SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

توافق أدوار الأمن السيبراني المؤسسية

مع مركز عمليات الأمن السيبراني كخدمة (SOCaaS)

جدول المحتويات

الملخص التنفيذي

تزايدت شدة وتواتر الهجمات الإلكترونية بشكل مطرد على المستوى العالمي. حيث تكتمل هذه الزيادة بظهور جهات تهديد جديدة باستمرار، وأيضاً بتطور هجمات البرامج الضارة، وزيادة التعاون بين مجرمي الإنترنت [13]. علاوة على ذلك، فلقد وسعت شبكات المُنشآت الموزعة بشكل كبير من مساحات الهجوم، ممّا خلق فرصاً جديدة لمجرمي الإنترنت لتطوير تكتيكات وتقنيات وإجراءات جديدة. وبالتالي، تتجه المُنشآت المهتمة بالأمن نحو التقنيات الناشئة والخدمات التي من شأنها تعزيز الأمن السيبراني من أجل ضمان مستوىً أمني أعلى يشمل جميع جوانب المُنشأة.

وفي هذا السياق، اكتسبت الاستعانة الخارجية بمراكز عمليات الأمن السيبراني كخدمة (SOCaaS) من قبل مقدمي الخدمات الأمنية أهمية كبرى [12]. حيث يحظى مقدمو خدمات العمليات الأمنية المُدارة (MSSPs) بموظفين أكفاء لدعم الفرق الداخلية لأمن تقنية المعلومات من أجل الكشف الاستباقي واحتواء التهديدات الموجودة في الوضع الأمني للمؤسسة [4]. كما يوفر مركز عمليات الأمن السيبراني كخدمة أيضاً الحماية من التهديدات السيبرانية المستمرة والهجمات السيبرانية المتقدمة من خلال المراقبة الآنيّة والكشف والتحليل المتعمق للتنبيهات الأمنية [1].

تعمل شركة الإلكترونيات المُتقدّمة على تمكين المُنشآت من تعزيز مرونتها السيبرانية عبر مركزها لعمليات الأمن فبالتعاون مع مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة، يمكن للمُنشآت .السيبراني كخدمة تطوير بنية أمنية سيبرانية موثوقة تكون مؤهلة للتعامل مع الهجمات السيبرانية المُتقدّمة التي تحدث هذه الأيام. حيث تساعد شركة الإلكترونيات المُتقدّمة هذه المُنشآت على تحسين نطاق قدراتها الأمنية الرئيسية وتوسيعها مثل النطاقات الخاصة بالاستجابة للحوادث، وجمع المعلومات اللازمة حول التهديدات، وفرز التهديدات واصطيادها، وآلية تحديد الوصول، واختبار الاختراق، والتحليل الجنائي الرقمي، ومحاكاة عمليات الاختراق. علاوة على ذلك، فإن المساعدة الفورية من قبل موظفي الأمن السيبراني ذوي الخبرة في شركة الإلكترونيات المُتقدّمة تمكّن الفرق الداخلية لأمن تقنية المعلومات في المُنشآت من الإشراف على التنبيهات الأمنية وإدارتها. وبالتالي، مع تسخير هذه الإمكانيات المؤهلة والعمليات والتقنيات اللازمة، تمكّن خدمات الأمن السيبراني التي تقدِّمها شركة الإلكترونيات المُتقدّمة مُنشآت الجيل التالي من التركيز على استمرارية سير الأعمال، بالتزامن مع تعزيز وضعها الأمني.

مركز عمليات الأمن السيبراني كخدمة:
الدعامة الأساسية للممارسات الأمنية الحديثة

برز مركز عمليات الأمن السيبراني كخدمة (SOCaaS) كبوابة لإدارة المعلومات الأمنية والأحداث ومراقبة الامتثال للكيانات الحكومية والمُنشآت التجارية على حدٍ سواء التي تتطلع إلى تطبيق أنظمة دفاع سيبرانية متميزة. حيث يضيف موفِّرو خدمات العمليات الأمنية المُدارة ممن يقدمون مركز عمليات الأمن السيبراني كخدمة باستمرار خدمات جديدة لحل مشاكل تحديات الأعمال والمتطلبات المعقدة والأقسام المرتبطة بتطبيق مركز عمليات الأمن السيبراني كخدمة . [1]

أهم أسباب اختيار مركز عمليات الأمن السيبراني كخدمة للمراقبة الأمنية وضمان الامتثال

تخفيض التكاليف والإدارة المتعلقة باحتياجات موظفي الأمن السيبراني [4]

الكشف الاستباقي عن أماكن الهجوم المُحتمَلة [4]

تحسين البُنى التحتية الحالية لإدارة التهديدات [3]

المشاكل الحالية التي تعاني منها فرق الأمن السيبراني الداخلية

6+

عدد الأدوات التي تستخدمها فرق تقنية المعلومات ممّا يؤدي إلى الإجهاد التنبيهي

[5]

3M

أدوار أمنية شاغرة، مما يؤدي إلى نقص عالمي في مهارات الأمن السيبراني

[5]

%88

المؤسسات التي تبلغ عن تحديات في إيجاد المواهب وتوظيفها وإيجاد المهارات عالية المستوى

[6]

في ضوء هذه التحديات، تحتاج ممارسات الأمن السيبراني إلى التطور والتحسين والابتكار بشكل مستمر، من أجل مواجهة الطبيعة المتطورة للهجمات السيبرانية الحديثة. وهنا تبرز شركة الإلكترونيات المُتقدّمة كأحد أهم موفِّري خدمات الأمن السيبراني المُدارة (MSSP) في المملكة العربية السعودية والتي لديها ما يلزم من الخبرة لتوفير أحدث خدمات وحلول الأمن السيبراني للمُنشآت الرائدة.

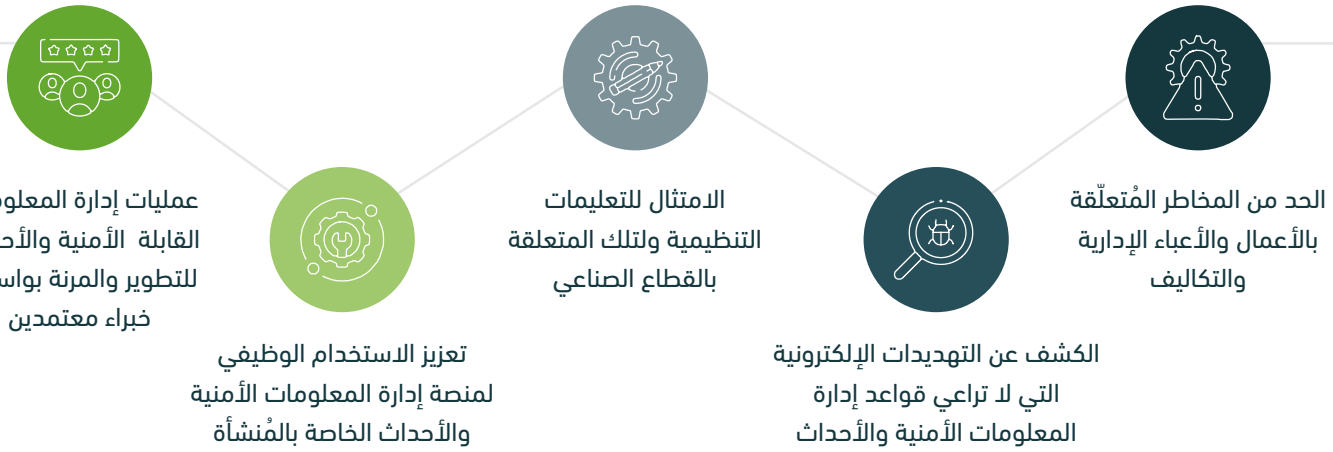
إن مركز عمليات الأمن السيبراني كخدمة يخلق بيئة أمنية شاملة من خلال التغلب على قيود إدارة المعلومات الأمنية والأحداث

لقد شقت العديد من التقنيات المتقدمة لمُراقبة وضمان الامتثال الأمني، مثل تقنية إدارة المعلومات الأمنية والأحداث (SIEM) طريقها عبر حلبة الأمن السيبراني. حيث تستخدم إدارة المعلومات الأمنية والأحداث (SIEM) طريقها عبر حلبة الأمن السيبراني. حيث تستخدم إدارة المعلومات الأمنية والأحداث. [8]

ومع ذلك، فإن إدارة المعلومات الأمنية والأحداث (SIEM) ليست كافية بحد ذاتها للتعامل مع الطبيعة الغريبة والمتطورة للهجمات في الوقت الحاضر. فبينما تستخدم إدارة المعلومات الأمنية والأحداث (SIEM) تقنيات متقدمة لاحتواء الهجمات السيبرانية، تتطلب المُنشآت الحديثة أيضاً وجود خبراء أمنيين وتنفيذ عمليات قابلة للتكرار لإعادة ضبط الوضع الأمني وتحسين قدراتها في الاستجابة للحوادث. [8]

مركز عمليات الأمن السيبراني كخدمة (SOCaaS): التغلب على قيود إدارة المعلومات الأمنية والأحداث (SIEM) [3]

يستفيد مركز عمليات الأمن السيبراني كخدمة من الإمكانات الأساسية التي تقدمها إدارة المعلومات الأمنية والأحداث من أجل دمجها مع استخبارات التهديدات والتحليلات المتقدمة للكشف عن الهجمات السيبرانية. حيث يساعد مركز عمليات الأمن السيبراني كخدمة في تخصيص منصة إدارة المعلومات الأمنية والأحداث وفقاً للاحتياجات المحددة لكل عميل، مما يُسهّل من دمج التقنيات الأمنية للمُنشأة.



تزايد أهمية خدمات العمليات الأمنية المُدارة (SecOps)

أهم أسباب استخدام خدمات العمليات الأمنية المُدارة * [2]

%52
تحسين قدرة موزّدي الخدمات على تقديم خدمات العمليات الأمنية المُدارة

%55
إعادة توجيه جهود العاملين في قطاع الأمن السيبراني نحو أهداف أكثر استراتيجية

%40
جني المزايا المتعلقة بانخفاض التكلفة

%42
التغلب على نقص الخبرة لفرق الأمن السيبراني الداخلية في العمليات الأمنية

%49
تعزيز إمكانات فريق مركز العمليات الأمنية

*كما ذكر المتخصصون في تقنية المعلومات والأمن السيبراني من مؤسسات القطاعين الخاص والعام

الاستعانة بمصادر خارجية للحلول الأمنية: ضرورة مُلِحّة للمُنشآت الحديثة

يعمل موفِّرو الخدمات الأمنية المُدارة على التعجيل بتحديث خدماتهم الخاصة بـمركز عمليات الأمن السيبراني كخدمة من أجل تدعيم البنية التحتية الأمنية، وتبسيط استخدام البيانات، وتوفير التوجيهات الأمنية العالمية، والقضاء على مختلف أشكال التهديدات الأمنية. لذلك، وكجزء من العروض التي يقدمها مركز عمليات الأمن السيبراني كخدمة ، يحتاج موفِّرو الخدمات الأمنية المُدارة إلى توفير منصات مرنة تستوعب تعدد المستفيدين، بالإضافة إلى حلول قابلة للتطوير، وليس مجرد مجموعة من المنتجات الأمنية. [14]

العوامل المساهمة في اعتماد مركز عمليات الأمن السيبراني كخدمة

الحاجة إلى حماية الأنظمة المادية السيبرانية

بحلول عام 2023 ، ستعيد 75% من المُنشآت هيكلة إدارة المخاطر وحوكمة الأمن السيبراني لمعالجة الأنظمة المادية السيبرانية الجديدة (CPS) وجعلها متوائمة ومتوافقة مع تقنية المعلومات والتقنيات التشغيلية وإنترنت الأشياء (IoT) والاحتياجات المادية للأمن السيبراني. [7]

الحاجة إلى احتواء التهديدات السيبرانية من الجيل التالي

بحلول عام 2025 ، ستستخدم 50% من المُنشآت الخدمات المُدارة لكشف التهديدات والاستجابة لها (MDR)، وذلك لمراقبة التهديدات السيبرانية والكشف عنها وتفعيل وظائف الاستجابة التي توفر قدرات خاصة باحتواء التهديدات. [8]

الحاجة إلى مواهب متميزة في مجال الأمن السيبراني

بحلول عام 2025 ، يمكن أن يتسبب النقص في عدد الكوادر المؤهلة والموهوبة في مجال الأمن السيبراني في أكثر من نصف الحوادث السيبرانية الكبيرة. [15]

ستعمل هذه العوامل دائماً على استخدام واسع لما يوفره موِردو الخدمات الأمنية المُدارة، وهذا ما يدفع بهؤلاء الموردين إلى السعي باتجاه انشاء مراكز عمليات الأمن السيبراني كخدمة من أجل الحوكمة الأمنية والتحكم بالتهديدات.

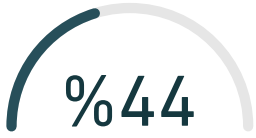
موفِّري الخدمات الأمنية المُدارة يكتسبون قوة دافعة

عالمياً

على مستوى دول مجلس التعاون الخليجي

على مستوى المملكة العربية السعودية

من المُنشآت تجد أن خدمة التحليلات الجنائية الرقمية المُقدّمة من خلال مركز العمليات الأمنية مفيدة من أجل فهم بيئة التهديد السيبراني الخارجي. [9]



من المُنشآت العاملة داخل الدول الأعضاء في مجلس التعاون الخليجي لديها مراكز للعمليات الأمنية تديرها أطراف ثالثة. [11]

تُنفق المملكة على الخدمات الأمنية المُدارة ما نسبته 23% من إجمالي الإنفاق الأمني. [10]

بنية مركز عمليات الأمن السيبراني كخدمة التي تُقدّمها شركة الإلكترونيات المُتقدّمة للمُنشآت

مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة هو بنية مُخصّصة من مركز العمليات الأمنية التي يمكن تطبيقها على مختلف الأنشطة التجارية والحكومية والصناعية لتعزيز عمليات الأمن السيبراني وترقيتها. تتيح هذه الخدمة القابلة للنشر السريع للمُنشآت العمل على إنشاء بيئة متجانسة وموثوقة ومرنة للبحث عن التهديدات وكشفها ومراقبتها، وبالتالي صنع مساراتها الخاصة لبناء المرونة السيبرانية على مستوى المُنشأة.

مركز عمليات الأمن السيبراني كخدمة

المراقبة الأمنية والاستجابة للأحداث سواءً بشكل كلي أو جزئي مستعان بها خارجياً من أحد موفّري الخدمات الأمنية المُدارة

الركائز الأساسية

أشخاص	العمليات	التقنية
↓↓	↓↓	↓↓
التحقيق في التهديدات	إصلاح الثغرات الأمنية	تطبيق التقنيات

المكونات الأساسية

ال‌تحليل الخاص بإدارة المعلومات الأمنية والأحداث	مجموعات القواعد	دفاعات القطاعات المحيطة
• محللو الأمن السيبراني	• مؤشرات التسوية (IOC)	• مراقبة الأصول
• معلومات عن الحوادث	• موجزات الاستخبارات السريعة	• تسجيل الأحداث
• تقييم البيئة الأمنية الخاصة بالعملاء	• سير عمل إدارة الحوادث	• أمن البيانات

مزايا الخدمات المُدارة

النشر - إدارة المنصات - الكشف عن التهديدات السيبرانية تقديم التقارير حول الامتثال - حالات الاستخدام المخصصة - لوحات المعلومات – الأدلة الخاصة بتصعيد الحوادث عند حدوثها

المستخدمون النهائيون الرئيسيون

الهيئات والمُنشآت الحكومية	المُنشآت التجارية	المُنشآت الرائدة في مجال الصناعة

حلول شركة الإلكترونيات المُتقدّمة

اختبار الاختراق، الأمن السحابي، الخدمات المُدارة للأمن السيبراني، إدارة المعلومات الأمنية والأحداث، إدارة السجلات، آلية تحديد الوصول، التحليل الجنائي للشبكة، الاستجابة للحوادث

حلول شركة الإلكترونيات المُتقدّمة (من شركائها المعتمدين)

أمن التطبيقات، نمذجة الشبكة، استخبارات التهديد، أمن الشبكة، أمن المضيف، النطاق السيبراني، التحليلات الجنائية للمضيف، التحليلات الجنائية للأجهزة المحمولة، إدارة الهوية والامتيازات

شركة الإلكترونيات المُتقدّمة تعجّل من مسار تعزيز المرونة السيبرانية

يستخدم مركز عمليات الأمن السيبراني كخدمة مزيجاً من الأشخاص والعمليات والتقنيات لإدارة المعلومات الأمنية المركز في تحليل التهديدات، ورؤية مناطق الهجوم، ويُقدّم الاستجابة القابلة والأحداث في المُنشآت. لذلك، يُبدع هذا[9] أو لمركز العمليات الأمنية الذي تم للتنفيذ في الحوادث الأمنية.[9] يمكن لمركز عمليات الأمن السيبراني كخدمة الاستعانة به من الخارج المساعدة في أداء الوظائف والأدوار الأمنية الرائدة لفرق الأمن السيبراني. علاوة على ذلك، يساعد مركز العمليات الأمنية الذي تم الاستعانة به من الخارج فرق الأمن السيبراني الداخلية من خلال مشاركة عبء الكشف المستمر عن التهديدات والتصيد والفرز – وهو يُمثل تحدياً مستمراً تواجهه مراكز العمليات الأمنية الداخلية.

