدون فقط على الأساليب التقليدية، بل بدأوا باستخدام الذكاء الاصطناعي نفسه لتطوير هجمات أكثر تعقيدًا وفعالية، مثل رسائل التصيد الاحتيالي المتقنة والبرمجيات الخبيثة الذكية، مما يجعل اكتشافها أكثر صعوبة.

وعلى الجانب الآخر، يمثل الذكاء الاصطناعي نفسه أداة قوية لتعزيز الأمن السيبراني، حيث تستخدمه المؤسسات في الكشف المبكر عن التهديدات وتحليل البيانات بسرعة عالية، مما يساعد في تقليل زمن الاستجابة وتحسين دقة اكتشاف الهجمات.

ومن أهم الاتجاهات الحديثة تبني نموذج "الثقة الصفرية (Zero Trust) " الذي يعتمد على التحقق المستمر من ، جميع المستخدمين والأنظمة وعدم منح الثقة بشكل افتراضي، مما يعزز من مستوى الحماية خاصة في البيئات الرقمية المعقدة.

ورغم هذه المزايا، لا تزال هناك تحديات مثل نقص المهارات، وغياب المعايير التنظيمية، وزيادة استقلالية الأنظمة الذكية التي قد تؤدي إلى صعوبة التحكم الكامل فيها.

في الختام، يمثل الذكاء الاصطناعي الوكيل مستقبلًا واعدًا، لكنه يتطلب استراتيجيات أمنية متقدمة لتحقيق التوازن بين الابتكار والحماية.