مع الاعتماد المتزايد على التكنولوجيا الرقمية، تواجه سلاسل التوريد تحديات مستقبلية أكثر تعقيدًا، خاصة مع ظهور وتوسع على الرغم من الدور الكبير لهذه التقنيات في تحسين كفاءة .(AI) والذكاء الاصطناعي (IoT) الأنظمة الذكية مثل إنترنت الأشياء العمليات، فإنها تزيد من نقاط الضعف في الأنظمة وتجعلها أكثر عرضة للهجمات السيبرانية. أجهزة إنترنت الأشياء، التي تُستخدم لتتبع الشحنات ومراقبة المخزون، مما يجعلها هدفًا سهلاً للهجمات التي يمكن أن تعطل العمليات أو تسرب البيانات الحساسة.

يوفر الذكاء الاصطناعي فرصًا لتعزيز الأداء من خلال التحليل المتقدم والتنبؤ الدقيق، لكنه أيضًا يُستغل من قِبل المهاجمين السيبرانيين لتطوير هجمات أكثر تعقيدًا، مثل التصيد المتقدم أو اكتشاف نقاط الضعف بشكل أسرع. يشكل الاعتماد المتزايد على الحوسبة السحابية تحديًا إضافيًا، حيث إن أي خرق أمني في الأنظمة السحابية قد يؤدي إلى تعريض البيانات الهامة للخطر، مما يؤثر على جميع الأطراف المعنية في سلسلة التوريد. يشكل الأمن السيبراني للأطراف الثالثة تحديًا كبيرًا، إذ يعتمد نجاح سلسلة التوريد على تعاون مجموعة كبيرة من الموردين والشركاء الذين قد يكونون أقل تجهيزًا من الناحية الأمنية، ما يجعلهم نقاط دخول محتملة للهجمات. يجب على المؤسسات الاستثمار في استراتيجيات أمان شاملة تشمل تحديث الأنظمة، تعزيز التعاون بين الشركاء، وزيادة وعي الموظفين بأهمية الحماية السيبرانية لضمان استدامة وكفاءة سلاسل التوريد.