يتضمن حماية قوية ومدعومة بقدرات الذكاء الاصطناعي للنقاط الطرفية

«كاسبرسكي» تطلق حل «Kaspersky Next» الجديد في الشرق الأوسط

قدمت كاسبرسكي خط منتجاتها الرائد الجديد «Kaspersky Next»، والذي يجمع كلاً من الحماية القوية للنقاط الطرفية، والشفافية، وسرعة حل الاكتشاف والاستجابة للنقاط الطرفية (EDR)، مع الوضوح والأدوات القوية لحل الاكتشاف والاستجابة الموسعة (XDR). يتوفر هذا المنتج في منطقة الشرق الأوسط، حيث أصبح بإمكان للعملاء الآن اختيار أحد ثلاث مستويات للمنتجات المصممة وفقاً لمتطلبات أعمالهم، وتعقيد بنيتهم التحتية لتكنولوجيا المعلومات، ومواردهم المتاحة.

وفقاً لتقرير «تحديث مراكز العمليات الأمنية ودور الاكتشاف والاستجابة الموسعة» الصادر عن Enterprise Strategy Group من دراسة استقصائية أجريت بالشراكة مع كاسبرسكي، قالت 52 % من الشركات أن العمليات الأمنية قد أصبحت أكثر صعوبة اليوم مما كانت عليه قبل عدة سنوات. وتعود الأسباب الرئيسية لهذا التحدي إلى: مشهد التهديدات المتطور والمتغير بسرعة (ذكره 41 % من المشاركين)، وسطح الهجوم الآخذ بالتوسع (40 %)، والافتقار إلى مهارات وموظفي الأمن السيبراني لمواكبة التحليلات والعمليات الأمنية (20 %).

في خضم مشهد التهديدات السيبرانية دائم التطور، من الضروري أن تمتلك الشركات حل أمن سيبراني شامل يمكنها الوثوق به والاعتماد عليه للحماية الفعالة. وباعتبارها شركة رائدة في مجال الابتكار والتكنولوجيا، تعمل كاسبرسكي باستمرار على تطوير حلولها لتلبية جميع متطلبات الأمن السيبراني للشركات، وتساعدها على بناء أطر عمل متينة للأمن السيبراني.

يعد Kaspersky Next خطاً جديداً من منتجات الأمن السيبراني، حيث يتضمن حماية قوية ومدعومة بقدرات الذكاء الاصطناعي للنقاط الطرفية. ولا يكتفي هذا الحل بكونه منصة حماية نقاط طرفية (EPP) كلاسيكية، بل يضيف كذلك الاكتشاف والاستجابة للنقاط الطرفية والاكتشاف والاستجابة الموسعة للعملاء المؤسساتيين بغض النظر عن حجمهم أو الصناعة التي يعملون فيها. وباعتبارهما أكثر حلول الأمن السيبراني تقدما وفعالية، يساعد حلا الاكتشاف والاستجابة للنقاط الطرفية والاكتشاف والاستجابة الموسعة من كاسبرسكي الشركات على الصمود في وجه الهجمات الأكثر انتشاراً، ومراوغة، وتعقيداً، وهو ما يوفر للشركات الوضوح الكامل، والتحكم، والاستجابة السريعة، بالإضافة إلى التصيد الاستباقي عن التهديدات.


الحل الرائد الجديد "Kaspersky Next" من "كاسبرسكي"

لا يعد حل Kaspersky Next محدوداً بنوع تثبيت محدد، إذ من الممكن تثبيته على السحابة أو بشكل محلي على حد سواء. كما يمكن للشركات إدارته إما عبر وحدة تحكم مبسطة لأداء مهام الأمن السيبراني الأساسية بسرعة، أو عبر وحدة تحكم مؤسساتية المستوى مع عناصر تحكم دقيق إضافية ومراقبة متقدمة.

وتساعد مجموعة المنتجات الجديدة الشركات على بناء مهام الأمن السيبراني المهمة، لتوفير حماية قوية ضد أنواع متعددة من التهديدات التي تواجهها الشركات بكثرة مثل برمجيات الفدية، والبرمجيات الخبيثة، واختراق البيانات، كما تساعد في تجنب اختراق البنية التحتية عبر اختراق البريد الإلكتروني للأعمال، وهجمات سلسلة التوريد، والثغرات ونقاط الضعف الأخرى.

يتضمن حل Kaspersky Next EDR Optimum حماية قوية للنقاط الطرفية مع الوظائف الأساسية من حيث الاكتشاف والاستجابة للنقاط الطرفية، بالإضافة إلى عناصر التحكم المتقدمة، وإدارة التحديثات الأمنية، والأمن السحابي. حيث يتم توجيه ميزات مراقبة التهديدات، والتحقيق، والاستجابة لمساعدة الشركات على صد الهجمات بسرعة، ومع استهلاك أقل قدر من الموارد. ويوصى بهذا الحل للشركات التي تمتلك فرق أمن معلومات صغيرة.

يقوم مستوى Kaspersky Next XDR Expert بتجميع البيانات، وتحليلها، وربطها من مصادر مختلفة عبر البنية التحتية لتكنولوجيا المعلومات في المؤسسة، ويوفر ذلك مراقبة مباشرة ورؤى عميقة حول المخاطر الإلكترونية المتطورة لتقديم اكتشاف متقدم للتهديدات واستجابة آلية. وهو حل الأمن السيبراني الفعال القادر أيضاً على التكامل مع موردي الطرف الثالث. حيث يوصى بهذا الحل للشركات التي تمتلك فرق أمن سيبراني خبيرة أو مراكز عمليات أمنية (SOC).

يعد حل Kaspersky Next EDR Foundations حماية قوية للنقاط الطرفية بحيث تحدد التهديدات وتحيدها قبل أن تتمكن من إلحاق الضرر بعمليات الأعمال. حيث تعمل أدوات التحكم الأمنية المرنة والمباشرة برفقة سيناريوهات تكنولوجيا المعلومات المضمنة على تمكين التشغيل دون تدخل، والسماح للشركات بتخصيص سياسات الأمان الخاصة بها لتناسب احتياجاتها الفريدة. كما يوصى بهذا الحل للشركات التي تستخدم أقسام تكنولوجيا المعلومات لمهام أمن المعلومات.

يوفر مستوى Kaspersky Next EDR Optimum حماية قوية للنقاط الطرفية مع الوظائف الأساسية من حيث الاكتشاف والاستجابة للنقاط الطرفية، بالإضافة إلى عناصر التحكم المتقدمة، وإدارة التحديثات الأمنية، والأمن السحابي. حيث يتم توجيه ميزات مراقبة التهديدات، والتحقيق، والاستجابة لمساعدة الشركات على صد الهجمات بسرعة، ومع استهلاك أقل قدر من الموارد. ويوصى بهذا الحل للشركات التي تمتلك فرق أمن معلومات صغيرة.

يقوم مستوى Kaspersky Next XDR Expert بتجميع البيانات، وتحليلها، وربطها من مصادر مختلفة عبر البنية التحتية لتكنولوجيا المعلومات في المؤسسة، ويوفر ذلك مراقبة مباشرة ورؤى عميقة حول المخاطر الإلكترونية المتطورة لتقديم اكتشاف متقدم للتهديدات واستجابة آلية. وهو حل الأمن السيبراني الفعال القادر أيضاً على التكامل مع موردي الطرف الثالث. حيث يوصى بهذا الحل للشركات التي تمتلك فرق أمن سيبراني خبيرة أو مراكز عمليات أمنية (SOC).

يعد حل Kaspersky Next جزءاً من النظام البيئي لمنتجات الشركة الموجهة للمؤسسات، وهو مصمم ليكون متوافقاً بشكل مباشر مع حلول وخدمات كاسبرسكي الأخرى. ومع الطلب المتزايد على حلول الأمن السيبراني الأكثر شمولا، يمكن للشركات الانتقال بسهولة من مستوى إلى آخر وفق متطلباتها الحالية للأمن السيبراني.

بهذه المناسبة، قال أنطون إيفانوف، الرئيس التقني لشركة كاسبرسكي: «نطلق اليوم حل الاكتشاف والاستجابة الموسعة الرائد في السوق ونعيد ابتكار عروض منتجات الشركة، بينما نبدأ فصلاً جديداً من تاريخنا كمزود خدمات للشركات. حيث يجعل حل Kaspersky Next كلا من الاكتشاف والاستجابة للنقاط الطرفية والاكتشاف والاستجابة الموسعة أموراً أكثر بساطة للشركات والمؤسسات بمختلف أحجامها. إذ أننا نقدم أعلى مستويات الحماية المدعومة بخبرتنا الفريدة لجميع العملاء، بدءاً من أولئك الذين لا يمتلكون ضباط أمن إلكتروني، إلى أولئك الذين يمتلكون فرق الأمن السيبراني الخبيرة. وهدفنا هو السماح للشركات ببناء أنظمة أمن معلومات موثوقة، وفعالة مقابل التكلفة، وبأعلى مستويات الجودة وفق متطلباتها الخاصة.»

مع الحفاظ على مقاييس ائتمانية قوية

«إس آند بي غلوبال»: شركات النفط الخليجية يمكنها تحقيق أهداف صافي الانبعاثات الصفري

قالت وكالة ستاندرد آند بورز للتصنيفات الائتمانية "إس آند بي غلوبال" إن شركات النفط الوطنية الخليجية يمكنها استيعاب الاستثمارات الإضافية اللازمة؛ للتحرك لتحقيق أهداف صافي الانبعاثات الصفري مع الحفاظ على مقاييس ائتمانية قوية، على افتراض قيامها بمطالبات نقدية معتدلة من المساهمين.

جاء ذلك في تقرير نشرته الوكالة أمس الثلاثاء، بعنوان: "شركات النفط الخليجية غير قلقة حالياً بشأن أهداف صافي الانبعاثات الصفري".

وقالت روان عويدات، محلل ائتماني في الوكالة: "يجب أن يتراوح متوسط الاستثمارات منخفضة الكربون لشركات النفط الوطنية الخليجية بين 15 – 25 مليار دولار أمريكي سنوياً على الأقل حتى عام 2026 لمواكبة حجم استثمارات نظيراتها المدرجة عالمياً".

وذكرت أنه حتى بعد أخذ هذه الاستثمارات في الاعتبار، فإن التأثير الإجمالي على نسبة الدين إلى الأرباح قبل اقتطاع الفوائد والضرائب والإهلاك وإطفاء الدين لدى شركات النفط الوطنية سيكون أقل من 2.0 مرة، في المتوسط.

وتوقعت "عويدات" أن تمتلك شركات النفط الوطنية الخليجية هوامش مالية كافية ومزايا تنافسية؛ لاستيعاب الاستثمارات الإضافية اللازمة لمواكبة نظيراتها العالمية، وأن تتمكن من الحفاظ على نسبها الائتمانية على مدى السنوات الخمس المقبلة.

ويأتي ذلك نظراً للحصة الصغيرة نسبيًا لمصادر الطاقة المتجددة في توليد الكهرباء في دول الخليج، مقارنة بالمناطق الأخرى، وأهداف صافي الانبعاثات الصفري لدول الخليج، مع توقعات زيادة الاستثمارات في مجال الطاقة المتجددة، بما يمثل فرصة للسندات الخضراء والاجتماعية وسندات الاستدامة والمرتبطة بالاستدامة.

وأوضح التقرير أنه على الرغم من استفادة شركات النفط الوطنية من الميزانيات العمومية القوية، إلا أنه سيتعين عليها تقييم احتياجات الأرباح مقابل توزيعات الأرباح. لذلك ستراقب الوكالة التزامات شركات النفط الوطنية المتعلقة بالسياسة المالية، والتي ستساعد في تحديد احتياجاتها من التمويل الخارجي.

وكشف أنه في الفترة التي سبقت انعقاد مؤتمر الأمم المتحدة المعني بالمناخ "كوب 28" قامت العديد من الشركات الحكومة في المنطقة بتحديث استراتيجياتها للاستدامة، ففي يناير2024، رفعت شركة أدنوك الإماراتية قيمة استثماراتها المستهدفة منخفضة الكربون حتى عام 2030 بأكثر من 50 % إلى 23 مليار دولار، من 15 مليار دولار سابقا.

ويعني ذلك أن الاستثمارات منخفضة الكربون ستمثل 15 % من إجمالي استثمارات أدنوك المخطط لها خلال نفس الفترة، وستمثل استثمارات أرامكو السعودية في مجال الطاقة المتجددة 10 % من استثمارات الشركة المخطط لها على المدى القريب.

وكالة ستاندرد آند بورز

بهدف تعزيز قطاع الخدمات المالية

«الاتحاد للمدفوعات» تطلق مشروع التمويل المفتوح في الإمارات

جانب من توقيع الاتفاقية

وقعت شركة الاتحاد للمدفوعات، التابعة لمصرف الإمارات العربية المتحدة المركزي، اتفاقية شراكة مع شركة "Core42"، إحدى شركات مجموعة "G42" الإماراتية المزودة لحلول تمكين الذكاء الاصطناعي، بهدف إطلاق وتنفيذ مشروع التمويل المفتوح في دولة الإمارات، ضمن مبادرات برنامج تحوّل البنية التحتية المالية للمصرف المركزي.

شهد توقيع الاتفاقية خالد محمد بالعمي، محافظ مصرف الإمارات العربية المتحدة المركزي. ووقعت الاتفاقية فاطمة الجابري، مساعد المحافظ لقطاع مكافحة الجرائم المالية، سلوك السوق وحماية المستهلك، عضو مجلس إدارة شركة الاتحاد للمدفوعات، وكيريل إيفتيموف، الرئيس التنفيذي لشركة Core42.

يأتي إطلاق مبادرة التمويل المفتوح في إطار دعم الرؤية الشاملة لدولة الإمارات لإرساء معايير عالمية لقطاع التمويل المفتوح، استناداً إلى أفضل الممارسات والتجارب الناجحة لتقديم آلية عمل التمويل المفتوح الأقوى في العالم، حيث ستكون الإمارات أول دولة على مستوى العالم تقوم بتنفيذ إطار شامل ومركز لواجهة برمجة التطبيقات، والذي يتيح الوصول إلى جميع أسواق الخدمات المصرفية والتأمينية والشركات الأخرى الخاضعة لترخيص ورقابة المصرف المركزي بعد موافقة العميل.

وتعد المبادرة جزءاً أساسياً من جهود المصرف المركزي المستمرة لتحقيق رؤيته وأهدافه الاستراتيجية، وذلك من خلال توفير فرص جديدة في قطاع الخدمات المالية وتعزيز الشمول المالي الرقمي، وتمكين العملاء عبر منصة رقمية من تبادل المعلومات بشأن المنتجات المالية مع أطراف أو مؤسسات مالية أخرى بشكل آمن وفعّال. كما تقدّم مزايا مختلفة للعملاء مثل إجراء المدفوعات والمعاملات المالية من خلال أطراف ثالثة، بالإضافة إلى إتاحة الفرصة للحصول على عروض أسعار حول الخدمات المالية.

وتُمكن مبادرة التمويل المفتوح ابتكار المنتجات والخدمات، من خلال دمجها بسلاسة ضمن المنظومات الرقمية للقطاعات الأخرى لدعم خدماتها وتعزيزها. وسيخضع جميع المشاركين لنظام ترخيص ورقابة فعّال، حيث سيتم توفير الخدمات المصرفية المفتوحة في المرحلة الأولى، وخدمات التأمين المفتوح في المرحلة الثانية، بحيث تكون متاحة للعملاء في العام 2024.

وكانت شركة الاتحاد للمدفوعات وقعت مؤخراً اتفاقيات شراكة مع شركتي "Ozone API"، و"Raidia"، كمزودي خدمات التكنولوجيا اللازمة بدعم من شركة Core42 لتنفيذ المشروع.