اليوم، تعرب الشركات عن اهتمام أكبر بالاستعانة بقدرات مراكز العمليات الأمنية الرئيسية التي يتم الاستعانة بها من الخارج لتمكين محللي مركز العمليات الأمنية لديها من إدارة الهجمات الإلكترونية والاستجابة لها بشكل أفضل.[16]

قدرات مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة من الجيل التالي*

اختبار الاختراق

تقدم شركة الإلكترونيات المُتقدّمة اختباراً تجريبياً مُحكماً يتكون من تقييم نقاط الضعف الأمني واختبار البرمجيات والمسح الأمني للشبكة بشكل عام. حيث يعمل فريق متخصص من الخبراء أيضاً على تطوير وتنفيذ أنشطة اختبار الاختراق المخصصة تلبية لاحتياجات العملاء المعينة.

إدارة المعلومات الأمنية والأحداث (SIEM)

يمكن لإدارة المعلومات الأمنية والأحداث في شركة الإلكترونيات المُتقدّمة أن تجمع المعلومات من أجهزة الأمن والشبكات وقواعد البيانات وسجلات التطبيقات بكفاءة وتحللها وتعرضها، مع توفير إمكانات آلية تحديد الوصول. يمكنها أيضاً تحديد اتصالات القيادة والتحكم (C2) بشكل فعّال.

التحليلات الجنائية للشبكة

توفر التحليلات الجنائية للشبكة التي يغطيها مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة قدرات استقصائية مثل رصد عينات من البرمجيات الضارة وتحديد محاولات اختراق البيانات وتقييم عمليات استغلال الشبكة.

آلية تحديد الوصول

تفحص البيئة المعزولة لإمكانية آلية تحديد الوصول التابعة لشركة الإلكترونيات المُتقدّمة بدقة سلوك الملفات وعناوين الويب وتقدّم التقارير عن نتائج التحليل بسهولة. وباستخدام هذه الآلية، يمكن تحليل عينات البرمجيات الضارة بأمان وتنفيذها لوضع خطط الاستجابة للحوادث المستقبلية بشكل أفضل.

استخبارات التهديدات

إن لدى موظفي الأمن السيبراني في شركة الإلكترونيات المُتقدّمة القدرات والخبرات المحلية العالية، وهم متخصصون في جمع المنظمات العاملة في دعم استخبارات التهديدات القابلة للتنفيذ وتوجيههم باتجاه مواجهة الأنشطة الخطيرة لمجرمي الإنترنت.

الاستجابة للحوادث (IR)

رفع طلبات بناءً على تنبيهات مهام توفر استراتيجيات الاستجابة للحوادث في شركة الإلكترونيات المُتقدّمة أمنية (بواسطة النظام أو حالات الاستخدام المصممة خصيصاً للمُنشأة) لبدء التحقيق في هذه التنبيهات في الوقت المناسب واتخاذ ما يلزم من إجراءات ضد الانتهاكات التي تم التحقق منها.

*القائمة لا تشمل العروض التي يقدمها مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة

الأشخاص والعمليات والتقنيات:
جوهر مركز عمليات الأمن السيبراني
كخدمة من شركة الإلكترونيات المُتقدّمة

من خلال تسخير القوة التي يتمتع بها خبراء الأمن السيبراني المخضرمين والعمليات الاستباقية والتقنيات الحدودية، تساعد شركة الإلكترونيات المُتقدّمة المُنشآت على تطوير استراتيجيات فعالة لإدارة الأمن السيبراني الشاملة. تم تصميم مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة لتمكين ودعم المُنشآت في معالجة التعقيدات المترتبة على إدارة ورصد التنبيهات الأمنية على مدار الساعة.

