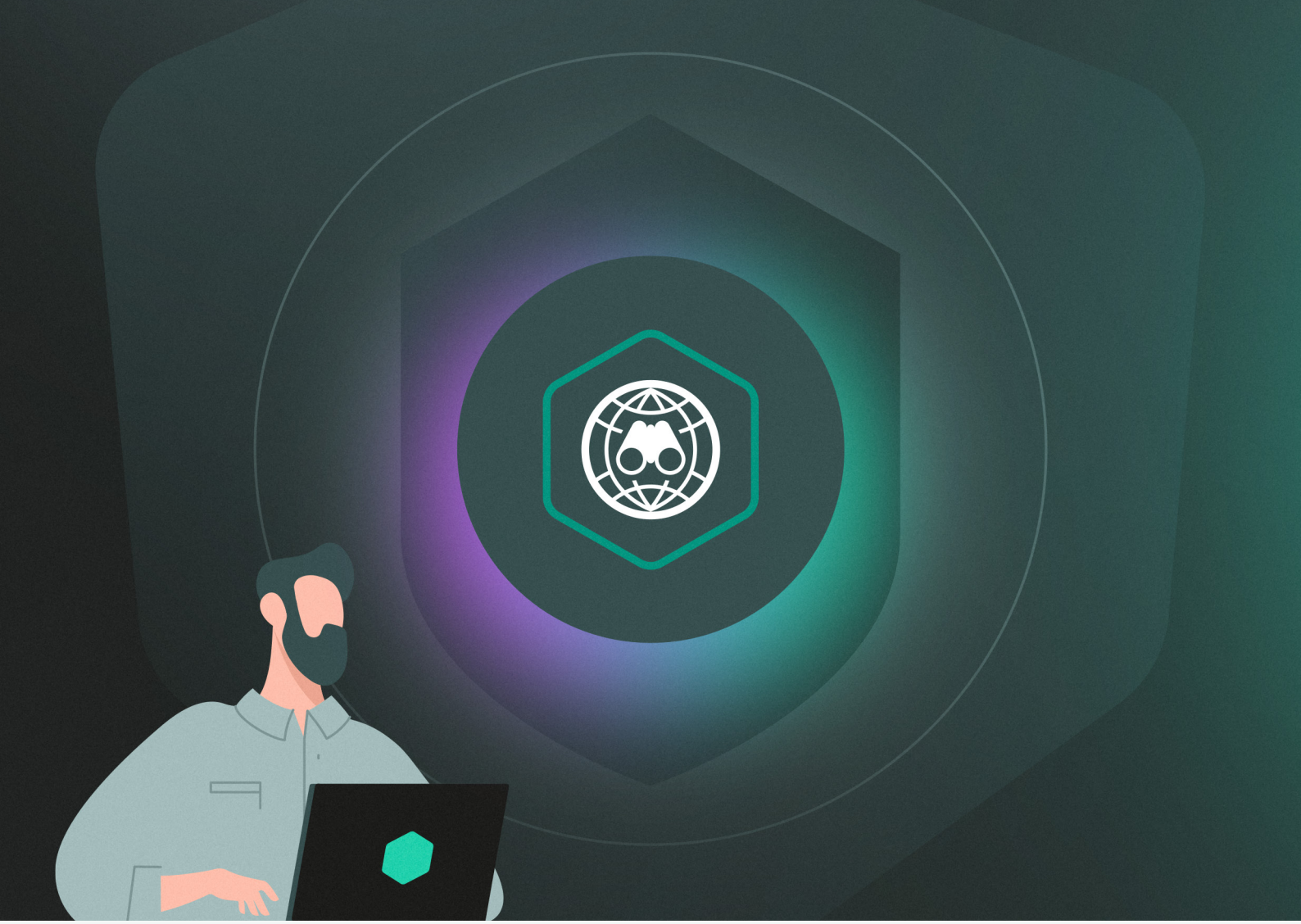


Kaspersky Threat Intelligence

تقييم مصادر المعلومات المتعلقة بالتهديدات

kaspersky واجهوا المستقبل بأمان

اعرف المزيد عبر kaspersky.com
#bringonthefuture

المقدمة

مع توسُّع نطاق التهديدات وتزايد تعقيدها، لا يكفي التفاعل مع الحادث، كما أن البيئات المتزايدة التعقيد توفر فرصًا متنوعة للمهاجمين. تمتلك كل صناعة وكل منظمة بياناتها الفريدة الخاصة بها التي تسعى إلى حمايتها، وتستخدم مجموعتها الخاصة من التطبيقات والتقنيات وما إلى ذلك. كل هذا يقدم عددًا مهولاً من التنوع في الأساليب الممكنة لتنفيذ هجومٍ مع ظهور أساليب جديدة يوميًّا.

لاحظنا في العامين الماضيين اختفاء الحدود بين الأنواع المختلفة للتهديدات ومختلف أنواع الجهات التي تشن التهديدات. إن الأساليب والأدوات التي كانت في السابق تمثل تهديدًا لعدد محدود من المنظمات انتشرت الآن على نطاق أوسع في السوق. من الأمثلة على ذلك ما فعلته مجموعة **Shadow Brokers** بوضع أدوات اختراق متقدمة في متناول مختلف الجماعات الإجرامية، التي لم يكن لها القدرة على الوصول إلى أدوات معقدة مثل هذه إلا من خلال ذلك التسريب. مثال آخر هو ظهور حملات تهديدات مستعصية متقدمة ومستهدفة لا تركِّز على التجسس الإلكتروني فحسب، بل على السرقة، سرقة الأموال لتمويل أنشطة أخرى تشارك فيها مجموعة التهديدات المستعصية المتقدمة. والأمثلة الأخرى كثيرة.

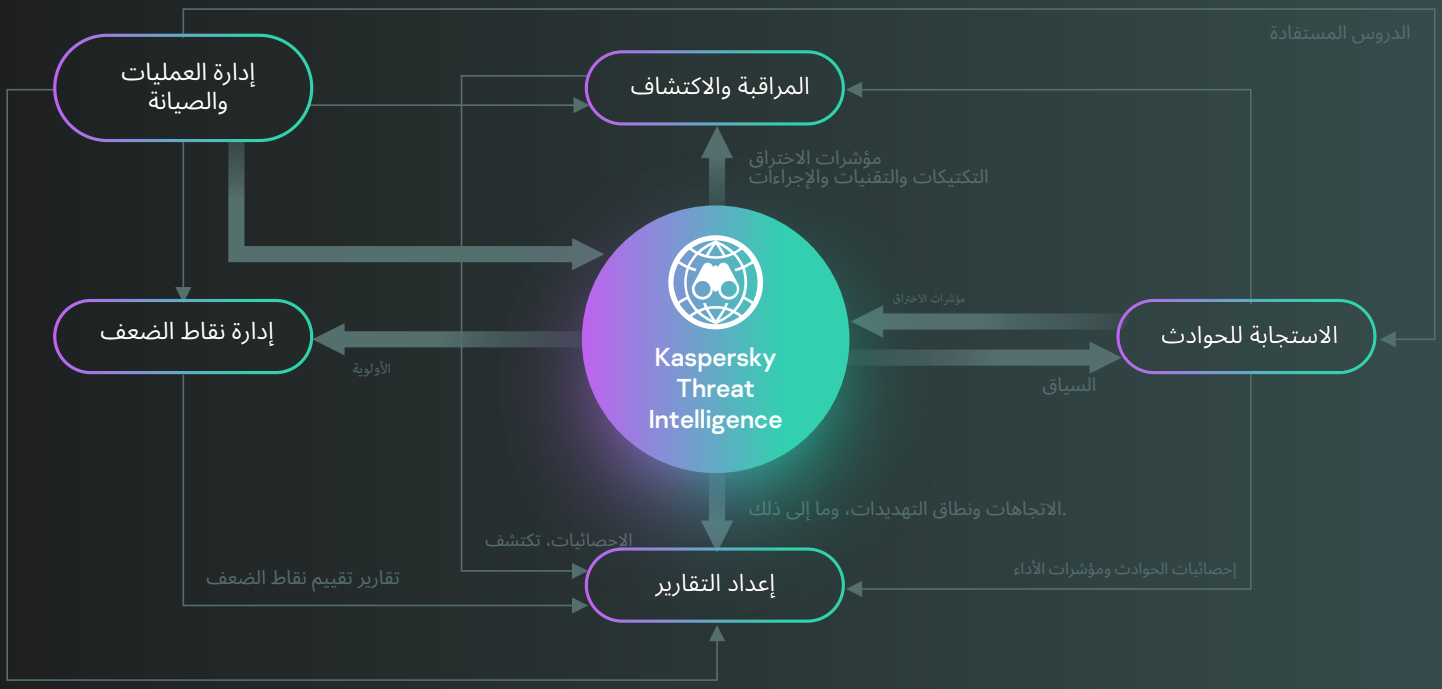
الحاجة إلى منهجية جديدة

إن الأساليب والأدوات التي كانت في السابق تمثل تهديدًا لعدد محدود من المنظمات انتشرت الآن على نطاق أوسع في السوق.

مع زيادة وقوع المؤسسات الكبيرة في فخ الهجمات المتقدمة والمستهدفة، يتضح لنا أن الأساليب الدفاعية الناجحة تتطلب منهجيات جديدة. ولكي تستطيع الشركات حماية نفسها، فإنها بحاجة إلى اتباع منهجية استباقية مع الحرص على التحسين المستمر لأدوات الأمن لديها؛ لتتمكن من مقاومة بيئة التهديدات دائمة التغير. والطريقة الوحيدة لمواكبة هذه التغييرات هي تطوير برنامج فعَّال للمعلومات المتعلقة بالتهديدات.

أصبحت المعلومات المتعلقة بالتهديدات بالفعل إحدى العناصر الرئيسية في عمليات الأمن التي تتم في الشركات بمختلف الأحجام في كل الصناعات والبلاد. فهي تتوفر في صيغ يمكن قراءتها واستخدامها بشكل بشري وآلي على حدٍّ سواء، وبهذا يتاح للمعلومات المتعلقة بالتهديدات دعم فرق الأمن بمعلومات مفيدة طوال عملية إدارة الحوادث وكذلك الإمداد بما يفيد في اتخاذ قرارات استراتيجية بناءً على معلومات وبيانات حديثة (الشكل 1).

وبرغم ذلك، أسهم الطلب المتنامي على المعلومات المتعلقة بالتهديدات الخارجية في زيادة وفرة موردي المعلومات المتعلقة بالتهديدات؛ حيث يوفر كل مورد مجموعة من الخدمات المختلفة. وجود سوق واسع وتنافسي مع خيارات لا حصر لها ومعقدة يمكن أن يشعرك بالارتباك والحيرة في اختيار الحل المناسب لمؤسستك.



الشكل 1
عمليات الأمن المبنية على المعلومات المتعلقة بالتهديدات

المعلومات المتعلقة بالتهديدات غير المخصصة لظروف شركتك يمكن أن تضرك بدلاً من إفادتك ويمكن أن تفاقم من سوء الموقف! مسؤولو التحليل الأمني في العديد من الشركات اليوم يقضون أكثر من نصف وقتهم في تصنيف التحذيرات الإيجابية الزائفة بدلاً من المقاومة الاستباقية للتهديدات والاستجابة لها مما يؤدي إلى زيادة كبيرة في وقت الاكتشاف. يؤدي إمداد فريق الأمن لديك بمعلومات غير مفيدة أو غير دقيقة إلى زيادة عدد التحذيرات الزائفة ويكون له تأثير سلبي خطير في قدرات الاستجابة والأمن العام لشركتك.

بيئة ازدهار المعلومات المفيدة...

كيف يمكن إذًا تقييم المصادر المتنوعة للمعلومات المتعلقة بالتهديدات وتحديد الأكثر صلة بمؤسستك من بينها ومن ثم تطبيقها بفاعلية؟ كيف يمكنك الانتقال بين الكميات الضخمة للمعلومات المتعلقة بالبيانات التي يسوق لها الموردون مع ادعاء كل مورد أن ما يوفره من معلومات هو الأفضل؟

من المهم أن تجيب عن هذه الأسئلة كي تحقق أقصى استفادة، لكن لا يجب أن تكون أول ما يدور في بالك. تنجذب العديد من المنظمات للرسائل المغرية والعروض الواعدة من الموردين الخارجيين الذين يدعون قدرتهم على توفير معلومات ستقفز بالشركة للأمام وترفع من مستواها كثيرًا، متناسين حقيقة أن معظم المعلومات القيمة توجد داخل شبكة الشركة نفسها...

يمكن للبيانات المستخرجة من أنظمة اكتشاف عمليات التسلل والوقاية منها وجدار الحماية وسجلات التطبيقات وسجلات وحدات التحكم في الأمن الأخرى أن تكشف الكثير عمَّا يحدث داخل شبكة الشركة. يمكن لهذا أن يحدد أنماط الأنشطة الضارة للمؤسسة، ويمكنه أن يميز بين المستخدم العادي وسلوك الشبكة ومن ثم يساعد في المحافظة على مسار ثابت لنشاط الوصول إلى البيانات.

الشكل 2

الاستفادة من المصادر الخارجية للمعلومات المتعلقة بالتهديدات

فكر بطريقة المهاجمين

لتطوير برنامج فعَّال من المعلومات المتعلقة بالتهديدات، يجب على جميع الشركات -بما في ذلك الشركات التي لديها بالفعل مراكز لإدارة العمليات الأمنية- أن تضع نفسها مكان المهاجم وتفكر مثله كي تستطيع تحديد الأهداف المحتملة وحمايتها. استخراج قيمة حقيقية من برنامج معلومات متعلقة بالتهديدات يتطلب فهمًا واضحًا تمامًا وتحديدًا للأصول المهمة ومجموعات البيانات وعمليات الأعمال الضرورية لتحقيق أهداف المؤسسة. تحديد هذه الأساسيات المهمة يتيح للشركات تأسيس نقاط لجمع البيانات من حولها ومن ثم إثراء البيانات التي يتم جمعها بمعلومات متعلقة بالتهديدات متوفرة من مصادر خارجية. بالنظر إلى الموارد المحدودة التي تكون موجودة في العادة لدى أقسام أمن المعلومات، فإن تحديد سمات مؤسسة بأكملها مهمة صعبة. لذلك؛ فإن الحل هو اتباع منهجية مبنية على المخاطر والتركيز على الأهداف الأسرع تأثرًا أولًا.

بمجرد تحديد المصادر الداخلية للمعلومات المتعلقة بالتهديدات وإدخالها في نظام العمل، يمكن للشركة أن تبدأ بالتفكير في إضافة معلومات خارجية في تدفقات العمل الموجودة.

الثقة هي الأساس

تتنوع المصادر الخارجية للمعلومات المتعلقة بالتهديدات في مستويات ثقتها:

من بين الخيارات الجيدة التي يمكن البدء بها الوصول إلى مجتمعات تشارك معلومات خاصة بصناعة معينة، ومن أمثلة هذا مركز تبادل معلومات الخدمات المالية وتحليلها (FS-ISAC). توفر هذه المجتمعات معلومات قيمة من مصادر خارجية، على الرغم من أنها غالبًا ما تكون مغلقة على أعضائها ويجب الاشتراك فيها للوصول إليها

توجد مصادر مفتوحة متاحة مجانًا لكنها غالبًا ما تفتقد إلى السياق ومن ثم تتسبب في ظهور عدد كبير من النتائج الإيجابية الزائفة

تتميز المصادر التجارية للمعلومات المتعلقة بالتهديدات بأنها أكثر اعتمادًا وموثوقية على الرغم من ارتفاع ثمن الوصول إليها في بعض الأحيان

المبدأ الأساسي لاختيار المصادر الخارجية للمعلومات المتعلقة بالتهديدات يجب أن يكون الجودة وليس الكم. قد تعتقد بعض المؤسسات أنه كلما زادت مصادر المعلومات المتعلقة بالتهديدات التي يمكن دمجها زاد معها نسبة الاستفادة مما يحصلون عليها. قد يكون هذا حقيقيًّا في بعض المواقف، مثال ذلك أن تكون المعلومات قادمة من مصادر موثوقة للغاية وبعضها مصادر مدفوعة، بشرط أن تكون المعلومات المتعلقة بالتهديدات مخصصة للمؤسسة واحتياجاتها والتهديدات التي تتعرض لها. في غير هذه الحالات، ثمة مخاطرة كبيرة في إمداد العمليات الأمنية في شركتك بمعلومات غير مرتبطة بمجالك.

يمكن أن يكون التداخل بين المعلومات التي يوفرها موردو المعلومات المتعلقة بالتهديدات صغيرًا جدًّا، كما أن الرؤى التي يوفرونها ستكون متفردة في أوجه معينة؛ وذلك لأن مصادرهم للمعلومات وطرق جمعهم لها تختلف وتتباين. على سبيل المثال: أحد الموردين بسبب وجوده الدائم في منطقة معينة فإنه يوفر تفاصيل أكثر عن التهديدات الناشئة عن تلك المنطقة، بينما يتمكن مورد آخر من توفير تفاصيل أكثر عن أنواع معينة من التهديدات. ومن ثم؛ فإن الوصول إلى كلٍّ من نوعي المصادر قد يكون مفيدًا، فعند الاعتماد عليهما معًا، يمكنها مساعدتك على رؤية الصورة الكاملة من زاوية أوضح والتصرف بكفاءة أعلى في اكتشاف التهديدات والاستجابة للحوادث. فقط ضع في حسبانك أن هذه الأنواع من المصادر الموثوق بها تتطلب تقييمًا مسبقًا وحذرًا لضمان أن المعلومات التي ستتوفر لك مناسبة لاحتياجات مؤسستك وأنها تعتمد على أمور منطقية، مثل عمليات الأمن والاستجابة للحوادث وإدارة المخاطر وإدارة نقاط الضعف وإدارة التطوير، وما إلى ذلك.

هناك أمور يجب أخذها في الاعتبار عند تقييم عروض المعلومات المتعلقة بالتهديدات المدفوعة

حتى الآن لا يوجد منهجية واضحة لتقييم العروض المدفوعة المختلفة للمعلومات المتعلقة بالتهديدات، لكن إليك بعض الأمور التي يجب أن تكون على دراية بها عند محاولة التقييم بنفسك:

إذا كنت تبحث عن محتوى أكثر استراتيجية لمعرفة خطة الأمن الطويلة المدى وما إلى ذلك:

- عرض عالي المستوى لاتجاهات الهجمات
- التقنيات والأساليب التي يستخدمها المهاجمون
- التحفيزات
- السمات...

البحث عن مورد معلومات متعلقة بالتهديدات له سجل مثبت في الكشف المستمر للتهديدات المعقدة والتحقيق فيها في منطقتك أو صناعتك. قدرة المورد على تخصيص قدراته البحثية وفق احتياجات شركتك أمر في غاية الأهمية كذلك

ابحث عن المعلومات ذات الوصول العالمي. ليس للهجمات حدود، فيمكن شن هجمة تستهدف شركة في أمريكا الجنوبية من أوروبا والعكس صحيح. هل يعمل المورد على توريد المعلومات عالميًا ويجمع أنشطة تبدو مفككة في حملات متماسكة ومتناغمة؟ سيساعدك هذا النوع من المعلومات على اتخاذ الإجراءات المناسبة

السياق يجمع المعلومات المتعلقة من البيانات المجردة. ليس لمؤشرات التهديدات التي لا تتضمن سياقًا أي قيمة تذكر، بل يجب أن تبحث عن موردين يساعدونك على الإجابة عن السؤال المهم: "لماذا تعد هذه المعلومات مهمة؟". يوفر سياق العلاقة (مثل المجالات المرتبطة بعناوين IP المكتشفة أو روابط URL التي تم تحميل الملفات المحددة منها وما إلى ذلك) قيمة إضافية ترفع من كفاءة التحقيق في الحوادث وتدعم "إدارة" الحوادث على نحو أفضل من خلال كشف مؤشرات الاختراق التي تم الحصول عليها حديثًا في الشبكة

من المفترض أن تتوفر بشركتك بعض قواعد التحكم في الأمان المطبقة بالفعل مع تحديد العمليات المرتبطة بها، وهذا أمر مهم لك كي تستطيع الاستفادة من المعلومات المتعلقة بالتهديدات باستخدام الأدوات التي تستخدمها وتعرفها بالفعل. ومن ثم؛ يجب أن تبحث عن مصادر وآليات تكامل وتنسيقات للمعلومات تدعم التكامل السلس للمعلومات المتعلقة بالتهديدات في عمليات الأمن الحالية

الخاتمة

ولهذا السبب فإننا في **Kaspersky** نركز على أبحاث التهديدات منذ أكثر من عقدين من الزمان، ونعمل على دعمك بأحدث المعلومات المتعلقة بالتهديدات من جميع أنحاء العالم مع كميات هائلة من بيانات التهديدات الغنية وتقنيات التعلّم الآلي المتقدمة ومجموعة فريدة من الخبراء العالميين، لمساعدتك على البقاء آمنًا من الهجمات الإلكترونية غير المعهودة سابقًا.

www.kaspersky.com