

إدارة الكفاءة والفعالية في العمليات الأمنية مع أتمتة مركز العمليات الأمنية

مركز العمليات الأمنية (SOC) هو كيان دائم التطور يتجه الآن نحو الأتمتة التي تعمل بالطاقة البشرية. يمكن لهذه الخطوة أن تعزز من عمليات اكتشاف التهديدات، وتسريع الاستجابة للحوادث، وربط الأحداث مع بعضها بكفاءة عالية، وبالتالي، تحسين عملية صنع القرار المتعلق بالعمليات الأمنية.

كيف يمكن للأتمتة أن تساعد في تسهيل العمليات الأمنية

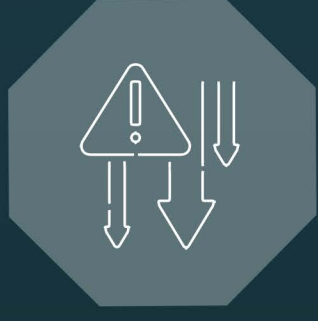
التنبؤ
بالتهديدات المستقبلية



فرز
تهديدات المستوى 1



تقليل
الإنذارات الخاطئة



ربط
سلوك المستخدم
بمؤشرات التهديد



الكشف
عن الهجمات
والتهديدات الأولية



من المؤسسات تستثمر في أتمتة مركز العمليات
الأمنية باستخدام استراتيجيات مختلفة

90%

مكنت الاستثمارات في الأتمتة الشركات من:



تعزيز إنتاجية
الموظفين



التعجيل بتصعيد
المسائل الحساسة



تحسين الكشف
عن التهديدات



تحسين متوسط
وقت الاستجابة



تعزيز ترتيب
أولويات الحوادث



عزل الأصول
المتضررة بسرعة أكبر

يعمل مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المتقدمة على تمكين المنشآت من الدمج بشكل فعال بين مجموعة من حلول الأمن السيبراني القابلة للتطوير، بما في ذلك إدارة المعلومات الأمنية والأحداث، والتحليلات الجنائية للشبكة، والاستجابة للحوادث، واستخبارات التهديدات، التي تعتبر ضرورية لأتمتة العمليات الأمنية بشكل عام.