وقالت فاطمة الجابري، مساعد المحافظ لقطاع مكافحة الجرائم المالية، سلوك السوق وحماية المستهلك، عضو مجلس إدارة شركة الاتحاد للمدفوعات: "يمثل تنفيذ مشروع التمويل المفتوح خطوة متقدمة في مجال تطور قطاع الخدمات المالية في دولة الإمارات، وتعزيز تحوّل البنية التحتية المالية للمصرف المركزي. وسيسهم المشروع في تسريع تبني الخدمات المالية الرقمية، وتوفير مزيد من المنتجات والخدمات المالية المبتكرة والآمنة والرقمية في الدولة، بالإضافة إلى تقديم تجربة مالية سلسة، ما يضمن للمستهلكين إدارة الموارد والمعاملات المالية، والوصول بسلاسة إلى مجموعة متنوعة من المنتجات المالية".

مع حصولها على شهادتي اعتماد للأمن السيبراني

«الخليج للحاسبات الآلية» ترسي معايير جديدة للصناعة

في إنجاز تاريخي جديد، حصلت الخليج للحاسبات الآلية، الشركة الرائدة في توفير الحلول الرقمية الشاملة، على شهادتي اعتماد جديدتين من مجلس مختبري الأمن الأخلاقي المسجلين (CREST)، ومركز دبي للأمن الإلكتروني (DESC)، في مجال اختبار الاختراق والاستجابة للحوادث.

ويعد حصول شركة الخليج للحاسبات الآلية على هاتين الشهادتين، دليلاً واضحاً على ريادتها وعمق خبرتها في تقديم في تقديم أحدث حلول الأمن السيبراني، ويعكس التزامها الراسخ بالحفاظ على الجذور المحلية وتبني أرقى المعايير العالمية. وجدير بالذكر أن مؤسسات القطاعين العام والخاص في جميع أنحاء المنطقة تتجه بشكل متزايد في هذا العصر الذي يتسم بتصاعد التهديدات السيبرانية المتطورة، للتعاون مع مقدمي حلول أمن سيبراني معتمدين ممن يستوفون المعايير الصارمة لكل من مجلس مختبري الأمن الأخلاقي المسجلين (CREST)، ومركز دبي للأمن الإلكتروني (DESC). ويعد مجلس مختبري الأمن الأخلاقي المسجلين (CREST)، هيئة دولية غير ربحية مكرسة لإنشاء عالم رقمي آمن من خلال بناء القدرات والإمكانات والاتساق والتعاون داخل صناعة الأمن السيبراني العالمية. هذا وتم تأسيس مركز دبي للأمن الإلكتروني (DESC) في عام 2014، وهو هيئة تنظيمية تشرف على إطار الأمن السيبراني وتعزيز مبادرات الأمن الإلكتروني في إمارة دبي. وتمثل شهادتا الاعتماد الجديدتان ضماناً للعملاء بأن خدمات الأمن السيبراني المقدمة من شركة الخليج للحاسبات الآلية هي على أعلى مستويات الجودة، ويتم تقديمها من قبل خبراء يتمتعون بالمؤهلات والمهارات المناسبة. كما تسلط هاتين الشهادتين الضوء على التزام الشركة الراسخ بأعلى المعايير في اختبار الاختراق وخدمات الاستجابة للحوادث، مما يضمن حصول العملاء على أفضل حلول الأمن السيبراني في فئتها، وباعتبارها عضواً يحمل اعتماداً مزدوجاً، سيتم الاعتراف بعروض الأمن السيبراني التي تقدمها شركة الخليج للحاسبات الآلية في منطقة أوروبا والشرق الأوسط وأفريقيا. ويتم تسهيل الاعتماد لهذه الخدمات في دبي، بواسطة مجمع دبي للابتكار السيبراني، من خلال برنامج Dubai Cyber Force، وهو عبارة مبادرة تم إطلاقها بالتعاون بين مؤسسة CREST ومركز دبي للأمن الإلكتروني.