استخدام الذكاء الاصطناعي في أنظمة SIEM لتعزيز الأمن السيبراني

اعداد: م. الاء رضا

مع التزايد المستمر في تعقيد الهجمات السيبرانية وتنوعها، فإن الاعتماد على الأساليب التقليدية القائمة لم يعد كافيًا لمواجهة التهديدات الحديثة، مما أدى إلى دمج تقنيات الذكاء الاصطناعي كعامل أساسي في تطوير هذه أنظمة الأمن السيبراني منها SIEM.

إلا أن الحجم الهائل للبيانات وتنوعها جعل من الصعب تحليلها يدويًا أو عبر قواعد ثابتة وهنا يأتي دور الذكاء الاصطناعي حيث يتيح معالجة كميات ضخمة من البيانات بسرعة عالية، مع القدرة على التعلم المستمر من الأنماط والسلوكيات المختلفة داخل الشبكة.

حيث تقوم الأنظمة الحديثة ببناء نموذج للسلوك الطبيعي للمستخدمين والأجهزة، ثم الكشف عن أي انحراف قد يشير إلى نشاط ضار .هذا النهج يساعد في اكتشاف الهجمات غير المعروفة التي لا يمكن رصدها باستخدام التوقيعات التقليدية.

كما ساهم الذكاء الاصطناعي في تقليل مشكلة الإنذارات الكاذبة، والتي كانت تمثل عبئًا كبيرًا على فرق الأمن .الأنظمة الحديثة قادرة على تصفية التنبيهات غير المهمة والتركيز على التهديدات الحقيقية.

ومن أبرز التقنيات الحديثة المستخدمة في هذا المجال :التعلم العميق، التعلم غير الخاضع للإشراف، تحليل سلوك المستخدم والكيانات (UEBA) التحليل التنبؤي، والأتمتة والاستجابة الذكية (SOAR) .

كما تشير الاتجاهات الحديثة إلى استخدام الذكاء الاصطناعي التوليدي لدعم تحليل التهديدات وتعزيز الأمان بشكل استباقي.

ورغم هذه الفوائد، لا تزال هناك تحديات مثل جودة البيانات وصعوبة تفسير قرارات النماذج والمخاوف المتعلقة بالخصوصية .ومع ذلك، فإن مستقبل أنظمة الأمن السيبراني. الختام، فإن دمج الذكاء الاصطناعي في أنظمة لم يعد خيارًا، بل ضرورة لتعزيز الأمن ومواكبة التهديدات المتطورة .

المصادر

Exabeam – AI in Cybersecurity (2025)

Stellar Cyber – SIEM Trends (2026)

Hunters Security – Next-Gen SIEM (2025)

Bhatia, R. – Future of SIEM (2025)