Kaspersky Threat Intelligence

واجهوا المستقبل بأمان kaspersky

Kaspersky Threat Intelligence

تتيح لك خدمة المعلومات المتعلقة بالتهديدات من **Kaspersky** الوصول إلى المعلومات التي تحتاج إليها للحدّ من هذه التهديدات الإلكترونية، والتي يوفرها فريق من الباحثين والمحلّلين الرائدين عالميًا.

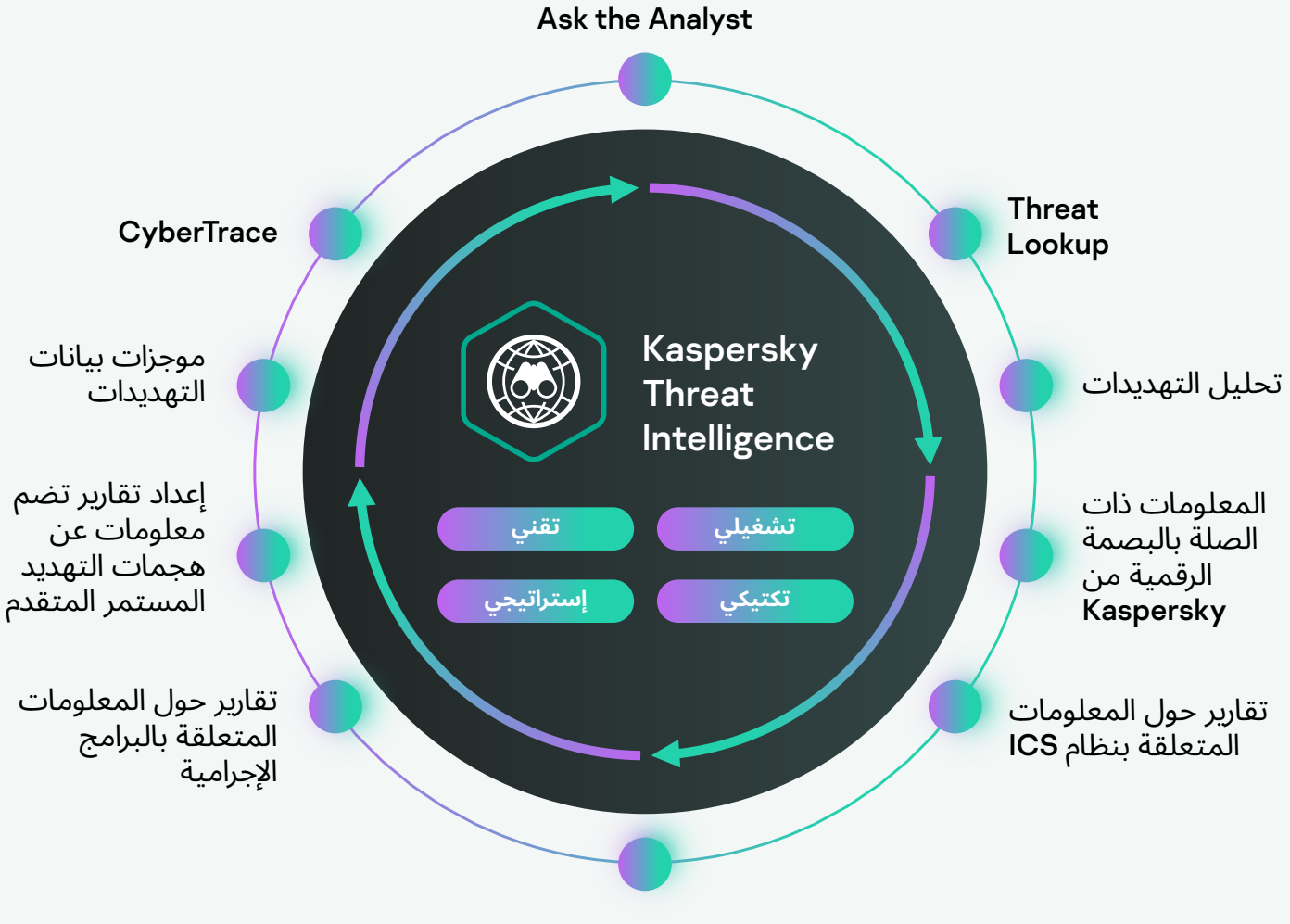
بفضل ما يتوفر لدى **Kaspersky Lab** من معرفة وخبرة ومعلومات شاملة تتعلق بكل جانب من جوانب الأمن الإلكتروني، أصبحت **Kaspersky Lab** الشريك الموثوق فيه لدى وكالات إنفاذ القانون والهيئات الحكومية المتميزة، بما فيها الإنتربول وفِرق التصدي للطوارئ الحاسوبية **(CERT)**. توفر لك خدمة المعلومات المتعلقة بالتهديدات من **Kaspersky** إمكانية الوصول الفوري إلى المعلومات التقنية والتكتيكية والتشغيلية والإستراتيجية المتعلقة بالتهديدات.

التحديات

يعد تعقب تهديدات أمن تكنولوجيا المعلومات وتحليلها وتفسيرها والحدّ منها باستمرار مهمة كبيرة. تواجه المؤسسات على مستوى كل القطاعات نقصًا في البيانات المحدّثة ذات الصلة التي تحتاج إليها لمساعدتها في إدارة المخاطر المرتبطة بتهديدات أمن تكنولوجيا المعلومات.

تتضمن مجموعة المعلومات المتعلقة بالتهديدات من Kaspersky ما يلي

موجزات بيانات التهديد و**CyberTrace** (منصة معلومات متعلقة بالتهديد) و**Threat Lookup** وخدمة تحليل التهديدات (محرك **Cloud Sandbox** و**Cloud Threat Attribution**) ومجموعة من خيارات إعداد تقارير المعلومات المتعلقة بالتهديدات وخدمات توفير خبرات المعلومات المتعلقة بالتهديدات عند الطلب.



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 والطوابع الزمنية والموقع الجغرافي وعناوين IP التي تم تحليلها لموارد الويب 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