سمات مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة

- بنية قابلة للتطوير بقدرة تحليلية قوية
- بنية تم اختبارها مع تاريخ حافل بعمليات النشر الناجحة
- يُسهل الاستجابة للحوادث بكفاءة وسرعة وفي الوقت المناسب
- يجمع عقوداً من الخبرة في إدارة الأمن السيبراني

المزايا التي تعود على المُنشآت المُستفيدة من مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة

- رؤية أشمل وأكبر للوضع الأمني العام
- برامج لإدارة المعلومات الأمنية مُصمّمة خصيصاً لاحتياجات المُنشأة
- توفير شامل للوقت والجهد والنفقات الخاصة بمركز العمليات الأمنية التابع للمُنشأة
- تعزيز القدرة على الكشف عن الحوادث السيبرانية، والاستجابة لها، وأيضاً، التعافي منها

يمكّن مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة المُنشآت من تحسين قدراتها الأمنية الحالية. يتحقق ذلك من خلال الإشراف الشامل على جميع أنواع الحوادث الأمنية مع تقليص حالات الإنذارات الخاطئة إلى ما يقرُب من الصفر. علاوة على ذلك، تساعد شركة الإلكترونيات المُتقدّمة المُنشآت على الاستفادة من الإمكانات الأصلية لإدارة المعلومات الأمنية والأحداث (SIEM) لديها لتسريع اكتشاف التنبيهات الأمنية وتقليل الوقت المستغرق لاحتواء الانتهاكات الأمنية.

الخاتمة

لقد عزز مشهد التهديد السيبراني المتزايد باستمرار الحاجة إلى إدارة استباقية للأمن السيبراني. حيث أن تزايد الابتكار في مجال تكتيكات التهديد السيبراني والتعاون بين مجرمي الإنترنت يجعل من الضروري في المُقابل للمُنشآت أن تعمل على تطوير تكتيكاتها المبتكرة والمنظمة للدفاع السيبراني. وحالياً، تُعد مراقبة التنبيهات الأمنية في الوقت الفعلي، واستخبارات التهديدات القابلة للتنفيذ، بالإضافة إلى الاستجابة الفعّالة للحوادث، والتقييم الأمني المُتعمِّق وظائف أساسية لإنشاء الكيانات والشركات المستقبلية والحفاظ عليها. ومع التقنيات الحديثة لمركز عمليات الأمن السيبراني كخدمة، يمكن للمُنشآت تحقيق المكاسب من خلال تطوير استراتيجيات دفاع سيبراني مرنة لإدارة التنبيهات الأمنية بشكل فعّال.

اليوم، يشعر محللو مركز العمليات الأمنية داخل المُنشآت بالإرهاق من كثافة وتواتر التنبيهات الأمنية – وهو سبب رئيسي يجعل مركز عمليات الأمن السيبراني كخدمة الآن أمراً بالغ الأهمية من أجل بناء استراتيجيات دفاع سيبراني من المستوى التالي. حيث يمكن تعزيز أنشطة الدفاع السيبراني المختلفة مثل جمع معلومات التهديدات وتحليل المشكلات الأمنية والاستجابة للهجمات بشكل كبير من خلال الاستعانة بمراكز العمليات الأمنية الخارجية. يُعدّ مركز العمليات الأمنية الخارجي في وضع أفضل لمواجهة التهديدات السيبرانية نظراً لقدرته العالية على مراقبة وإدارة المشكلات الأمنية بشكل فوري. علاوة على ذلك، يمكّن مركز العمليات الأمنية الخارجي المُنشآت من التواصل مع مجموعة كبيرة من مهندسي الأمن السيبراني العاملين لدى موفِّري خدمات الأمن السيبراني المُدارة ومحللي مركز العمليات الأمنية ومتصيدي التهديدات وخبراء الأمن السيبراني.

أثبتت شركة الإلكترونيات المُتقدّمة نفسها كمقدم خدمة موثوق به لحلول وخدمات إدارة الأمن السيبراني المتطورة. حيث يدعم مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة فرق الأمن السيبراني داخل المُنشآت للإشراف على وضعها الأمني، وتمكينها من اكتشاف التهديدات والمخاطر الأمنية الأخرى بشكل فوري تقريباً. كما توفر شركة الإلكترونيات المُتقدّمة أيضاً الوصول إلى التقنيات الذكية والخبراء السيبرانيين المعتمدين الذين يعززون وضعها باعتبارها أحد موفِّري خدمات الأمن المُدارة الرائدة في جميع أنحاء دول مجلس التعاون الخليجي. وبالتالي، فإن العروض الشاملة للأمن السيبراني في مركز عمليات الأمن السيبراني كخدمة من شركة الإلكترونيات المُتقدّمة قد تمكّن المُنشآت من تحديد أولويات الوظائف المطلوبة للقيام بالأعمال الروتينية، مع تأمين شبكات الشركة وتطبيقاتها وخوادمها بكفاءة عالية.

المراجع

1. After Nines Inc. (2021). Top 250 MSSPsTM 2021 Edition. [online] MSSP Alert. Available at: https://www.msspalert.com/wp-content/uploads/2021/09/Top-250-MSSPs-2021-Report.pdf.
2. TechTarget (2022). SOC Modernization and the Role of XDR. [online] usa.kaspersky.com. Available at: https://go.kaspersky.com/rs/802-IJN-240/images/ESG%20eBook%20-%20kaspersky%20-%20XDR%20and%20SOC%20Modernization%20-%20June%202022.pdf.
3. NTT (2020). Security Operations Center as a Service. [online] Available at: https://hello.global.ntt/-/media/ntt/global/products-and-services/managed-services/managed-security-services/security-operation-center-as-a-service/mss-v3-datasheet-socaas.pdf.
4. Stripe OLT (2022). Top 7 Benefits of Outsourcing Your Managed SOC. [online] Stripe OLT. Available at: https://www.thecloudcommunity.net/media/ianjh0jr/infographic-top-7-benefits-of-outsourcing-your-soc-2-2.pdf.
5. Arctic Wolf and Frost & Sullivan (2020). SOC-as-a-Service or DIY SOC? [online] Available at: https://cybersecurity.arcticwolf.com/rs/840-OSQ-661/images/AWN_SOC-as-a-Service-or-DIY_Infographic.pdf?a=infographics.
6. Splunk (2023). The State of Security 2023. [online] Available at: https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2023.pdf.
7. Gartner (2021). IT Roadmap for Cybersecurity Excerpt. [online] Available at: https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/documents/insights/the-it-roadmap-for-cybersecurity-excerpt.pdf.
8. Bussa, T., Kavanagh, K., Shoard, P., Collins, J., Lawson, C. and Schneider, M. (2020). Market Guide for Managed Detection and Response Services. [online] Gartner. Available at: https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/Market_Guide_for_MDR_2020.pdf.
9. Devo and Ponemon Institute (2020). 2020 Devo SOC Performance Report. [online] Available at: https://www.devo.com/wp-content/uploads/2020/06/DevoSOCPerformanceReport_2020.pdf?hsCtaTracking=cee86df1-bf12-4b50-befe-31a8aafaec8e%7C66198d1e-9063-41ff-8ed0-90daa77c8a2d.
10. IDC (2020). Cyber Security and its Impact on Digital Saudi. [online] Available at: https://resources.trendmicro.com/rs/945-CXD-062/images/Cybersecurity-and-its-Impact-on-Digital-Saudi.pdf.
11. IDC (2020a). Battle for the Modern Security Operations Center. [online] Available at: https://www.intelligentcio.com/wp-content/uploads/sites/12/2020/11/IDC-Spotlight-SOC-META_v1.pdf.
12. Crowley, C. and Pescatore, J. (2021). A SANS 2021 Survey: Security Operations Center. [online] Available at: https://sansorg.egnyte.com/dl/b5945iNBTy.
13. Accenture Security (2020). Cyber Threatscape Report 2020. [online] Available at: https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf.
14. Morin, J. (2020). The Future Of SOCaaS. [online] Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/08/03/the-future-of-socaas/?sh=ec0ddc6225a7.
15. Gartner (2023). Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025. [online] Gartner. Available at: https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025.
16. SANS (2023). SANS 2022 SOC Survey | SANS Institute. [online] www.sans.org. Available at: https://www.sans.org/white-papers/sans-2022-soc-survey/.

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

SAMI Advanced Electronics Company
King Khalid International Airport Industrial Estate
P.O. Box 90916,
Riyadh 11623, Saudi Arabia

+966112201350 **Email** - info@aecl.com

/AECSaudiArabia