تقارير حول معلومات التهديدات المستعصية المتقدمة من Kaspersky

kaspersky واجهوا المستقبل بأمان

تقارير حول معلومات التهديدات المستعصية المتقدمة من Kaspersky

يحصل العملاء الذين يستخدمون خدمة إعداد تقارير معلومات التهديدات المستعصية المتقدمة من **Kaspersky** على وصول مستمر وفريد إلى تحقيقاتنا واكتشافاتنا، بما في ذلك البيانات الفنية الكاملة (في مجموعة من التنسيقات) الخاصة بكل تهديد من التهديدات المستعصية المتقدمة بمجرد اكتشافه بالإضافة إلى كل التهديدات التي لن يتم الإفصاح عنها أبدًا. بالنسبة إلى التقارير التي تحتوي على ملخص تنفيذي موجه إلى الشركات ويتضمن معلومات يسهل استيعابها وتصف التهديدات المستعصية المتقدمة ذات الصلة مع تقديم وصف فني مفصل للتهديدات المستعصية المتقدمة ومؤشرات الاختراق ذات الصلة وقواعد **YARA** لمنح الباحثين في مجال الأمن ومحللي البرامج الضارة ومهندسي الأمن ومحللي أمن الشبكة والباحثين في مجال التهديدات المستعصية المتقدمة بيانات قابلة للتنفيذ تتيح الاستجابة السريعة والدقيقة للتهديدات.

سيقوم خبراؤنا أيضًا بتنبيهك فورًا بأي تغييرات يكتشفونها في أساليب المجموعات الإجرامية عبر الإنترنت. سيمكنك أيضًا الوصول إلى قاعدة البيانات الخاصة بتقارير التهديدات المستعصية المتقدمة الكاملة من **Kaspersky**، وهي مكون بحثي وتحليلي قوي آخر في أنظمة الحماية الأمنية لديك.

الفوائد

الوصول المتميز
احصل على مواصفات فنية حول أحدث التهديدات أثناء التحقيقات المستمر قبل إطلاقها للجمهور العام

معلومات حول التهديدات المستعصية المتقدمة غير المعلنة
لأسباب متنوعة، لا يتم الإعلان عن كل التهديدات عالية الخطورة للجمهور العام. ولكننا نشاركها مع كل عملائنا

MITRE ATT&CK
تم تصميم جميع التكتيكات والتقنيات والإجراءات الموصوفة في التقارير لإطار MITRE ATT&CK، ما يزيد من تحسين الاكتشاف والاستجابة من خلال التطوير وترتيب الأولويات لحالات استخدام المراقبة الأمنية المقابلة، وإجراء تحليلات للفجوات واختبار الأساليب الدفاعية الحالية ضد التكتيكات والتقنيات والإجراءات ذات الصلة

ملفات تعريف الجهات التي تشن التهديدات
بما في ذلك بلد المنشأ المشكوك فيه والنشاط الأساسي وعائلات البرمجيات الضارة المستخدمة والصناعات والمناطق الجغرافية المستهدفة ووصف جميع التكتيكات والتقنيات والإجراءات المستخدمة، مع تخطيط لإطار MITRE ATT&CK

الوصول إلى البيانات الفنية
بما في ذلك قائمة موسَّعة بمؤشرات الاختراق، المتوفرة بتنسيقات قياسية تتضمن openIOC أو STIX، والوصول إلى قواعد Yara

التحليل الاستعادي
الوصول إلى كل التقارير الخاصة التي تم إصدارها سابقًا خلال فترة اشتراكك

واجهة برمجة التطبيقات RESTful
تكامل سلس لسير عمليات الأمن وإضافة سمة الأتمتة عليها بسهولة

المراقبة المستمرة لحملات التهديدات المستعصية المتقدمة
قم بالوصول إلى المعلومات القابلة للتنفيذ أثناء التحقيقات (معلومات حول توزيع التهديدات المستعصية المتقدمة ومؤشرات الاختراق والبنيات التحتية للأوامر والتحكم، وما إلى ذلك

www.kaspersky.com