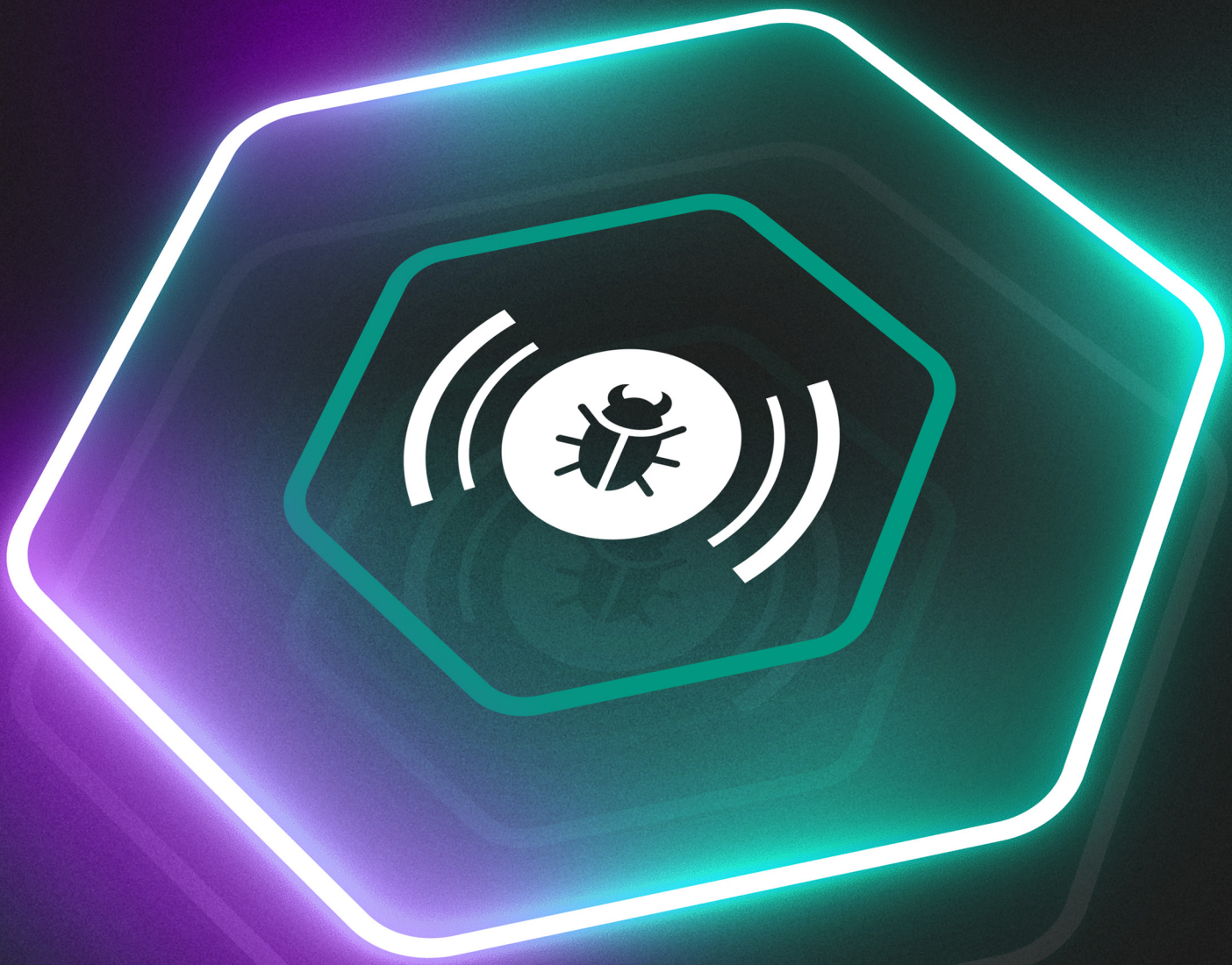


موجزات بيانات التهديدات من Kaspersky

kaspersky واجهوا المستقبل بأمان

موجزات بيانات التهديدات من Kaspersky

تحدث الهجمات الإلكترونية كل يوم. وهي لا تتوقف عن النمو والازدياد في التعقيد والغموض مع ظهور محاولات جديدة كل يوم لاختراق أنظمة الحماية لديك. يستخدم أعداؤك حاليًا سلاسل قتل تطفلية معقدة وحملات وتكتيكات وتقنيات وإجراءات مخصصة (TTP) من أجل تعطيل أعمالك أو الإضرار بعملائك. أضحى جليًّا الآن أن الحماية تتطلب أساليب جديدة تعتمد على المعلومات المتعلقة بالتهديدات.

من خلال دمج المعلومات المتعلقة بالتهديدات الحديثة والتي تحتوي على بيانات عن عناوين IP وروابط URL وملفات التجزئة الخطيرة والمشبوهة في أنظمتك الأمنية مثل منصات معلومات الأمان وإدارة الأحداث وتنسيق الأمان والأتمتة والاستجابة ومعلومات التهديدات، يمكن للفرق الأمنية أتمتة عملية فرز التحذيرات الأولية، مع تزويد المتخصصين في الفرز بسياق كافٍ لتحديد الإنذارات التي يجب التحقيق فيها أو تصعيدها إلى فرق الاستجابة للحوادث بشكل فوري لكي يتم إجراء مزيد من التحقيق والاستجابة.

البيانات السياقية

يتم إثراء كل سجل في كل موجز بيانات بسياق قابل للتطبيق (أسماء التهديدات التي تم تحليلها لموارد الويب IP والطوابع الزمنية والموقع الجغرافي وعناوين المصابة بالفيروسات وملفات التجزئة والانتشار وما إلى ذلك). وتساعد البيانات السياقية على كشف "الصورة الكبرى" مما يؤدي كذلك إلى التحقق من صحة البيانات ودعم استخدامها على نطاق واسع. وعند وضع هذه البيانات في سياق، يمكن استخدامها بسهولة أكبر للإجابة عن أسئلة من وماذا وأين ومتى التي تؤدي إلى التعرف على خصومك، ما يساعدك على اتخاذ قرارات وإجراءات سريعة.

أهم الميزات

الجمع والمعالجة

يتم جمع موجزات البيانات من مصادر متكاملة ومتنوعة وموثوقة للغاية، مثل **Kaspersky Security Network** وأدوات تتبع الويب ونظام مراقبة شبكة بوت نت (مراقبة شبكات بوت نت وأهدافها وأنشطتها على مدار الساعة طيلة أيام الأسبوع طوال أيام السنة) ومصائد البريد العشوائي وفرق البحث وشركائنا.

بعد ذلك يتم، في الوقت نفسه، فحص كل البيانات المجمعة بعناية وتنقيحها باستخدام أساليب معالجة مسبقة متعددة، مثل المعايير الإحصائية وبيئات الاختبار المعزولة والمحركات التجريبية وأدوات التشابه وتنميط السلوك والتحقق من أدوات التحليل والتحقق من قوائم السماح.

يتم إنشاء موجزات البيانات تلقائيًا في الوقت الفعلي بناءً على النتائج في جميع أنحاء العالم (توفر **Kaspersky Security Network** رؤية لنسبة مهولة من كل عمليات المرور الداخلية التي تغطي عشرات الملايين من المستخدمين النهائيين في أكثر من 213 بلدًا)، ما يوفر معدلات اكتشاف عالية ودقة كبيرة

سهولة التطبيق. مستندات تكميلية وعينات ومدير حساب تقني مخصص ودعم تقني من **Kaspersky**، تجتمع كلها لتفعيل التكامل المباشر

تُعد موجزات البيانات الممتلئة بالنتائج الإيجابية الزائفة لا قيمة لها، لذلك يتم تطبيق اختبارات وعوامل تصفية شاملة وصارمة للغاية قبل إطلاق الموجزات لضمان تقديم بيانات تم فحصها بنسبة 100%

تنسيقات توزيع خفيفة وبسيطة (**JSON** و**CSV** و**OpenIoC** و**STIX**) عبر بروتوكول **HTTPS** أو **TAXII** أو آليات تسليم مخصصة تدعم التكامل السهل للموجزات في حلول الأمن.

مئات الخبراء، يتضمنون محللي أمن من جميع أنحاء العالم وخبراء أمن على أعلى مستوى في العالم من **GReAT** وفرق متخصصة في البحث والتطوير للمساهمة في إنشاء هذه الموجزات. يستقبل مسؤولو الأمن المعلومات المهمة والإنذارات التي تنشأ عن البيانات ذات أعلى جودة من دون التعرض لخطر استقبال المؤشرات والتحذيرات غير الضرورية.

يتم إنشاء كل الموجزات ومراقبتها من خلال بنية تحتية تتسامح مع الأخطاء، ما يضمن التوفر المستمر

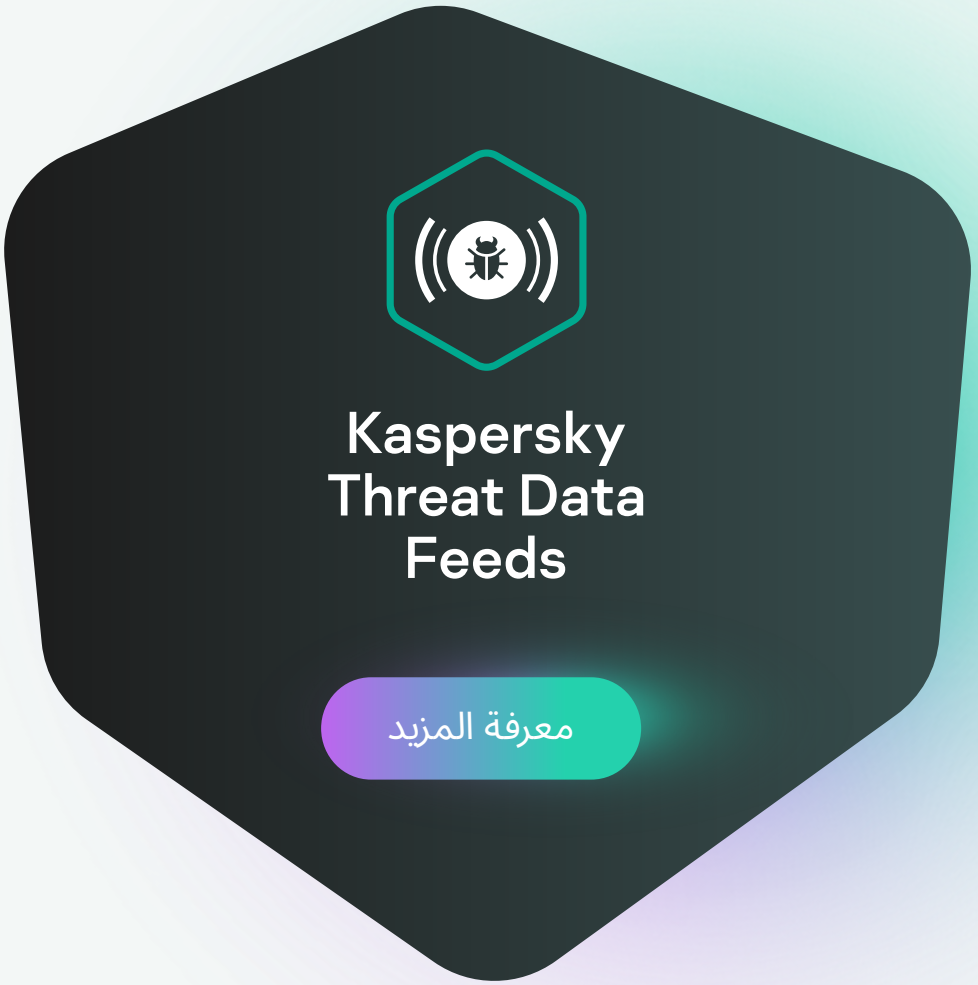
الفوائد

منع تسرب الأصول الحساسة وحقوق الملكية الفكرية من الأجهزة المصابة بالفيروسات إلى خارج المؤسسة. اكتشاف الأصول المصابة بالفيروسات بسرعة لحماية سمعة علامتك التجارية، ما يساعد على الحفاظ على مزايا المنافسة وتأمين فرص الأعمال

تحسين الاستجابة للحوادث والقدرات التحليلية من خلال أتمتة عملية الفرز الأولية مع تزويد محللي الأمن بسياق كافٍ لتحديد الإنذارات فورًا التي يلزم التحقيق فيها أو تصعيدها إلى فرق الاستجابة للحوادث لإجراء مزيد من التحقيقات والاستجابة

تقوية حلول الدفاع عن الشبكة لديك، ويشمل هذا معلومات الأمن وإدارة الأحداث وجدران الحماية وأنظمة منع التسلل/أنظمة منع التطفل (**IPS/IDS**) ووكيل الأمن وحلول نظام أسماء النطاقات (**DNS**) ومكافحة التهديدات المستعصية المتقدمة مع مؤشرات اختراق محدثة (**IOC**) باستمرار وسياق قابل للتطبيق، ما يوفر معرفة معمقة بالهجمات الإلكترونية وفهمًا أكبر لنوايا أعدائك وقدراتهم وأهدافهم. إلى جانب ذلك، تُعد أنظمة أمن المعلومات وإدارة الأحداث الرائدة (مثل **HP ArcSight** و**IBM QRadar** و**Splunk** وما إلى ذلك) ومنصات معلومات التهديد مدعومة بالكامل

بصفتنا موردًا لخدمات الأمن المدارة (**MSSP**)، نعمل على تطوير شركتك من خلال توفير معلومات متعلقة بالتهديدات رائدة في مجالك بصفتها خدمة مميزة لعملائك. بصفتنا فريق استجابة لطوارئ الكمبيوتر (**CERT**)، نعمل على تحسين اكتشاف التهديدات الإلكترونية وقدرات التحديد لديك وتطويرها



www.kaspersky.com