Kaspersky CyberTrace

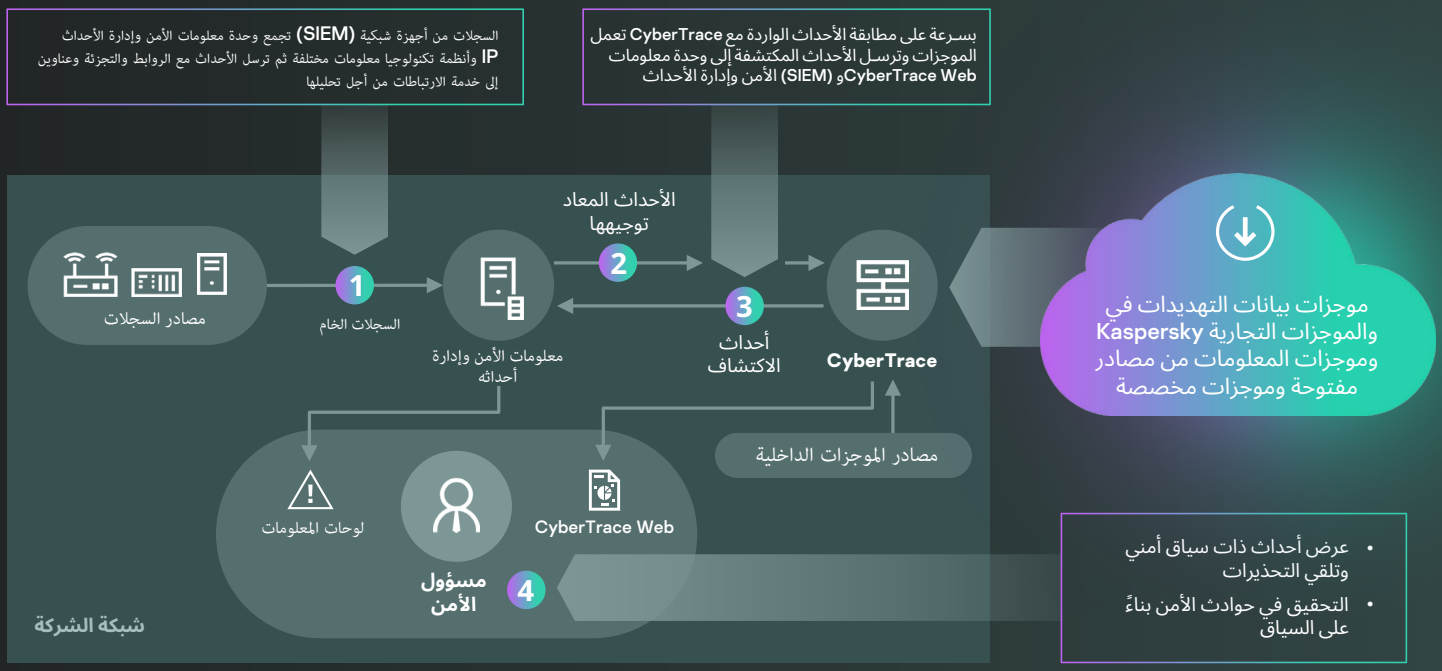
من خلال دمج المعلومات المتعلقة بالتهديدات الحديثة والقابلة للقراءة آليًا في عناصر التحكم في الأمن الحالية، مثل أنظمة معلومات الأمن وإدارة الأحداث (SIEM)، يمكن أن تقوم مراكز عمليات الأمن بأتمتة عملية الفرز الأولية مع توفير سياق كافٍ لمحللي الأمن ليتمكنوا من تحديد التنبيهات التي يجب التحقيق فيها أو تصعيدها إلى فرق الاستجابة للحوادث للتحقيق فيها بشكل إضافي والاستجابة لها. لكن النمو المستمر والمتزايد في عدد موجزات بيانات التهديدات ومصادر المعلومات المتعلقة بالتهديدات المتوفرة تجعل من الصعب على المؤسسات أن تحدد المعلومات المفيدة لهم من غير المفيدة! يتم توفير المعلومات المتعلقة بالتهديدات في تنسيقات مختلفة وتتضمن عددًا كبيرًا من مؤشرات الاختراق، ما يصعّب على وحدات معلومات الأمن وإدارة الأحداث أو عناصر التحكم في أمن الشبكة استيعابها.

Kaspersky CyberTrace عبارة عن منصة معلومات متعلقة بالتهديدات تتيح دمج موجزات بيانات التهديدات بسلاسة في حلول معلومات الأمن وإدارة الأحداث (SIEM) لمساعدة المحللين على الاستفادة من المعلومات المتعلقة بالتهديدات في سير عمل العمليات الأمنية لديهم بفعالية أكبر. يمكن لهذه المنصة أن تندمج مع أي موجز للمعلومات المتعلقة بالتهديدات (من **Kaspersky** أو الموردين الآخرين أو معلومات المصادر المفتوحة أو موجزات العملاء لديك) بصيغة **JSON** أو **STIX** أو **XML** أو**CSV**، وأن تدعم التكامل الفريد مع عدد كبير من حلول معلومات الأمن وإدارة الأحداث ومصادر السجلات.

توفر منصة **Kaspersky CyberTrace** مجموعة من الأدوات لاستخدام المعلومات المتعلقة بالتهديدات بفعالية وتتضمن ما يلي:

- قاعدة بيانات تتضمن مؤشرات ذات إمكانية البحث عن نصوص كاملة والبحث باستخدام استعلامات البحث المتقدمة لتوفير إمكانية إجراء عمليات بحث معقدة عبر كل حقول المؤشرات، بما فيها حقول السياق
- توفّر الصفحات التي تحتوي على معلومات مفصّلة حول كل مؤشر تحليلاً أعمق. تعرض كل صفحة كل المعلومات المتعلقة بأحد المؤشرات من كل مزوّدي المعلومات المتعلقة بالتهديدات (مسح البيانات المكررة) ليتمكّن المحللون من مناقشة التهديدات في التعليقات وإضافة معلومات داخلية متعلقة بالتهديدات حول المؤشر
- رسمًا بيانيًا بحثيًا يسمح باستكشاف البيانات وعمليات الاكتشاف المخزنة في **CyberTrace** بصورة مرئية واكتشاف علامات التهديد
- تقوم ميزة تصدير المؤشرات بدعم تصدير مجموعات المؤشرات إلى وحدات التحكم في الأمن، مثل قوائم السياسات (قوائم الحظر)، بالإضافة إلى مشاركة بيانات التهديدات بين عمليات **Kaspersky CyberTrace** أو مع الأنظمة الأساسية الأخرى للمعلومات المتعلقة بالتهديدات.
- ويبسط وضع علامات على مؤشرات الاختراق تلك الإدارة. وبوسع أي منا أن ينشئ أي علامة ويحدد وزنها (الأهمية) ويستخدمها في وضع العلامات على مؤشرات الاختراق يدويًا. ويمكنك كذلك فرز مؤشرات الاختراق وترشيحها بناءً على هذه العلامات وأوزانها
- تسمح لك ميزة الارتباط التاريخي (الفحص الرجعي) بتحليل العناصر التي تتم مراقبتها من الأحداث التي تم التحقق منها سابقًا باستخدام أحدث الموجزات للعثور على التهديدات المكشوفة سابقًا
- عامل تصفية يرسل أحداث الاكتشاف إلى حلول إدارة المعلومات وأحداث الأمان، ما يقلل الحمل عليها بالإضافة إلى المحللين
- تدعم ميزة تعدد البرامج موفري خدمات الأمن المدارة وحالات الاستخدام من قِبل المؤسسات الكبيرة
- تقوم إحصاءات استخدام الموجزات الخاصة بقياس فعالية الموجزات المتكاملة ومصفوفة تقاطع الموجزات بالمساعدة على اختيار المزوّدين الأكثر أهمية للمعلومات المتعلقة بالتهديدات
- تسمح لك **HTTP RestAPI** بالبحث عن المعلومات المتعلقة بالتهديدات وإدارتها

تستخدم الأداة عملية داخلية من التحليل والمطابقة للبيانات مما يقلل بشكل كبير من العبء على وحدة أمن المعلومات وإدارة أحداثه. تعمل أداة **Kaspersky CyberTrace** على تحليل السجلات والأحداث الجديدة وتطابق بسرعة بين البيانات الناتجة مع الموجزات التي لديها ومن ثم تنشئ تحذيراتها الخاصة عن اكتشاف التهديدات. يمكن الاطلاع على بنية عالية المستوى لتكامل الحل في الشكل أدناه:



مع Kaspersky CyberTrace وموجزات البيانات من Kaspersky، سيمكن للمحللين في مركز عمليات الأمن لديك القيام بما يلي:

- تنقيح الكميات المهولة من الإنذارات الأمنية وترتيبها من حيث الأولوية بكفاءة
- تحسين وتسريع عمليات الفرز والاستجابة الأوَّلية
- تحديد التحذيرات الخطيرة على المؤسسة بشكل فوري واتخاذ قرارات أكثر فائدة بناءً على معلومات حقيقية لمعرفة التحذيرات التي يجب تصعيدها إلى فرق الاستجابة للحوادث
- تشكيل آلية دفاعية استباقية ومبنية على المعلومات

Kaspersky Threat Lookup

ليس للجرائم الإلكترونية اليوم أي حدود، وتتحسن القدرات التقنية بسرعة: لقد لاحظنا أن الهجمات تزداد تعقيدًا مع قدرة المجرمين الإلكترونيين على استخدام موارد الإنترنت المظلم في تهديد الأشخاص المستهدفين. علاوة على ذلك، تزداد التهديدات الإلكترونية باستمرار من حيث تكرار حدوثها ومدى التعقيد والغموض مع ظهور محاولات جديدة كل يوم لاختراق أنظمة الحماية لديك. يستخدم المهاجمون سلاسل قتل معقدة وتكتيكات وتقنيات وإجراءات معقدة في حملاتهم لزعزعة أعمالك وسرقة أصولك أو التسبب في ضرر لعملائك.

توفر خدمة **Kaspersky Threat Lookup** كل المعارف التي اكتسبتها **Kaspersky** بشأن التهديدات الإلكترونية والعلاقات فيما بينها، والتي تم تجميعها معًا في خدمة ويب قوية واحدة. يتمثل الهدف من هذه الخدمة في توفير أكبر قدر ممكن من البيانات لفرق الأمن في شركتك كي يستطيعوا منع الهجمات الإلكترونية قبل وقوعها وتسببها في ضرر لمؤسستك. توفر لك المنصة أحدث المعلومات الدقيقة المتعلقة بالتهديدات فيما يتعلق بروابط **URL** والمجالات وعناوين **IP** وتجزئات الملفات وأسماء التهديدات والبيانات الإحصائية/السلوكية وبيانات **WHOIS/DNS** وسمات الملفات وبيانات الموقع الجغرافي وسلاسل التنزيل والطوابع الزمنية، وما إلى ذلك. النتيجة رؤية عالمية للتهديدات الجديدة والناشئة مما يساعد في تأمين مؤسستك وتقوية الاستجابة للحوادث.

أهم الميزات

التحقيقات في الحوادث: يعزز الشكل البياني التحقيقات في الحوادث من خلال تمكينك من استكشاف البيانات بصورة مرئية وعمليات الاكتشاف المخزنة في **Threat Lookup**. توفر عرضًا رسوميًا للعلاقة بين عناوين **URL** والمجالات وعناوين **IP** والملفات والسياقات الأخرى حتى يمكنك فهم النطاق الكامل لإحدى الحوادث وتحديد الأسباب الجذرية لها.

البحث عن التهديدات: خذ زمام المبادرة في مكافحة الهجمات واكتشافها والاستجابة لها لتقليل تأثيرها ومنع تكرار حدوثها. تعقب العناصر الهجومية وتخلص منها بأقصى سرعة ممكنة. كلما سارعت في اكتشاف التهديدات، قل الضرر الذي ينتج عنها وكانت الإصلاحات أسرع وتمكنت عمليات الشبكة من العودة إلى طبيعتها في أسرع وقت.

معلومات موثوقة: أكثر ما يميز خدمة **Kaspersky Threat Lookup** هو موثوقية بيانات المعلومات المتعلقة بالتهديدات لدينا الغنية بالسياق القابل للتطبيق. تُعد **Kaspersky** رائدة في مجال اختبارات مكافحة البرمجيات الضارة[1]، وتظهر جودة معلومات الأمن التي لا مثيل لها التي نوفرها من خلال تقديم أعلى مستويات الاكتشاف مع نسبة تحذيرات زائفة تقترب من الصفر

مجموعة كبيرة من تنسيقات التصدير: يمكن إصدار مؤشرات الاختراق أو السياق القابل للتطبيق في مجموعة من التنسيقات المستخدمة على نطاق واسع والأكثر تنظيمًا والقابلة للقراءة آليًا مثل **STIX** أو **OpenIOC** أو **JSON** أو **Yara** أو **Snort** أو **CSV** من أجل الاستمتاع بكامل مزايا المعلومات المتعلقة بالتهديدات أو أتمتة سير العمليات أو دمجها في التدابير الأمنية، مثل وحدات إدارة معلومات الأمان وأحداثه **(SIEM)**

واجهة ويب سهلة الاستخدام أو واجهة برمجة التطبيقات **RESTful**: استخدم الخدمة في الوضع اليدوي من خلال واجهة الويب **(عبر متصفح ويب)** أو قم بالوصول عبر واجهة برمجة التطبيقات **RESTful**؛ حسب تفضيلاتك.

البحث الرئيسي: ابحث عن المعلومات عبر كل منتجات معلومات التهديدات النشطة والمصادر الخارجية **(بما في ذلك مؤشرات اختراق التهديدات لمعلومات المصادر المفتوحة وشبكة الويب المظلمة وشبكة الويب السطحية)** في واجهة واحدة وقوية.

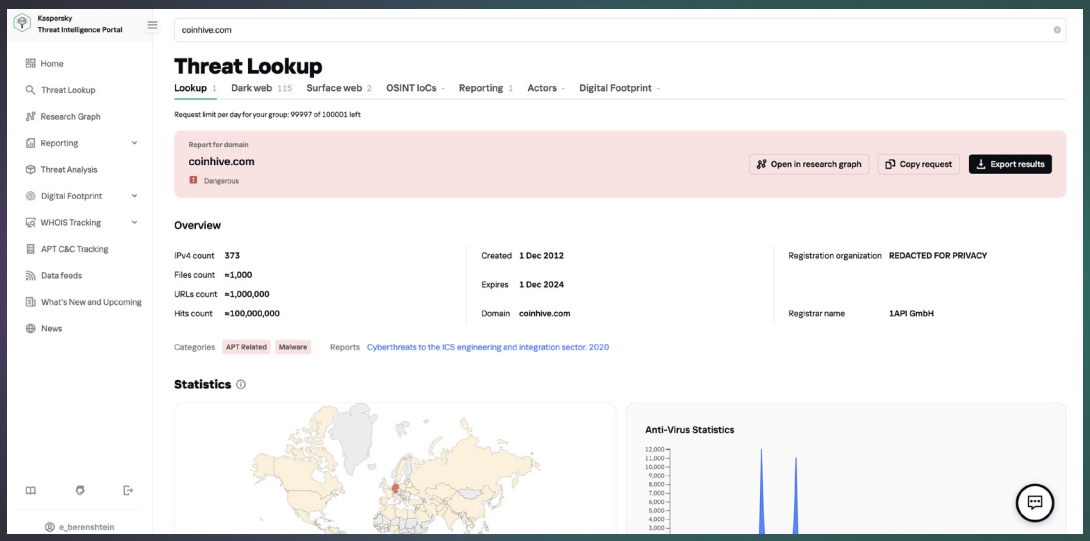
الفوائد

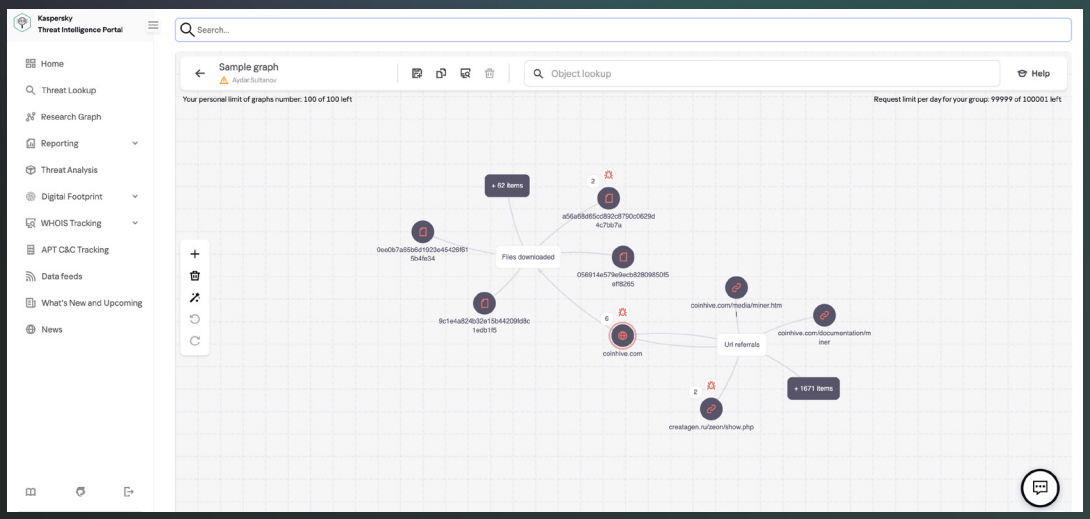
تعزيز مستويات الاستجابة للحوادث لديك من خلال إمكانات تقصي أثر التهديدات لتعطيل سلسلة التدمير قبل تعرض الأنظمة والبيانات المهمة للخطر

تشخيص وتحليل حوادث الأمن على المواقع المستضيفة والشبكة بكفاءة وفاعلية أعلى وترتيب أولوية الإشارات من الأنظمة الداخلية ضد التهديدات غير المعروفة

إجراء أبحاث معمقة عن مؤشرات الاختراق عبر سياق للتهديد تم التحقق منه بعناية كي يتيح لك ترتيب الهجمات من حيث الأولوية والتركيز على الحد من التهديدات التي تشكل الخطر الأكبر على شركتك

[1] kaspersky.com/top3





أصبح الآن بمقدورك

التحقق مما إذا كان الكائن المكتشف واسع الانتشار أم فريدًا من نوعه

الاستفادة من البيانات التفصيلية المتقدمة التي تشمل الشهادات أو الأسماء شائعة الاستخدام أو مسارات الملفات أو روابط **URL** ذات الصلة لاستكشاف الكائنات المشبوهة الجديدة

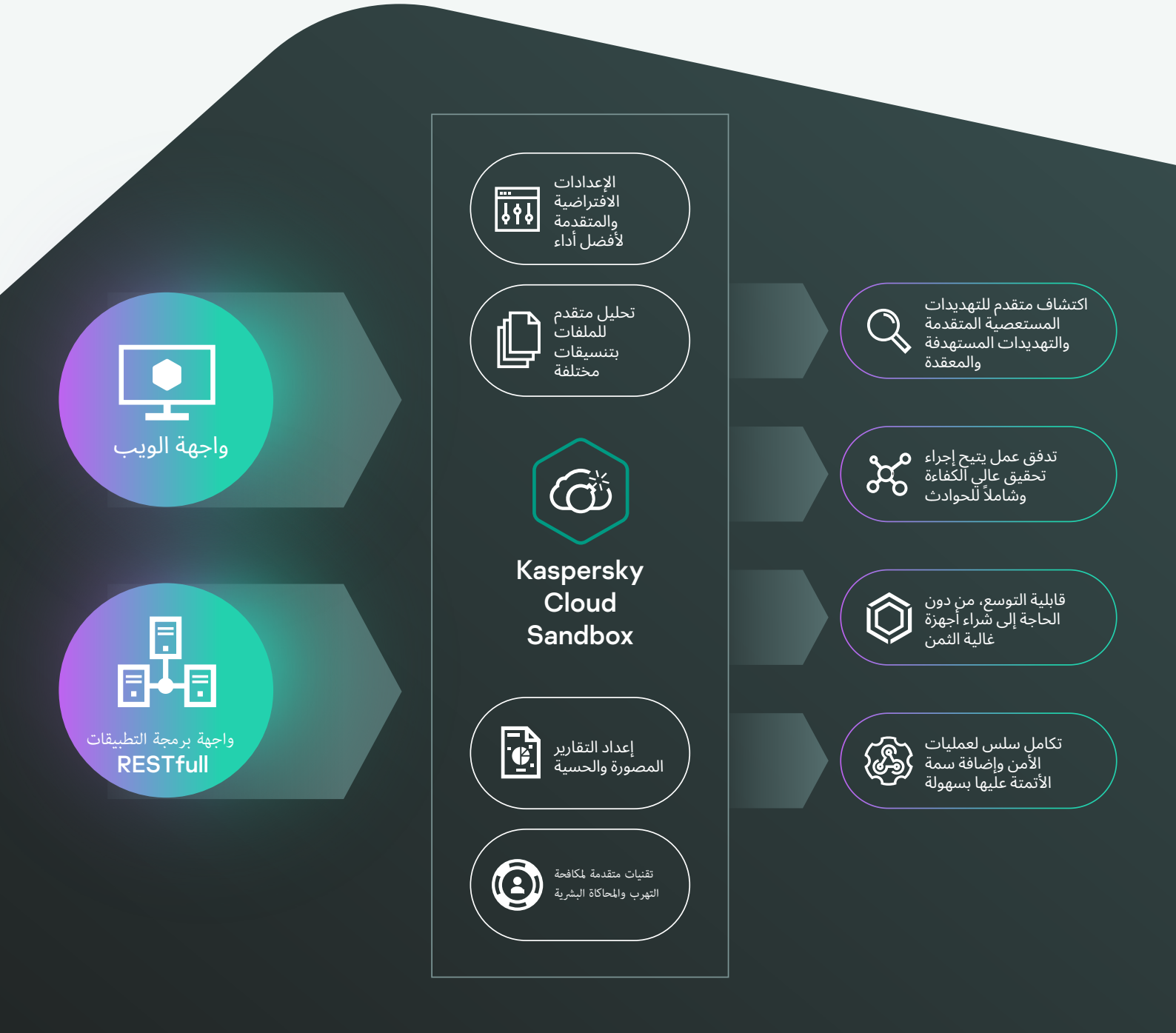
البحث عن مؤشرات التهديدات عبر واجهة قائمة على الويب أو عبر واجهة برمجة التطبيقات **RESTful**.

فهم أسباب التعامل مع أي كائن على أنه كائن ضار

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.



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**

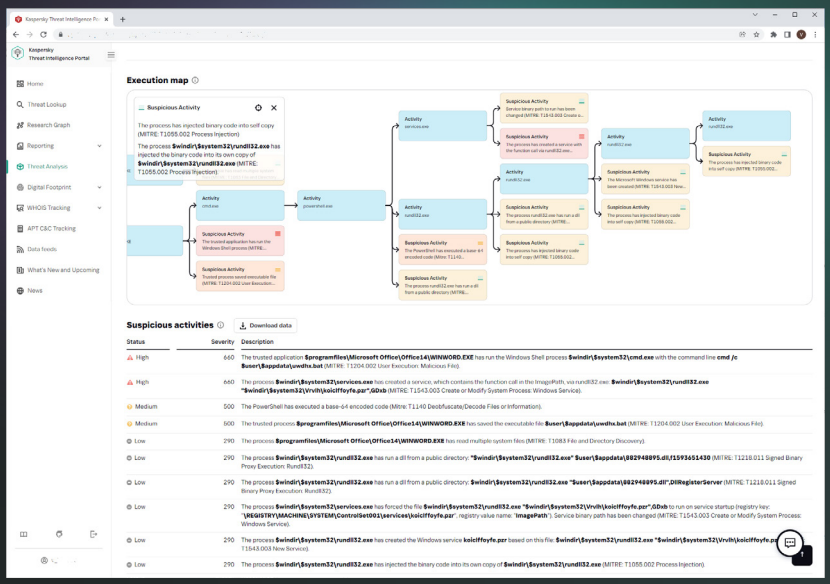
الاكتشاف الاستباقي للتهديدات والتخفيف منها

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.

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

المعلومات ذات الصلة بالبصمات الرقمية من Kaspersky

كلما زادت أعمالك، ازدادت بيئات تكنولوجيا المعلومات تعقيدًا وانتشارًا، ما يفرض المزيد من التحديات: حماية وجودك الرقمي الكبير من دون تحكم مباشر أو ملكية مباشرة. تتيح البيئات المتغيرة والمترابطة للشركات التمتع بفوائد كبيرة. لكن زيادة التواصل والترابط يساهم كذلك في انتشار الهجمات واتساع رقعتها. يتمتع المهاجمون الآن بالكثير من المهارات، لذلك؛ من المهم أن ترى صورة دقيقة لوجود مؤسستك الرقمي وتضع عينك كذلك على التغييرات التي تحدث وتستطيع الاستجابة للمعلومات الحديثة عن الأصول الرقمية المعرضة للخطر.

يمكن للمؤسسات أن تستخدم مجموعة كبيرة من أدوات الأمن في عملياتها الأمنية، لكن لا تزال ثمة تهديدات رقمية تحوم حولها: ومن ثم ستحتاج إلى القدرة على اكتشاف الأنشطة الداخلية المريبة وخطط ومخططات الهجوم للمجرمين عبر الإنترنت الموجودة على منتديات شبكة الإنترنت المظلمة، وما إلى ذلك. قامت **Kaspersky** بإنشاء المعلومات ذات الصلة بالبصمات الرقمية من أجل مساعدة محللي الأمن على استكشاف كيفية رؤية الخصوم لموارد شركتهم ومن ثم اكتشاف الهجمات المحتملة فورًا وتعديل أنظمة الدفاع لديهم بناءً على ذلك.

ما الطريقة المُثلى لشن هجوم على مؤسستك؟ ما الطرق غير المكلفة التي يتم بها شن الهجمات على مؤسستك؟ ما المعلومات المتاحة للمهاجمين الذين يستهدفون شركتك؟ هل تم اختراق بنيتك التحتية بالفعل من معرفتك؟

تجيب المعلومات ذات الصلة بالبصمة الرقمية من **Kaspersky** عن هذه الأسئلة وغيرها، حيث يجمع خبراؤنا صورة كاملة لحالة الهجوم الحالي، ويحددون نقاط الضعف المعرَّضة للاستغلال ويكتشفون أدلة الهجمات السابقة والحالية والمخطّط لها.

يوفر المنتج ما يلي:

- جرد محيط الشبكة باستخدام أساليب غير تطفلية لتحديد موارد شبكة العميل والخدمات المعرضة التي تمثل نقطة دخول محتملة للهجمات، مثل واجهات الإدارة التي تُترك على محيط الشبكة دون قصد أو الخدمات ذات التهيئة الخاطئة أو واجهات الأجهزة، وغيرها الكثير.
- تحليل مخصص لنقاط الضعف الحالية مع مزيد من التسجيل والتقييم الشامل للمخاطر بناءً على التقييم الأساسي لنظام تسجيل نقاط الضعف الشائعة (CVSS) وتوفر نقاط الاستغلال العامة وتجربة اختبار الاختراق وموقع مورد الشبكة (المضيف/البنية التحتية).
- تحديد ومراقبة وتحليل أي هجمات مستهدفة نشطة أو هجمات يتم التخطيط لها حاليًا أو حملات تهديدات مستعصية متقدمة تستهدف شركتك ومجالك ومنطقة العمليات.
- أدلة على التهديدات وأنشطة شبكات روبوتات الإنترنت التي تستهدف تحديدًا عملاءك وشركاءك والمشتركين في شبكتك، ومن ثم استخدام أنظمتهم المُصابة لشن هجوم عليك.
- مراقبة سرية لمواقع تخزين النصوص والمنتديات العامة والمدونات وقنوات المراسلة الفورية والمنتديات والمجتمعات المخفية والمحظورة عبر الإنترنت من أجل اكتشاف الحسابات المخترقة أو تسرب المعلومات أو الهجمات المخطط لشنها على مؤسستك ويتم مناقشتها هناك.

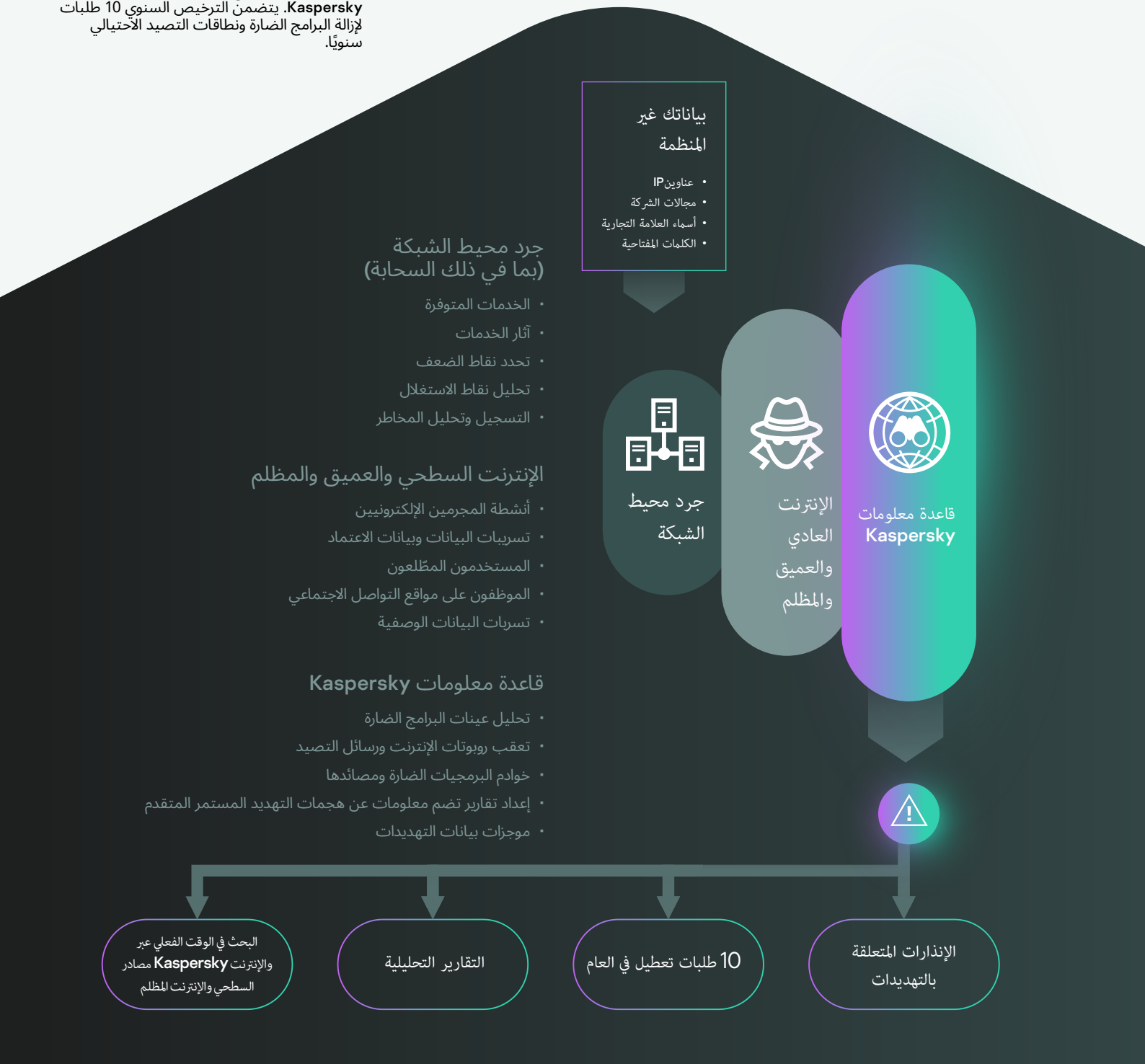
أهم الميزات

ابحث في الإنترنت السطحي والإنترنت المظلم للحصول على معلومات في الوقت الفعلي تقريبًا تتعلق بأحداث الأمان التي تهدد أصولك بالإضافة إلى البيانات الحساسة المعرضة للخطر المتعلقة بالمجتمعات والمنتديات المقيدة غير الشرعية. يتضمن الترخيص السنوي 50 بحثًا في اليوم عبر المصادر الخارجية وقاعدة معارف **Kaspersky**.

يتوفر المنتج على بوابة معلومات التهديدات من **Kaspersky**. يمكنك شراء أربعة تقارير من التقارير ربع السنوية تتضمن إنذارات التهديدات السنوية في الوقت الفعلي أو شراء تقرير واحد يتضمن إنذارات نشطة لمدة ستة أشهر.

تستخدم معلومات البصمات الرقمية من **Kaspersky** تقنيات معلومات المصادر المفتوحة **(OSINT)** مع التحليل الآلي واليدوي للإنترنت السطحي والعميق والمظلم إلى جانب قاعدة المعارف الداخلية في **Kaspersky** لتوفير توصيات ورؤى قابلة للتطبيق.

تمثل معلومات البصمات الرقمية من **Kaspersky** أحد الحلول الفردية مع خدمة التعطيل من **Kaspersky**. يتضمن الترخيص السنوي 10 طلبات لإزالة البرامج الضارة ونطاقات التصيد الاحتيالي سنويًا.



خدمة إعداد تقارير المعلومات المتعلقة بالتهديدات في أنظمة التحكم الصناعية (ICS) من Kaspersky

توفر خدمة إعداد تقارير المعلومات المتعلقة بالتهديدات عن أنظمة التحكم الصناعية (ICS) من Kaspersky معلومات تفصيلية ووعيًا أكبر عن الحملات الضارة التي تستهدف المؤسسات الصناعية، وكذلك معلومات عن نقاط الضعف التي يتم العثور عليها في أنظمة التحكم الصناعية الشائعة والتقنيات المستخدمة فيها. يتم تقديم التقارير عبر بوابة على الإنترنت، مما يعني أنه يمكنك بدء استخدام الخدمة على الفور.

التقارير المضمنة في اشتراكك

1. **تقارير التهديدات المستعصية المتقدمة** تقارير عن التهديدات المستعصية المتقدمة الجديدة وحملات التهديدات الكبيرة التي تستهدف المؤسسات الصناعية وتحديثات عن التهديدات النشطة.

2. **بيئة التهديدات.** تقارير عن التغييرات الكبيرة في عالم التهديدات لأنظمة تحكم الأفراد والعوامل القوية المكتشفة حديثًا وتؤثر على مستويات أمن أنظمة التحكم الصناعية وتعرض أنظمة التحكم الصناعية للتهديدات، ويشمل ذلك معلومات إقليمية وخاصة بكل بلد وصناعة.

3. **نقاط الضعف التي تم العثور عليها.** تقارير عن نقاط الضعف التي اكتشفتها Kaspersky في معظم المنتجات الشائعة المستخدمة في أنظمة التحكم الصناعية وإنترنت الأشياء في مجال الصناعة والبنى التحتية في مختلف الصناعات.

4. **تحليل لنقاط الضعف ومقاومتها.** توفر التحذيرات التي تصدرها Kaspersky توصيات قابلة للتطبيق من خبراء للمساعدة على تحديد نقاط الضعف في بنيتك التحتية والعمل على إزالتها.

تمكّنك بيانات معلومات التهديدات من

ربط

الأنشطة الضارة والمشبوهة التي تكتشفها في البيئات الصناعية بنتائج أبحاث Kaspersky لتحديد سمات عمليات اكتشاف الحملات الضارة المقصودة وتحديد التهديدات والاستجابة الفورية للحوادث

اكتشاف ومنع

التهديدات المبلغ عنها لحماية الأصول المهمة، مثل البرمجيات ومكونات الأجهزة، ولضمان أمان العمليات التكنولوجية واستمرارها

الاستفادة من

المعلومات المتعلقة بالتقنيات والتكتيكات والإجراءات المستخدمة في الهجمات ونقاط الضعف المكتشفة حديثًا والتغييرات المهمة الأخرى في عالم التهديدات من أجل:

- تحديد وتقييم المخاطر التي تفرضها التهديدات المبلغ عنها والتهديدات المشابهة الأخرى
- تخطيط التغييرات في البنية التحتية الصناعية وتصميمها لضمان سلامة الإنتاج واستمرار العمليات التكنولوجية
- إجراء أنشطة للوعي الأمني بناءً على تحليل لحالات واقعية لإنشاء سيناريوهات تدريب للموظفين والتخطيط لتمارين الفريق الأحمر ضد الفريق الأزرق
- اتخاذ قرارات إستراتيجية مدروسة لتطبيقها في الأمن الإلكتروني وضمان مرونة العمليات

إجراء

تقييم لنقاط الضعف في البيئات الصناعية لديك وأصولك بناءً على تقييمات دقيقة لنطاق نقاط الضعف وشدتها واتخاذ قرارات مدروسة حول إدارة الإصلاحات أو تنفيذ إجراءات وقائية أخرى توصي بها Kaspersky

Kaspersky Ask the Analyst

لا يتوقف مجرمو الإنترنت عن ابتكار طرق معقدة لمهاجمة الشركات، وعالم التهديدات المتقلب وسريع النمو اليوم يتسم بتقنيات سريعة للجرائم الإلكترونية بشكل متزايد. تواجه الشركات حوادث معقدة تتسبب فيها هجمات لا تحدث عن طريق البرمجيات الضارة وهجمات بدون ملفات وهجمات لا تحتاج إلى موارد خارجية وهجمات تستغل الثغرات الأمنية الفورية، بل ويمكن كذلك اتباع طرق تشمل كل ما سبق لتشكّل تهديدات معقدة وهجمات مستهدفة ومشابهة للتهديدات المستعصية المتقدمة.

أبحاث مستمرة عن التهديدات

تمكّن **Kaspersky** من اكتشاف المجتمعات المغلقة والمنتديات المظلمة في جميع أنحاء العالم التي يرتادها اللصوص ومجرمو الإنترنت، بل وكذلك التسلل إليها ومراقبتها. يستفيد محللونا من هذا الوصول في العمل على الاكتشاف والتحقيق بشكل استباقي في التهديدات الأكثر ضررًا والأشهر بالإضافة إلى التهديدات المصممة لاستهداف مؤسسات بعينها

في عصر الهجمات الإلكترونية التي تشل أكبر الشركات والمجالات، صار خبراء الأمن الإلكتروني أهم بكثير من أي وقت مضى، لكن العثور عليهم والمحافظة على خدماتهم ليس بالأمر السهل. وحتى إذا كان لديك فريق أمن إلكتروني متخصص وخبير، لن يقدر خبراؤك على محاربة التهديدات المعقدة 24 ساعة في اليوم وحدهم – **بل يحتاجون إلى بعض الراحة والاستعانة بخبرة طرف خارجي.** يمكن للخبرات الخارجية أن تسلط الضوء على المسارات المحتملة للهجمات المعقدة وكذلك التهديدات المستعصية المتقدمة، ومن ثم تقديم مشورة قابلة للتنفيذ عن الطريقة الأكثر حسمًا للتخلص منها تمامًا.

نتائج Ask the Analyst

(اشتراك موحد على أساس الطلب)

خدمة **اسأل المحلل Kaspersky Ask the Analyst** توسع من أعمالنا في المعلومات المتلقة بالتهديدات، وهذا يوفر لك إمكانية طلب توجيهات وآراء عن تهديدات معينة قد واجهتها أو لديك فضول عنها. تخصص الخدمة المعلومات المتعلقة بالتهديدات وقدرات البحث القوية من **Kaspersky** وفقًا لاحتياجاتك الخاصة، وهذا يتيح لك بناء دفاعات صلبة ضد التهديدات التي تستهدف مؤسستك.

تحليل البرامج الضارة

- تحليل عينة برامج ضارة
- التوصيات بشأن إجراءات المعالجة الأخرى

التهديدات المستعصية المتقدمة والبرامج الإجرامية

معلومات إضافية عن التقارير المنشورة والأبحاث الجارية (بالإضافة إلى خدمة الإبلاغ عن المعلومات المتعلقة بالتهديدات المستعصية المتقدمة أو البرامج الجريمة)[1]

معلومات الإنترنت المظلم[2]

- أبحاث الإنترنت المظلم عن بعض الأشياء المعينة أو عناوين IP أو أسماء نطاقات أو أسماء ملفات أو رسائل بريد إلكتروني أو روابط أو صور بعينها
- البحث في المعلومات والتحليل

أوصاف التهديدات والثغرات الأمنية ومؤشرات الاختراق ذات الصلة

- وصف عام لعائلة برمجيات ضارة معينة
- محتوى إضافي للتهديدات (قيم التجزئة والروابط الإلكترونية والتحكم والسيطرة وما إلى ذلك)
- معلومات عن ثغرة أمنية محددة (مدى خطرها وآليات الحماية منها في منتجات **Kaspersky**)

الطلبات المتعلقة بنظام

- معلومات إضافية حول التقارير المنشورة
- المعلومات المتعلقة بنقاط الضعف في نظام ICS
- الإحصائيات الخاصة بالتهديد في نظام ICS والاتجاهات الخاصة بالمنطقة/المجال
- معلومات تحليل البرامج الضارة في نظام ICS وفقًا للوائح أو المعايير

[1] متوفرة فقط للعملاء مع خدمة الإبلاغ عن المعلومات الاستخبارية عن التهديدات المستعصية المتقدمة و/أو البرامج الإجرامية

[2] موجودة بالفعل في اشتراك **Kaspersky Digital Footprint Intelligence**

مزايا الخدمة

زد من خبراتك

تمتع عند الحاجة بوصول لخبراء في المجال دون الحاجة إلى البحث عن متخصصين يعملون بدوام كامل ودون تكبد مبالغ مالية كبيرة مقابل خدماتهم، ناهيك عن صعوبة العثور عليهم

عمليات فحص أسرع

تحديد نطاق الحوادث وترتيب أولوياتها بناءً على معلومات سياقية مخصصة ومفصلة

استجابة سريعة

استجب إلى التهديدات والثغرات الأمنية بسرعة باستخدام توجيهاتنا التي ترشدك لكيفية حجب الهجمات التي تحدث عبر طرق نقل التهديدات المعروفة

آلية العمل

يمكن شراء خدمة اسأل المحلل **Kaspersky Ask the Analyst** بشكل منفصل أو مع أي خدمات عن المعلومات المتعلقة بالتهديدات.

يمكنك تقديم طلباتك عبر حساب شركة Kaspersky على بوابة دعم عملاء الشركات سنرد عبر البريد الإلكتروني، لكن يمكننا أيضًا الترتيب لاجتماع فيديو و/أو جلسة مشاركة شاشة إذا كان هذا ضروريًا وكنت توافق عليه. بمجرد الموافقة على طلبك سيتم إخبارك بالموعد المتوقع لمعالجة هذا.

حالات استخدام الخدمة:

- احصل على تفاصيل إضافية عن أنشطة الإنترنت المظلمة التي تثير فضولك
- الحصول على تفاصيل عن الثغرات الأمنية والتوصيات عن كيفية الحماية من استغلالها
- الحصول على معلومات إضافية لمؤشرات اختراق تم توفيرها بالفعل
- توضيح أي تفاصيل في تقارير منشورة سابقة عن المعلومات المتعلقة بالتهديدات
- قدم ملفات البرامج الضارة لإجراء بحث شامل لها لفهم سلوك العينات المتوفرة وعملها
- اطلب مساعدة في تحديد إذا ما كان النشاط غير المعتاد المكتشف ذي صلة بتهديد مستعصي متقدم أو برنامج إجرامي أم لا
- ترتيب أولويات الإنذارات الحوادث بكفاءة مع معلومات سياقية تفصيلية وكذلك تصنيف مؤشرات الاختراق ذات الصلة التي يتم توفيرها عبر تقارير قصيرة
- الحصول على تقرير يحتوي على نظرة عامة على عائلة البرنامج الضار، ويشمل هذا سلوك البرنامج الضار وتأثيره المحتمل وتفاصيل عن أي نشاط ذي صلة قد لاحظته **Kaspersky**

توسيع معارفك ومواردك

توفر لك خدمة **Kaspersky Ask the Analyst** إمكانية الوصول إلى مجموعة رئيسية من أبحاث **Kaspersky** على أساس كل حالة على حدة. توفر هذه الخدمة تواصل شامل بين الخبراء لتعزيز قدراتك التي تتمتع بها بالفعل بمعرفة فريدة وموارد نادرة.

خدمة التعطيل من Kaspersky

التحدي

يقوم المجرمون عبر الإنترنت بإنشاء المجالات الضارة والاحتيالية التي تستخدم لمهاجمة شركتك وعلاماتك التجارية. يمكن أن يؤدي عدم القدرة على تقليل هذه التهديدات بسرعة، بمجرد تحديدها، إلى خسارة الإيرادات وتضرر العلامة التجارية وفقدان ثقة العملاء وتسرب البيانات والمزيد. لكن إدارة عمليات التعطيل لهذه المجالات عملية معقدة تتطلب خبرة ووقتًا.

الحل

تعمل **Kaspersky** على حظر أكثر من 15000 رابط **URL** احتيالي/خادع ومنع أكثر من مليون محاولة للضغط على روابط **URL** هذه كل يوم. تعني خبراتنا الواسعة في تحليل المجالات الضارة والاحتيالية أننا نعرف كيفية جمع كل الأدلة الضرورية لإثبات أنها ضارة. سنعتني بعملية إدارة التعطيل وسنوفر إمكانية اتخاذ إجراء سريع لتقليل المخاطر الرقمية حتى يتمكن فريقك من التركيز على المهام الأخرى ذات الأولوية.

توفر **Kaspersky** لعملائها حماية فعالة لخدماتهم وسمعتهم عبر الإنترنت من خلال العمل مع المنظمات الدولية ووكالات إنفاذ القانون الوطنية والإقليمية (مثل منظمة الشرطة الدولية **(INTERPOL)** والشرطة الأوروبية **(Europol)** ووحدة الجرائم الرقمية في **Microsoft** والوحدة القومية لمكافحة الجرائم عالية التقنية **(NHTCU)** التابعة لوكالة الشرطة في هولندا وشرطة مدينة لندن)، بالإضافة إلى فرق الاستجابة لطوارئ الكمبيوتر **(CERT)** في كل أنحاء العالم.

آلية العمل

يمكنك تقديم طلباتك عبر حساب شركة Kaspersky على بوابة دعم عملاء الشركات لدينا. سنقوم بإعداد كل الوثائق اللازمة وسنرسل طلب التعطيل إلى السلطة المحلية/الإقليمية ذات الصلة (فريق التصدي للطوارئ الحاسوبية **(CERT)**، المسجّل، وما إلى ذلك) التي تتمتع بالحقوق القانونية اللازمة لإغلاق المجال. ستتلقى إشعارات في كل خطوة من العملية حتى تتم إزالة المورد المطلوب بنجاح.

حماية سلسة

تقوم خدمة التعطيل من **Kaspersky** بسرعة بتقليل التهديدات التي تفرضها المجالات الضارة والاحتيالية قبل حدوث أي ضرر لعلامتك التجارية وشركتك. توفر الإدارة الشاملة للعملية كلها بتوفير الوقت الثمين والموارد.

مزايا الخدمة

التغطية العالمية

لا يهم مكان تسجيل مجال ضار أو احتيالي، ستطلب **Kaspersky** تعطيله من المؤسسة الإقليمية مع السلطة القانونية ذات الصلة.

الإدارة الشاملة

سنقوم بإدارة عملية التعطيل بالكامل وتقليل انشغالك بها إلى أدنى حد.

الرؤية الكاملة

سيتم إخطارك في كل مرحلة من العملية، بداية من تسجيل طلبك وانتهاءً بنجاح عملية التعطيل.

التكامل مع المعلومات ذات الصلة بالبصمة الرقمية

تندمج الخدمة مع المعلومات ذات الصلة ببصمة الإصبع الرقمية من **Kaspersky** التي توفر إعلامات في الوقت الفعلي حول التصيد الاحتيالي والمجالات الضارة المصممة للإضرار بعلامتك التجارية/مؤسستك أو إساءة استخدامها أو انتحالها. يعد الحل الفردي أحد العناصر المهمة لإستراتيجية الأمن الإلكتروني الشاملة.

الفوائد الرئيسية

تتيح رؤية التهديدات العالمية واكتشاف التهديدات الإلكترونية في الوقت المناسب وإعطاء الأولوية للتنبيهات الأمنية والاستجابة الفعالة لحوادث أمن المعلومات

يمنع ذلك إرهاق المحلل ويساعد على تركيز القوى العاملة على التهديدات الحقيقية

توفر الرؤى الفريدة للتكتيكات والتقنيات والإجراءات المستخدمة من قِبل الجهات التي تشن التهديدات عبر مختلف الصناعات والمناطق حماية استباقية من التهديدات المستهدفة والمعقدة

تتيح النظرة العامة الشاملة على وضعك الأمني مع توصيات قابلة للتنفيذ بشأن إستراتيجيات التخفيف تركيز إستراتيجيتك الدفاعية على المناطق المحددة بصفتها أهدافًا رئيسية للهجمات الإلكترونية

تساعد قدرات الاستجابة المحسّنة والمتسارعة للحوادث واكتشاف التهديدات على تقليل "وقت الكمون" للهجمات وتقليل الضرر المحتمل بصورة كبيرة

الخاتمة

يتطلب التصدي للتهديدات الإلكترونية اليوم رؤية شاملة للأساليب والأدوات التي تستخدمها الجهات التي تشن التهديدات. ويتطلب توليد هذه المعلومات وتحديد الإجراءات المضادة الأكثر فعالية تفانيًا مستمرًا ومستويات عالية من الخبرة. نعمل في **Kaspersky** على دعم عملائنا بأحدث المعلومات المتعلقة بالتهديدات من كل أنحاء العالم مع كميات من بيانات التهديدات الغنية وتقنيات التعلّم الآلي المتقدمة ومجموعة فريدة من الخبراء العالميين، لمساعدتهم على البقاء آمنين من الهجمات الإلكترونية غير المعهودة سابقًا.

FORRESTER®

تم تصنيف **Kaspersky** بصفتها رائدة في **Forrester Wave**: خدمات المعلومات المتعلقة بالتهديدات الخارجية لعام 2021

Kaspersky Threat Intelligence

معرفة المزيد

www.kaspersky.com