مركز عمليات الأمن السيبراني

الملخص

مركز عمليات الأمن السيبراني التابع لشركة الإلكترونيات المُتقدّمة والمتواجد داخل المقر الرئيسي للشركة في مدينة الرياض قادر على مراقبة واكتشاف وعزل التهديدات المُتعلّقة بالأمن السيبراني وإدارة المنتجات الأمنية للمُنشأة وأجهزة الشبكة والخوادم وأنظمة الأمان ومركز بيانات تقنية المعلومات. تتوافق الخدمات المُقدّمة من قِبَل مركز عمليات الأمن السيبراني (SOC) مع تعليمات وأنظمة الهيئة الوطنية للأمن السيبراني السعودية.

تقدم شركة الإلكترونيات المُتقدّمة نماذج وطرق عمل متعددة للخدمات مُصمّمة خصيصاً للتناسب مع احتياج العملاء. تستخدم النماذج العاملة خارج الموقع (عن بعد) قناة اتصال آمنة بين مركز عمليات الأمن السيبراني وموقع العميل. كما يمكن أن تكون منصة إدارة المعلومات الأمنية والأحداث (SIEM) في الموقع أو خارج الموقع حسب الحاجة.

إن الفريق العامل في مركز عمليات الأمن السيبراني في شركة الإلكترونيات المُتقدّمة هو فريق سعودي بالكامل وتمتع كوادره المختلفة بخبرات واعتمادات مُتقدّمة في التعامل مع التهديدات الأمنية ولديهم المهارات اللازمة كخبراء في العمل على الحلول الرائدة في إدارة المعلومات الأمنية والأحداث (SIEM) مثل حلول LogRhythm وQRadarg وRSAg وSplunkg وArcSightg. حيث يتم تدريب محللي مركز عمليات الأمن السيبراني لدينا على العمل مع حلول الأمن السيبراني المتقدمة هذه لتحقيق وتنفيذ ما نعرضه أدناه

الفوائد

- لا حاجة لتوظيف وإدارة وتدريب موظفين مختصين
- الالتزام باتفاقيات مستوى الخدمة (SLA) من أجل الحفاظ على رضا العملاء
- تتميز بالمرونة والقابلية العالية للتكيف
- استخدم موارد مكتب المُساندة عند الحاجة
- السماح للمُنشآت بالتركيز على نقاط قوتها وأعمالها الجوهرية
- تمكين الاستفادة من التكلفة المدفوعة عن طريق (المُشاركة في الموارد؛ نقل العمليات إلى الخارج)
- تسهيل تحمل المسؤوليات
- الشراكة القوية مع شركة الإلكترونيات المُتقدّمة تعني دعماً قوياً من الموردين

مركز عمليات الأمن السيبراني

AEC
A SAMI COMPANY

الحلول التي تقدمها شركة الإلكترونيات المُتقدّمة

الحوكمة

- إنشاء ومراجعة دليل العمل في مركز عمليات الأمن السيبراني (السياسات والإجراءات)
- التقييم والمعالجة

تحليل ومراقبة سجلات الأحداث

- المراقبة على مدار الساعة وطوال أيام السنة للتهديدات المحتملة وحركة مرور البيانات داخل الشبكة بالكامل ونقاط النهاية والسجلات والأحداث السيبرانيه
- إدارة مُتقدّمة للسجلات والثغرات الأمنية
- إدارة سير العمل وتذاكر الحوادث الأمنية السيبرانيه

إدارة منصة المعلومات الأمنية والأحداث (SIEM)

- الإدارة والإشراف على حلول المعلومات الأمنية وإدارة الأحداث (SIEM)
- تحديث وضبط دوري ومستمر لحالات الاستخدام

المعايير وإصدار التقارير

- تعريف وضبط مؤشرات أداء رئيسية (KPIs) ومجالات نتائج رئيسية (KRAs) مُحدّدة بدقّة
- سهولة الإعداد واستخدام ميزات البحث والتنبيه
- تقارير ولوحات معلومات قابلة لتعديلها حسب الحاجة

التحليل الجنائي الرقمي والاستجابة للأحداث

- تحليل الأسباب الجذرية للأحداث (RCA)
- حلول استعادة البيانات وتحليلها
- تحليل البرامج الضارة لفهم سلوك ملف معين أو عنوان إنترنت (URL) مشبوه والغرض من وجوده

استخبارات التهديدات

- نحديد درجة التهديد وتحديد الأولوية للتأكد من أن استخبارات التهديدات الخاصة بالمُنشأة ذات صلة بالحدث
- القيام بتجميع بيانات التهديد من مصادر متعددة وربطها وتحليلها في الوقت الفعلي لدعم الإجراءات الدفاعية
- اصطياد التهديدات وتحليلها بشكل مستمر

التدريب والشهادات

- تدريب محلل معتمد (CSA) ل مركز عمليات الأمن السيبراني (SOC)
- شهادات الأمن السيبراني
- التدريب على إدارة المعلومات والأحداث الأمنية (SIEM) - خاص بالموردين
- التدريب أثناء العمل (OJT)