

هشام عبد الرسول: الذكاء الاصطناعي والأمن السيبراني ركيزتان لاستدامة الأعمال في العصر الرقمي

قال المهندس هشام عبد الرسول، الرئيس التنفيذي لشركة راية لتكنولوجيا المعلومات، إن الاستثمار في الأمن السيبراني والذكاء الاصطناعي لم يعد خيارًا، بل ضرورة استراتيجية للشركات التي تسعى إلى البقاء والتطور في بيئة الأعمال المعاصرة، مشددًا على أن المؤسسات التي تدرك أهمية هذه التقنيات ستكون الأكثر قدرة على مواجهة تحديات المستقبل والتغلب عليها بكفاءة.

جاء ذلك على هامش مشاركة راية لتكنولوجيا المعلومات في فعاليات معرض ومؤتمر الأمن السيبراني وحماية المعلومات CAISEC 2025، الذي عقد نسخته الرابعة في القاهرة يومي 25 و26 مايو، حيث سلط الحدث الضوء على أحدث التطورات في مجال الأمن السيبراني والذكاء الاصطناعي.

وأضاف عبد الرسول في هذا السياق أن راية بصدد إنشاء قسم جديد مختص بحلول الذكاء الاصطناعي خلال النصف الثاني من العام لدعم الأعمال بالحلول ذات الصلة التي من شأنها دعم الخطط الاستراتيجية والتشغيلية. ومن المقرر أن تبدأ بالقطاع المالي لتوظيف حلول الذكاء الاصطناعي المتخصصة التي تستهدف بالأساس تعزيز الخدمات المستقبلية مع خطط لاستهداف مختلف القطاعات الحيوية الأخرى. وتُعد هذه الخطوة جزءًا من استراتيجية راية لتوسيع نطاق خدماتها وتقديم حلول تقنية متقدمة تلبي احتياجات الأسواق مع التركيز على الابتكار والاستدامة.

وتابع: "الذكاء الاصطناعي لم يعد مقتصرًا على تحسين العمليات التشغيلية، بل أصبح عاملاً جوهريًا في تعزيز استدامة الأعمال، حيث يساهم في تطوير أنظمة ذكية قادرة على التكيف مع التغيرات السريعة في السوق واتخاذ قرارات مبنية على تحليل دقيق للبيانات. ومن جهة أخرى، أصبح الأمن السيبراني حجر الأساس لحماية هذه الأنظمة وضمان استمرارية الأعمال في ظل المخاطر المتزايدة للهجمات الإلكترونية المصاحبة للتحول الرقمي".

يشار إلى أن الشركة استعرضت خلال مؤتمر CAISEC هذا العام أحدث حلولها المبتكرة لحماية المؤسسات وتعزيز التحول الرقمي، وذلك بالشراكة مع سيسكو، ومن بينها Cisco Hypershield الذي يعتمد على الذكاء الاصطناعي لرصد التهديدات السيبرانية وتحليلها بشكل استباقي، إضافةً إلى أدوات الذكاء الاصطناعي الخاصة بالأمن السيبراني بالاعتماد على الذكاء الاصطناعي التوليدي لتعزيز سرعة الاستجابة للهجمات. كما تستعرض راية حلول Cisco Duo لتأمين الهويات الرقمية عبر المصادقة متعددة العوامل MFA، إلى جانب تقنيات AI for Security التي تساعد المؤسسات على تحقيق أهدافها الأمنية بكفاءة وتقليل التعرض للمخاطر السيبرانية، مما يعزز قدرتها على التصدي للهجمات الإلكترونية وتأمين بياناتها الحيوية.