# الدفاع السيبراني المستقبلي مع الاستجابة الاستباقية للحوادث

يمثل مشهد التهديد المتطور باستمرار حاجة ماسة للمُنشآت المستقبلية لتعزيز إطار مرن للاستجابة للحوادث السيبرانية. اليوم، يُعد البحث المُحكم عن التهديدات والتحليلات المتقدمة ومعالجة الحوادث أمراً بالغ الأهمية لمواجهة الهجمات السيبرانية الحديثة.

## الاستجابة للتهديدات وتحليل وقت الاحتواء

**%54**
من المُنشآت تستغرق أقل من ساعة واحدة لاحتواء التهديدات

**%33**
من المُنشآت تستغرق من ساعة واحدة إلى 12 ساعة لاحتواء التهديدات

**%13**
من المُنشآت تستغرق 12 ساعة أو أكثر لاحتواء التهديدات

## أكثر أنواع الحوادث انتشاراً


الهندسة الاجتماعية


الوصول غير المصرح به


حجب الخدمة


هجوم الشيفرات الخبيثة


فقدان البيانات أو سرقتها


الاستخدام غير الملائم للبيانات وعمليات الاحتيال

**%76**
من المُنشآت تتحول إلى أطراف ثالثة لإدارة عملية الاستجابة للحوادث الخاصة بها

## نهج شامل لإدارة حوادث الأمن السيبراني


**استعد** للتهديدات القادمة


**اكشف وحلّل** المخاطر السيبرانية


**احتو واقضِ على الضرر وتعافَ منه**


**أجرِ معالجة ما بعد الحادث** لمنع تكرار الحوادث

يمكن لمركز العمليات الأمنية (SOC) من شركة الإلكترونيات المُتقدّمة مساعدة المنشآت على تحديد مؤشرات الاختراقات الأمنية (IoCs) وأيضاً الانتهاكات الأمنية المحتملة بسرعة ودقة. ومن خلال المراقبة المتسقة للتهديدات، والربط الدقيق بين الأحداث، وتقييم نقاط الضعف، يمكن لمركز العمليات الأمنية (SOC) من شركة الإلكترونيات المُتقدّمة تسهيل الاستجابة في الوقت الفعلي للحوادث وحماية البنية التحتية الحسّاسة للمُنشأة.

SAMI
ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة