تحسين دورة حياة استخبارات التهديدات مع موردي الخدمات الأمنية المُدارة

اليوم، تتعامل المُنشآت مع الملايين من مؤشرات التهديد، ممّا يجعل من الصعب قياس القيمة المُستفادة من إطار عمل استخبارات التهديدات الخاص بها. وقد عزّز ذلك الحاجة إلى منصات استخبارات التهديدات المؤتمتة المُدارة من قبل موردي الخدمات الأمنية. يمكن أن تساعد هذه المنصات الفرق الأمنية في الحصول على تفاصيل قابلة للتنفيذ على المناطق التي تتعرض للهجوم، ودفع الاستخبارات الصحيحة عبر مُنشآتهم بأكملها، والتصرف بشكل أسرع في مواجهة التهديدات المُحتملة.

يُمكن للمُنشآت بسهولة أن تستعين بالمصادر الخارجية لاستخبارات التهديدات لتعزيز عملياتها الأمنية المستقبلية.

%68 من المُنشآت تستعين بموجزات التهديدات المُقدّمة من قبل موزّدي الخدمات الأمنية العامة

كيف يعمل موردي الخدمات الأمنية المُدارة على تحسين دورة حياة استخبارات التهديدات

الأتمتة	التعاون	التواصل
نشر خرائط التهديدات ومعلومات الحوادث تلقائياً.	جمع المعلومات من مصادر متعددة، مثل الموجزات مفتوحة المصدر وموردي المعلومات.	إعداد تقارير تحليلية مفصلة لمرحلة ما بعد الأحداث.
كيفية المساعدة		
توسيع نطاق التحقيق، والتعرف بسرعة على أنماط التهديد/الهجوم ذات الصلة، وتطوير الروابط بين مختلف الجهات الفاعلة المهددة.	تطوير معلومات التهديد بشكل أفضل باستخدام البيانات الأولية، وتوسيع الوصول إلى المحللين الأمنيين ذوي الخبرة، والعمل بحسم ضد نقاط الضعف الأمني الحرجة.	تلخيص الحوادث بكفاءة للفِرق القيادية من أجل توجيه القرارات عالية المستوى الخاصة بالعمل واتخاذ إجراءات للتخفيف من الأضرار المستقبلية.

المنهجية التي تتبعها شركة الإلكترونيات المُتقدّمة لإدارة استخبارات التهديدات

جمع البيانات	• معلومات مفتوحة المصدر	• موجزات المصادر الخارجية التي تم التحقق منها	• تنبيهات الحوادث الداخلية من داخل المُنشأة
المعالجة	• التصنيف	• نمذجة البيانات	• إثراء المؤشرات وإعادة البيانات إلى حالتها الطبيعية
التحليل	• الربط بين المؤشر والحادث	• التصور التفصيلي	• ترتيب أولويات التنبيه الآلي
المشاركة	• منصة استخبارات التهديدات (مدمجة مع إدارة المعلومات الأمنية والأحداث (SIEM) ونظام الكشف عن نقطة النهاية والاستجابة لها (EDR))		

SAMI ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة