واجهوا المستقبل
بأمان

kaspersky

Kaspersky CyberTrace

إن عدد التنبيهات الأمنية التي يعالجها محللو أمن المعلومات كل يوم يزداد بشكل ملحوظ. ومع هذه الكمية من البيانات التي يتم تحليلها، فمن شبه المستحيل ترتيب أولويات التنبيهات وفرزها والتحقق منها بشكل فعال. ثمة الكثير من الأضواء الوامضة التي تصدر من منتجات أمن متعددة، ما يؤدي إلى إخفاء بعض التنبيهات الخطيرة إثر هذا التشويش وإرهاق المحلل. إن أنظمة معلومات الأمن وإدارة الأحداث **(SIEM)** وإدارة السجلات وأدوات تحليلات الأمن التي تعمل على تجميع البيانات الأمنية وربط الإنذارات ذات الصلة تساعد كلها في تقليل عدد التنبيهات التي تتطلب فحصًا إضافيًّا، لكن لا يزال محللو الأمن محملين أكثر من طاقتهم بكثير.

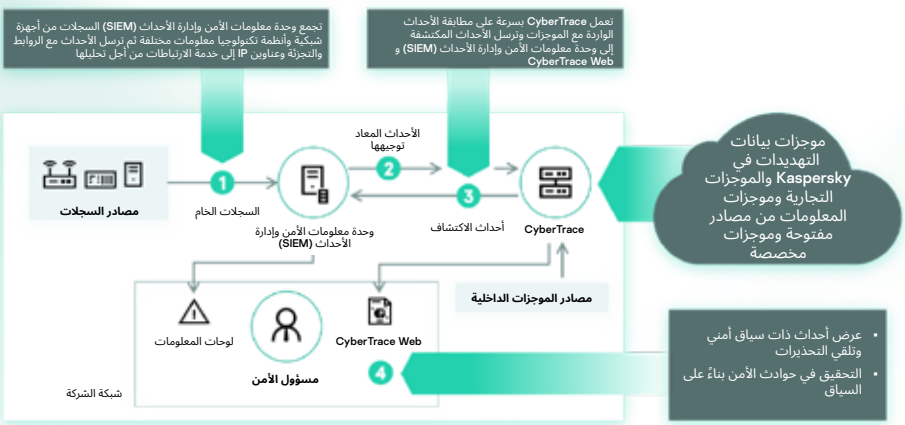
تمكين فرز التحذيرات وتحليلها بشكل فعال

من خلال دمج معلومات متعلقة بالتهديدات حديثة وقابلة 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 وتشمل عددًا كبيرًا من مؤشرات الاختراق (IoC)، ما يصعّب على أنظمة معلومات الأمن وإدارة الأحداث (SIEM) أو عناصر التحكم في أمن الشبكة استيعابها.

Kaspersky CyberTrace عبارة عن نظام أساسي للتحليل الذكي للتهديدات يتيح دمج موجزات بيانات التهديدات بسلاسة في حلول معلومات الأمن وإدارة الأحداث (SIEM) لمساعدة المحللين في الاستفادة من المعلومات المتعلقة بالتهديدات في سير عمل العمليات الأمنية لديهم بفعالية أكبر. يمكن لهذه الأداة التكامل مع أي موجز معلومات متعلقة بالتهديدات بأي تنسيق قد تريد استخدامه من تنسيقات JSON وSTIX و XML وCSV (سواء أكانت موجزات معلومات متعلقة بالتهديدات من Kaspersky أو موردين آخرين أو OSINT أو موجزات تخصصها بنفسك)، وبالتالي تدعم التكامل الجاهز مع عدد كبير من حلول معلومات الأمن وإدارة الأحداث (SIEM) ومصادر السجلات.

تستخدم أداة Kaspersky CyberTrace عملية داخلية من التحليل والمطابقة للبيانات الواردة، ما يقلل بشكل كبير من أعباء عمل أنظمة معلومات الأمن وإدارة الأحداث (SIEM). تعمل على تحليل السجلات والأحداث الواردة وتطابق بسرعة بين البيانات الناتجة مع الموجزات ومن ثم تنشئ تحذيراتها الخاصة عن اكتشاف التهديدات. يمكن الاطلاع على بنية عالية المستوى لتكامل الحل في الصورة أدناه:

يتم توفير المعلومات المتعلقة بالتهديدات في تنسيقات مختلفة وتشمل عددًا كبيرًا من مؤشرات الاختراق (IoC)، ما يصعّب على أنظمة معلومات الأمن وإدارة الأحداث (SIEM) أو عناصر التحكم في أمن الشبكة استيعابها.

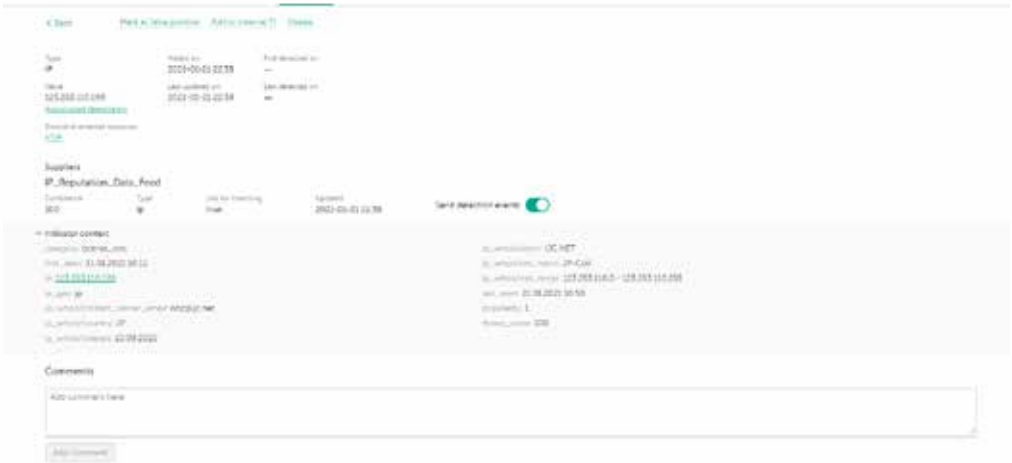


الشكل 1. مخطط دمج **Kaspersky CyberTrace**

ميزات المنتج

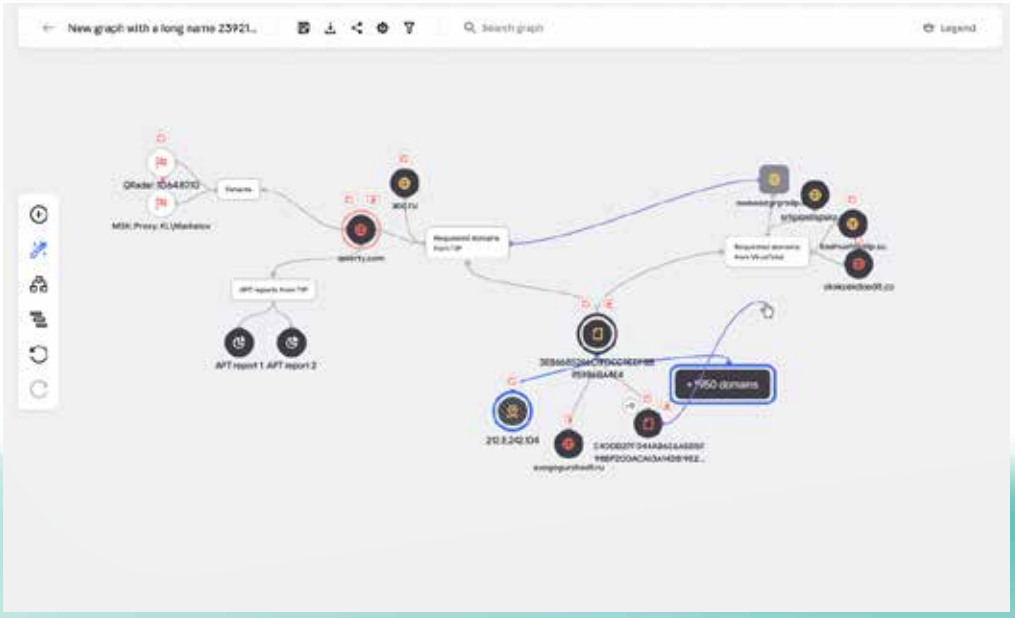
توفر أداة Kaspersky CyberTrace مجموعة من الأدوات التي تدير المعلومات المتعلقة بالتهديدات من أجل إجراء فرز فعَّال للتحذيرات والاستجابة الأوَّلية:

