SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

التحكم الكامل في منظومة الأمن
السيبراني للمؤسسة (MDR)

من خلال خدمات الكشف والاستجابة المُدارة المقدمة من شركة الإلكترونيات المتقدمة

جدول المحتويات

الملخص التنفيذي

أكدت السنوات الأخيرة على أهمية تعزيز المرونة السيبرانية للشركات الحديثة. فقد أدى الانتقال إلى العمل إلى (IoT) عن بُعد وانتشار أجهزة إنترنت الأشياء زيادة تعقيد مشهد الأمن السيبراني. ونتيجة لذلك، تصاعدت وتيرة وشدة الهجمات السيبرانية، مما يجعل من الضروري للمؤسسات تطوير وتنفيذ استراتيجيات أمن سيبراني شاملة وفعّالة

كما أصبح الأمن السيبراني أولوية وطنية أيضاً في المملكة العربية السعودية نظراً لجهود التحديث المتزايدة في جميع أنحاء المملكة. وتتولى المملكة زمام المبادرة من خلال الاستثمار بكثافة في مشاريع البحث والتطوير في مجال الأمن السيبراني، بالإضافة إلى تسهيل التعاون بين القطاعين العام والخاص، وتعزيز برامج التعليم والتدريب في مجال الأمن السيبراني. حيث تسعى هذه الجهود إلى بناء نظام بيئي سيبراني مرن قادر على التصدي للتهديدات الناشئة

أصبح الأمن السيبراني أولوية وطنية في المملكة ، خاصة مع جهود التحديث المتزايدة في مختلف الأنحاء. تتصدر المملكة المبادرة من خلال الاستثمار الكبير في مشاريع البحث والتطوير في مجال الأمن السيبراني، بالإضافة إلى تعزيز التعاون بين القطاعين العام والخاص، وتطوير برامج التعليم والتدريب المتخصصة في هذا المجال. تهدف هذه الجهود إلى بناء نظام بيئي سيبراني قوي ومرن قادر على مواجهة التهديدات المتجددة بفعالية

ولقد أثبتت خدمات الأمن المُدارة (MSS) على المستويين العالمي والوطني فعاليتها في رفع مستوى الأمن السيبر السيبراني داخل المنشآت بمختلف أحجامها. إلى جانب تعزيز الحماية، تساعد هذه الخدمات المنشآت في الامتثال للمعايير الصناعية من خلال حفظ السجلات، وإجراء عمليات التدقيق الأمنية، وإدارة البروتوكولات والسياسات الأمنية بشكل مستمر

وفي جميع أنحاء المملكة، تقوم خدمات الكشف والاستجابة المُدارة (MDR) من شركة الإلكترونيات المُتقدّمة بإنشاء بنية تحتية مرنة للأمن السيبراني. حيث تستفيد المُنشآت والشركات من الخبرة المحلية العميقة والتقنيات الحديثة لتقديم حلول شاملة تجمع بين الكشف المتقدم عن التهديدات، والاستجابة للحوادث، والمراقبة المستمرة. وبالتالي، تساهم في رحلة التحول الرقمي في المملكة العربية السعودية، وحماية الأصول الحيوية وتعزيز التوجه نحو مستقبل آمن ومزدهر

مراجعة وتحليل الوضع الراهن للأمن السيبراني على المستوى العالمي

في ظل مشهد الأعمال الحالي، أصبح الأمن السيبراني ضرورة استراتيجية لا غنى عنها، نظرًا لما هو على المحك من سمعة العلامة التجارية، واستمرارية الأعمال، والمخاطر المالية. وقد أدى انتشار نمط العمل على (IoT) من المنزل واعتماد أجهزة إنترنت الأشياء نطاق واسع إلى توسيع نطاق الهجمات السيبرانية. يستغل المجرمون السيبرانيون هذه الثغرات الجديدة ، مما يفرض على المؤسسات اعتماد استراتيجية أمن سيبراني استباقية وفعّالة لمواجهتها

فهم مشهد التهديدات السيبرانية الحديثة

العوامل الرئيسية للتهديدات

برامج الفدية 66%

من المُنشآت تعرضت لهجمات برامج الفدية في عام 2023 [1]

البرمجيات الخبيثة 56%

من الاختراقات في عام 2023 غير الداخلية للبيانات نتجت عن البرمجيات الخبيثة [2]

المخاطر الداخلية

4.90 مليون دولار,

متوسط تكلفة الاختراقات الناتجة عن التهديدات الداخلية [3]

التصيُّد الاحتيالي

4.76 مليون دولار,

تكلفة هجمات التصيد الاحتيالي، وهي ، أكثر العوامل شيوعاً [3]

الأنظمة السحابية 82%

من الاختراقات في عام 2023 تتضمن بيانات مخزنة في السحابة [3]

ارتفاع تكاليف الهجمات السيبرانية

بحلول عام 2025, 10.5 تريليون دولار من الأضرار السنوية المتوقعة بسبب الهجمات السيبرانية

زيادة الإنفاق على الأمن السيبراني

99% من المنظمات تخطط لزيادة ميزانياتها السيبرانية في الأشهر الاثنتي عشرة المقبلة [6]

51% من المنظمات تزيد استثماراتها في الأمن بعد عمليات الاختراق [3]

تصفّح المخاطر السيبرانية: الطريق نحو إطار عمل سيبراني مرن

لمواجهة المخاطر السيبرانية المتزايدة، تحتاج المُنشآت إلى تبني استراتيجية ديناميكية واستباقية تمكّنها من الحد من التهديدات المتطورة. ومع ذلك، فإن ما يقرب من نصف المُنشآت (49% منها) ليست مُجهزّة لمواجهة تحديات الأمن السيبراني. في الوقت نفسه، تضيع مُنشآت أخرى (54% من المُنشآت) وقتها الثمين في مواجهة التنبيهات ذات المستوى المنخفض، مما يؤدي إلى تباطؤ عمليات الاستجابة للحوادث. بالإضافة إلى ذلك، هناك عقبات داخلية كبيرة تمنع قادة الأمن السيبراني من التعامل مع المخاطر الخارجية المتزايدة [7]

العقبات الرئيسية التي تعيق تقدّم الأمن السيبراني [8]

غياب الخبرة المطلوبة

%38 أفادو بأن الأدوات الأمنية الحالية تتطلب مستوى عالٍ من الخبرة المتخصّصة

نقص في عدد الموظفين الكافي

%81 يتفقون على أن العمليات الأمنية تتعثر بسبب نقص المتخصصين في الأمن السيبراني

نقص في الأدوات المناسبة

%51 يكشفون أن الأدوات الحالية تكافح بصعوبة لاكتشاف التهديدات المُتقدّمة والتحقيق فيها

مجالات التركيز الرئيسية لمُنشأة تتمتع بالمرونة السيبرانية [7]

الأساس الآمن

نشر ضوابط مُحكمة ومُصادقة متعددة المستويات للتخفيف من أثر الأخطاء البشرية

أفضل الممارسات

اعتماد ممارسات أمنية منظّمة لتطبيق حماية قابلة للقياس وفعّالة

الاستجابة للحوادث

اختبار العمليات وتحديثها وتحسينها للتعامل مع التنبيهات بدقة

الدعم الخارجي

تعزيز الاستجابة من خلال خدمات الكشف المُدارة لاحتواء أسرع والاستفادة من الخبرة المُتقدّمة

تأمين المملكة سيبرانياً: نظرة على المشهد الأمني السيبراني في المملكة العربية السعودية

قامت خطط التنمية الوطنية في المملكة العربية السعودية، كجزء من رؤية 2030، وأيضاً مبادرات تنويع الاقتصاد، باعتماد التقنيات الناشئة كعامل رئيسي في التحول الصناعي. ومع ذلك، فإن استخدام هذه التقنيات جعل من القطاعين العام والخاص عرضة للتهديدات المتطورة في مشهد الأمن السيبراني العام في المملكة. وفي هذا السياق، يتوقع 40% من قادة الأعمال في المملكة تعرضاً معتدلاً لهذه المخاطر السيبرانية، بينما يستعد 20% منهم لتعرض كبير لهذه المخاطر في الأشهر القليلة المقبلة [9]

ومن خلال اتباع نهج استباقي للتخفيف من هذه المخاطر، تعمل المملكة على تطوير القدرات والإمكانيات لحماية التقنيات التي تُمكّن مبادرات النمو. حيث تلعب الاستراتيجية الوطنية للأمن السيبراني (NISS) والهيئة الوطنية للأمن السيبراني (NCA)، وهما برنامجان للأمن السيبراني أطلقتهما الحكومة السعودية، دوراً رئيسياً في جعل مُنشآت المملكة مرنة سيبرانياً [10]

تزايد الوعي بين مُنشآت الأعمال في المملكة العربية السعودية لتعزيز دفاعاتها وتحويل التهديدات إلى فرص

%62 يُشدّدون على أهمية الحفاظ على مستوى مثالي من حلول تقنيات الأمن السيبراني

%73 يعطون الأولوية للمخاطر الرقمية والتقنية، كما تُعتبر هذه المخاطر مصدر قلق رئيسي لأكثر من 51% من المُنشآت حول العالم

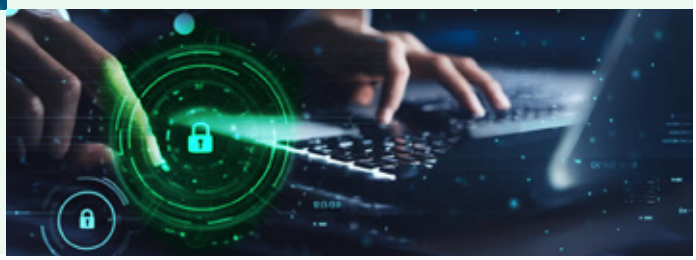
%33 يتوقعون زيادة تتراوح بين 6 إلى 10% في ميزانية الأمن السيبراني لمُنشآتهم

"%" تمثل النسبة المئوية لتنفيذي الأعمال والتقنية

تعزيز دور الأمن السيبراني: دور خدمات الأمن المُدارة

في السنوات الأخيرة، أدركت فرق الأمن السيبراني حول العالم تزايد حجم المخاطر السيبرانية واتخذت خطوات استباقية للتصدي لها. ومع ذلك، تستمر التهديدات وتتزايد الحاجة للحفاظ على المرونة السيبرانية، مما قد يسبب ضغطًا وإرهاقًا للمؤسسات، ويجعلها تتجه نحو اتخاذ إجراءات عاجلة لتعزيز دفاعاتها. في هذا السياق، تُعتبر الشراكة مع مقدمي خدمات الأمن المُدارة وسيلة فعّالة لتعزيز قدرات الاستجابة للحوادث، حيث تدعم هذه الخدمات فرق الأمن القائمة من خلال توفير خبرات متخصصة وأدوات متقدمة تُمكّن المؤسسات من مواجهة التهديدات المتطورة بكفاءة

40% من الاختراقات تم اكتشافها بواسطة أطراف خارجية أو جهات خارجية، بينما تم اكتشاف 33% منها بواسطة فرق وأدوات داخلية [3]



كشف 42% من مديري أمن المعلومات (CISOs) أنهم يخصصون نسبة 25% من ميزانية الأمن السيبراني لمُنشآتهم من أجل الاستعانة بمصادر خارجية [13]

الفوائد رئيسية للخدمات الأمنية المُدارة وفقاً لقادة الأمن السيبراني [7]

%55
احتواء التهديدات بسرعة والاستجابة لها

%53
تعزيز الخبرة الأمنية الداخلية

%50
تحسين أتمتة العمليات

%48
اكتشاف التهديدات بشكل أسرع

%39
تسجيل الأحداث بشكل أكثر قوة

%39
زيادة كفاءة الميزانية

خدمات الكشف والاستجابة المدارة (MDR) من شركة الإلكترونيات المُتقدّمة: تسهيل وتقديم نظام آمن ومتكامل للأمن السيبراني يغطي أنحاء المملكة العربية السعودية

توفر خدمات الكشف والاستجابة المُدارة (MDR) من شركة الإلكترونيات المُتقدّمة للمُنشآت السعودية حماية من التهديدات على مدار الساعة وإرشادات من قبل أفضل الخبراء. حيث يقوم فريقنا المحلي، المدعوم بأفضل الممارسات العالمية، بتأمين بيئة السحابة الهجينة الخاصة بالمُنشأة وتيسير الامتثال التنظيمي. فمن خلال الاستفادة من البرامج الرائدة في الصناعة وخبرات المهنيين المعتمدين، تعزز خدمات الكشف والاستجابة المُدارة (MDR) من شركة الإلكترونيات المُتقدّمة الوضع الأمني للمُنشأة

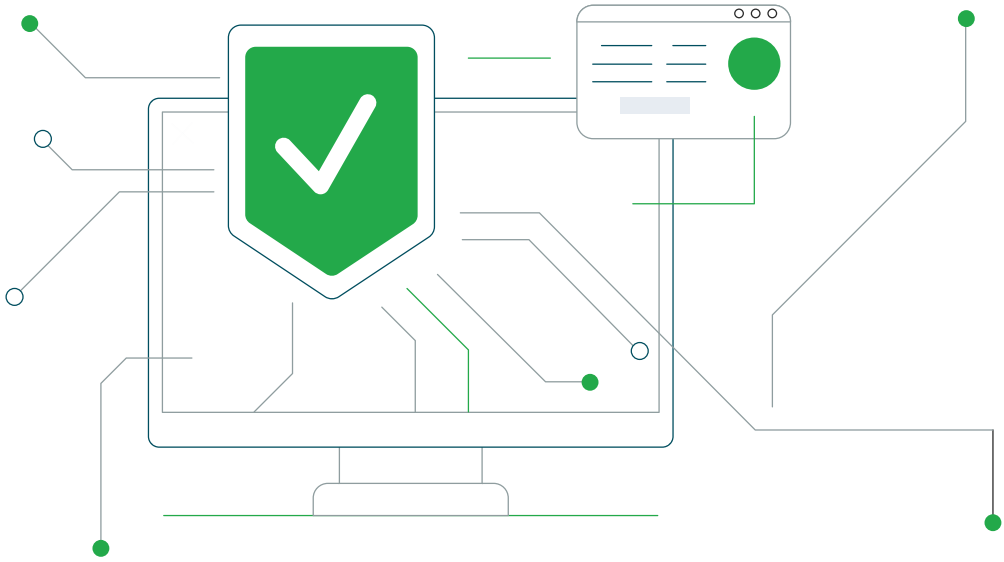
خدمات أساسية لحماية شاملة

الكشف عن التهديدات وتحليلها

- تحديد أولويات التهديدات
- تحليل البيانات للتهديدات
- البحث المستمر عن التهديدات

تحليل ومراقبة السجلات

- مراقبة على مدار الساعة
- إدارة السجلات والثغرات
- إنشاء تذاكر الحوادث وتطبيق سير عملها



التحليل الجنائي الرقمي والاستجابة للحوادث

- تحليل الأسباب الجذرية للحوادث
- تحليل البيانات واستعادتها
- فحص البرمجيات الخبيثة
- إدارة نظم المعلومات الأمنية والأحداث (SIEM)

تقارير الأمن والحوكمة

- مؤشرات الأداء الرئيسية (KPIs) ومؤشرات النتائج الرئيسية (KRAs) الأمنية
- بحث وتنبيهات سهلة الاستخدام
- تقارير ولوحات تحكم قابلة للتكوين
- إنشاء ومراجعة كتيبات مركز العمليات الأمنية (SOC)
- التقييمات الأمنية وعمليات التصحيح

الخاتمة

إن التقدم التقني في المملكة العربية السعودية يصاحبه بالضرورة زيادة في المخاطر السيبرانية. وقد أدى ذلك إلى زيادة التركيز على تحسين البيئة الأمنية السيبرانية العامة في المملكة وتعزيز المرونة السيبرانية لضمان أساس آمن للاقتصاد المعرفي المنشود. وفي هذا السياق، تتخذ الحكومة السعودية العديد من المبادرات لتوحيد جهود الأمن السيبراني. وقد أسهمت هذه الجهود في زيادة الوعي بالأمن السيبراني بين الشركات والمُنشآت السعودية، ممّا دفعها إلى اتخاذ تدابير استراتيجية لتحقيق الأمن السيبراني

أن (MSSP) يمكن لمقدمي خدمات الأمن المُدارة يلعبوا دورًا أساسيًا في تحقيق أهداف الأمن السيبراني للمملكة. فهم يقدمون حلاً فعالاً من حيث التكلفة لنشر التقنيات السيبرانية المتقدمة. من خلال توفير الوصول إلى فرق من الخبراء الأمنيين ذوي المهارات العالية والخبرة الواسعة، يمكّن مقدمو الخدمات المؤسسات والشركات بمختلف أحجامها من بناء منظومة أمنية سيبرانية قوية ومستقرة

في هذا السياق، برزت خدمات الكشف والاستجابة من شركة الإلكترونيات المُتقدّمة (MDR) المُدارة كحل متقدم يُمكن المنشآت من مواجهة التهديدات السيبرانية بكفاءة عالية. من خلال استخدام أدوات تقنية متطورة، تساعد هذه الخدمات في تقليل التكاليف وتحسين الأداء، بالإضافة إلى معالجة تحديات نقص الخبرات المتخصصة في مجال الأمن السيبراني. من شركة الإلكترونيات MDR وبذلك، تسهم خدمات المُتقدّمة في تعزيز البنية التحتية الر الرقمية اللازمة لدعم النمو الاقتصادي والابتكار، وتدعم تحقيق أهداف رؤية 2030 في بناء اقتصاد رقمي آمن ومزدهر للمملكة

المراجع

1. Deloitte (2024). Deloitte Cybersecurity Threat Trends Report 2024. Available at: https://www2.deloitte.com/us/en/pages/noindex/cyber/cybersecurity-threat-trends-report-2024-download.html.

2. Ponemon Institute (2024). Cost of Insider Risks. Available at: https://www2.dtexsystems.com/l/464342/2023-09-15/3w7l7k/464342/1694800570ZwvyrzsD/2023_Cost_of_Insider_Risks_Global_Report___Ponemon_and_DTEX___Dgtl.pdf.

3. IBM (2023). Cost of a Data Breach Report 2023. Available at: https://www.ibm.com/downloads/cas/E3G5JMBP.

4. Institute for Defense and Business (2024). COVID-19 and working from home: balancing cyber security and productivity. Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-home-office-cyber-security.html.

5. McKinsey (2023). What is cybersecurity? | Available at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity.

6. PricewaterhouseCoopers (2023). 99% of organisations will increase their cyber budgets, out of which 50% envisaged an increase between 6% and 15% in the next 12 months: PwC's 2024 Digital Trust Insights. Available at: https://www.pwc.in/press-releases/2023/99-of-organisations-will-increase-their-cyber-budgets-out-of-which-50-envisaged-an-increase-between-6-and-15-in-the-next-12-months-pwcs-2024-digital-trust-insights.html.

7. VMware, Inc (2021). The state of incident response 2021: It's time for a confidence boost 2 T H E STAT E O F I N C I D E N T R E S P O N S E 2 0 2 1. Available at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-the-state-of-incident-response-2021.pdf.

8. Enterprise Strategy Group (2022). SOC Modernization and the Role of XDR 1 SOC Modernization and the Role of XDR june 2022. Available at: https://www.cisco.com/c/dam/global/en_uk/products/se/2022/6/collateral/soc-modernization-xdr.pdf.

9. PricewaterhouseCoopers (2024). 27th Annual CEO Survey: Saudi Arabia findings. Available at: https://www.pwc.com/m1/en/publications/27th-annual-ceo-survey-ksa-findings.html

10. IDC Saudi Arabia (2020). Cybersecurity and its impact on digital Saudi. Available at: https://resources.trendmicro.com/rs/945-CXD-062/images/Cybersecurity-and-its-Impact-on-Digital-Saudi.pdf.

11. PricewaterhouseCoopers (2024). Digital Trust Insights 2024 - The KSA perspective. Available at: https://www.pwc.com/m1/en/publications/middle-east-digital-trust-insights-2024/the-ksa-perspective.html.

12. Deloitte (2021). COVID-19 and working from home: balancing cyber security and productivity. Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-home-office-cyber-security.html.

13. Deloitte (2023). Cybersecurity insights 2023: Budgets and benchmarks for financial services institutions. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-cybersecurity-insights-23-budgets-and-benchmarks.pdf.

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