تعزيز المرونة السيبرانية وإدارة المعلومات الأمنية والأحداث (SIEM) من قبل مركز العمليات الأمنية (SOC)

لا غنى عن إدارة المعلومات الأمنية والأحداث لضمان أمن المعلومات على مستوى المُنشأة. يمكن للشركات تبسيط سير العمل الأمني وتشغيل أنظمة أمنية عالية الأداء من خلال تجهيز مراكز للعمليات الأمنية واتباع حلول قائمة على إدارة المعلومات الأمنية والأحداث.

كيف تساعد إدارة المعلومات الأمنية والأحداث الشركات على تحسين المرونة السيبرانية

- الكشف عن التهديدات وتصيدها
- التحليل السلوكي والجنائي
- مُراقبة المعلومات الأمنية المركزية وإدارة السجلات
- الاستجابة للحوادث
- التنسيق والاستجابة الآلية

تتمتع إدارة المعلومات الأمنية والأحداث بدور بالغ الأهمية في تمكين مراكز العمليات الأمنية الحديثة

%90*

الكشف الدقيق عن التهديدات

من الشركات تقيّم إدارة المعلومات الأمنية والأحداث لديها على أنها فعالة إلى فعالة للغاية في تزويد مركز العمليات الأمنية بالبيانات والتنبيهات والسياق والأدلة التي يحتاجها

%90*

أتمتة المهام

من عمل المحللين من المستوى الأول يمكن تشغيله آلياً باستخدام حلول إدارة المعلومات الأمنية والأحداث

%50*

تحسين الموارد

من وقت الفريق الذي يُستهلك في تحسين عمليات الكشف والاستجابة يمكن تقليله باستخدام الحلول الخاصة بإدارة المعلومات الأمنية والأحداث

*تقريباً

إدراكاً لأهمية إدارة المعلومات الأمنية والأحداث في تعزيز الوضع الأمني للمنشأة، يقدم مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة الحديث منهجية إدارة المعلومات الأمنية والأحداث كحل أمني أساسي.

كيف يضمن مركز العمليات الأمنية من شركة الإلكترونيات المُتقدّمة الأمن السيبراني من خلال منهجية إدارة المعلومات الأمنية والأحداث

- دعم إدارة السجلات
- أتمتة إجراءات الاستجابة
- تحديد اتصالات القيادة والتحكم
- تحليل الأحداث والحوادث الأمنية في الوقت الفعلي

SAMI ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة