Kaspersky Cloud Sandbox

واجهوا المستقبل بأمان kaspersky

Kaspersky Cloud Sandbox

من المستحيل منع التهديدات المستهدفة في عصرنا الحالي باستخدام أدوات مكافحة الفيروسات التقليدية فقط فمحركات تطبيقات مكافحة الفيروسات تستطيع إيقاف التهديدات المعروفة ومشتقاتها فقط، بينما تستخدم الجهات التي تشن التهديدات المعقدة جميع الوسائل الممكنة والمتوفرة لديها في تجنب الاكتشاف الآلي. تستمر الخسائر الناتجة عن حوادث أمن المعلومات في النمو بصورة كبيرة، ما يسلط الضوء على الأهمية المتزايدة لقدرات اكتشاف التهديدات فورًا لضمان سرعة الاستجابة والتغلب على التهديدات قبل وقوع أي ضرر خطير.

يُعد اتخاذ قرار مدروس بناءً على سلوك ملفٍ ما مع العمل في الوقت نفسه على تحليل ذاكرة العمليات وأنشطة الشبكات وما إلى ذلك، النهج المثالي لفهم التهديدات الحالية بما فيها من تعقيد واستهداف وتخصيص حسب كل مؤسسة. قد تفتقر البيانات الإحصائية إلى المعلومات عن البرمجيات الضارة المعدلة حديثًا، لكن تقنيات العزل والفحص تمثل أدوات قوية تتيح إجراء عمليات فحص للملفات ومصادرها وجمع مؤشرات الاختراق بناءً على التحليل السلوكي واكتشاف الكائنات الخبيثة التي لم تكن ملحوظة من قبل.

واجهة الويب

واجهة برمجة التطبيقات RESTfull

الإعدادات الافتراضية والمتقدمة لأفضل أداء

تحليل متقدم للملفات بتنسيقات مختلفة

Kaspersky Cloud Sandbox

إعداد التقارير المصورة والحسية

تقنيات متقدمة لمكافحة التهرب والمحاكاة البشرية

اكتشاف متقدم للتهديدات المستعصية المتقدمة والتهديدات المستهدفة والمعقدة

تدفق عمل يتيح إجراء تحقيق عالي الكفاءة وشاملاً للحوادث

قابلية التوسع، من دون الحاجة إلى شراء أجهزة غالية الثمن

تكامل سلس لعمليات الأمن وإضافة سمة الأتمتة عليها بسهولة

التقارير الشاملة

- تحميل وتشغيل ملفات DLL
- اتصالات خارجية مع أسماء النطاقات وعناوين IP
- إنشاء الملفات وتعديلها وحذفها
- معلومات متعلقة بالتهديدات تفصيلية مع سياق قابل للتطبيق لكل مؤشر اختراق مكتشف
- نفايات سير العمليات ونفايات مرور الشبكة (PCAP)
- طلبات HTTP وDNS والاستجابة لها
- إنشاء امتدادات مشتركة
- واجهة برمجة التطبيقات RESTful
- مفاتيح السجل التي تم إنشاؤها وتعديلها
- عمليات من إنشاء الملف الذي تم تنفيذه
- لقطات الشاشة
- **وغيرها الكثير**

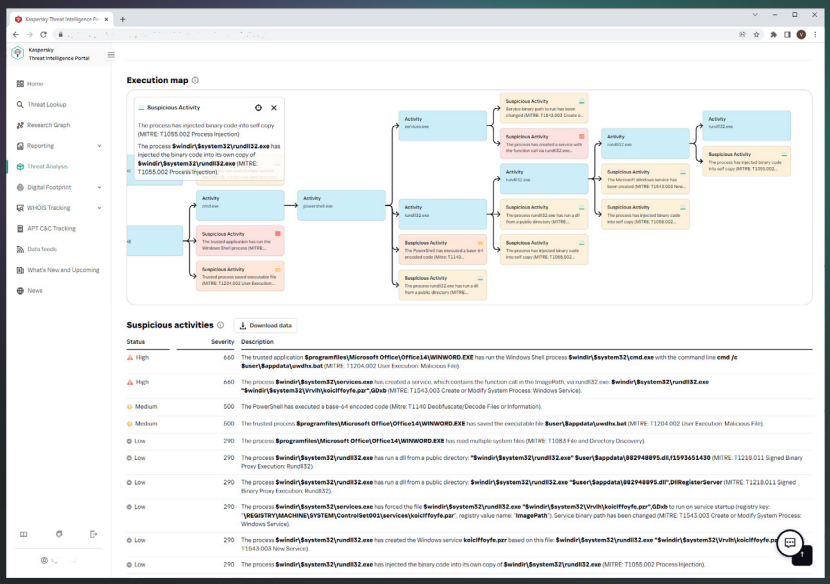
الاكتشاف الاستباقي للتهديدات والتخفيف منها

تستخدم البرامج الضارة مجموعة متنوعة من الطرق لتخفي إجراءاتها لمنع اكتشافها. إذا كان النظام لا يفي بالمعلمات المطلوبة، فإن البرنامج الضار سيدمر نفسه بلا شك مع عدم ترك أي أثر له. كي يتم تنفيذ الكود الضار، فإن بيئة العزل والفحص يجب أن تكون قادرة على محاكاة السلوك الطبيعي للمستخدم النهائي بدقة.

أداة **Kaspersky Cloud Sandbox** توفر منهجية مختلطة تجمع بين المعلومات المتعلقة بالتهديدات التي يتم جمعها من كميات مهولة من البيانات الإحصائية (باستخدام شبكة **Kaspersky Security Network** وغيرها من الأنظمة الحصرية لدينا) وتحليل سلوكي وحماية لا يمكن اختراقها ضد التسلل مع تقنيات محاكاة بشرية، مثل النقر الآلي وتصفح المستندات وعمليات وهمية.

تم تصميم هذا المنتج في معامل العزل في شركتنا وتطويره لأكثر من عقد من الزمان. تستفيد التقنية من كل معارفنا عن سلوكيات البرامج الضارة التي جمعناها على مدار أكثر من 20 عامًا من البحث المستمر على التهديدات. وهذا أتاح لنا اكتشاف أكثر من 360000 كائن ضار جديد كل يوم لتقديم حلول أمنية رائدة في هذا المجال لعملائنا.

وبصفتها جزءًا من بوابة المعلومات المتعلقة بالتهديدات، تُعد **Cloud Sandbox** المكون النهائي في سير عمل المعلومات المتعلقة بالتهديدات لديك. في حين توفر **Threat Lookup** أحدث المعلومات المتعلقة بالتهديدات التفصيلية عن روابط **URL** والمجالات وعناوين **IP** وتجزئات الملفات وأسماء التهديدات والبيانات الإحصائية/السلوكية وبيانات **WHOIS/DNS**، وما إلى ذلك، تتيح أداة **Cloud Sandbox** ربط المعرفة بمؤشرات الاختراق التي يتم إنشاؤها عبر العينة التي تم تحليلها.



يمكنك الآن إجراء تحقيقات في الحوادث شديدة الفعالية والتعقيد، ما يؤدي إلى الفهم الفوري لطبيعة التهديد، ثم وضع النقاط على الحروف وأنت تتعمّق لكشف مؤشرات التهديدات المترابطة.

يمكن أن يكون الفحص مكثفًا للموارد، لا سيما عندما يتعلق بالهجمات متعددة المراحل. تعزز **Kaspersky Cloud Research Sandbox** الاستجابة للحوادث لديك والأنشطة التحليلية، ما يوفر لك القدرة على قياس معالجة الملفات تلقائيًا من دون الحاجة إلى شراء تطبيقات غالية الثمن أو القلق بشأن موارد النظام.

www.kaspersky.com