- تسمح قاعدة بيانات مؤشرات ذات إمكانية البحث عن نصوص كاملة والبحث باستخدام استعلامات البحث المتقدمة بإجراء عمليات بحث معقدة عبر كل حقول المؤشرات، بما فيها حقول السياق. تبسّط تصفية النتائج بحسب مزوّد المعلومات عملية تحليل المعلومات المتعلقة بالتهديدات.
- توفّر الصفحات التي تحتوي على معلومات مفصّلة حول كل مؤشر تحليلاً أعمق. تعرض كل صفحة المعلومات كافة حول مؤشرٍ من كل مزوّدي المعلومات المتعلقة بالتهديدات (إلغاء التكرار) ليتمكّن المحللون من مناقشة التهديدات في التعليقات وإضافة معلومات داخلية متعلقة بالتهديدات حول المؤشر. إذا تم اكتشاف المؤشر، فستتوفر المعلومات حول تواريخ عمليات الاكتشاف والروابط إلى قائمة عمليات الاكتشاف.



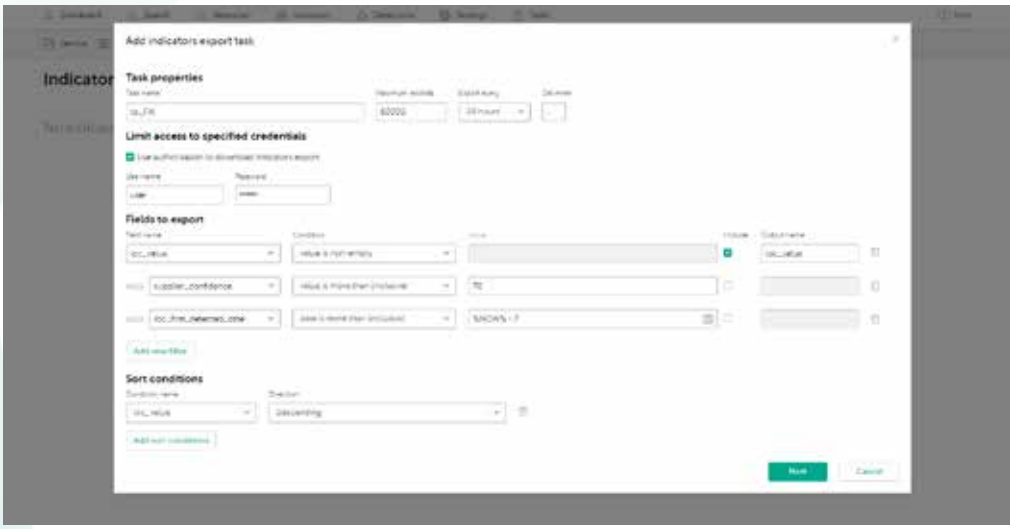
الصورة 2. معلومات مفصّلة حول مؤشر من كل مزوّدي المعلومات المتعلقة بالتهديدات

- ويسمح الرسم البياني البحثي باستكشاف البيانات والكشوف المخزنة في CyberTrace بصورة بصرية واكتشف ملامح أي تهديدات. ويسمح كذلك بالتصور البياني للعلاقة بين عناوين URL والمجالات والبرامج المتكاملة وعناوين IP والملفات وغيرها من السياقات التي تمت مواجهتها أثناء إجراءات التحقيقات.
ويتضمن الرسم البياني كذلك السمات التالية: التحولات، والرسم البياني المصغر، والعقود التجميعية، وإضافة الروابط يدويًا، وإضافة المؤشرات، والبحث عن العُقد على الرسم البياني.



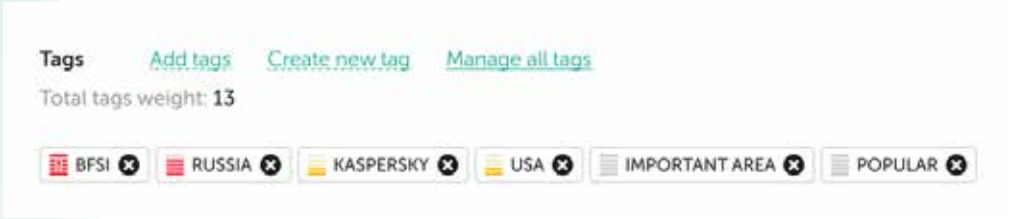
الشكل 3. الرسم البياني البحثي

- تقوم ميزة تصدير المؤشرات بدعم تصدير مجموعات المؤشرات إلى عناصر التحكم في الأمن، مثل قوائم السياسات (قوائم الحظر)، بالإضافة إلى مشاركة بيانات التهديدات ما بين عمليات Kaspersky CyberTrace أو مع الأنظمة الأساسية الأخرى للمعلومات المتعلقة بالتهديدات.



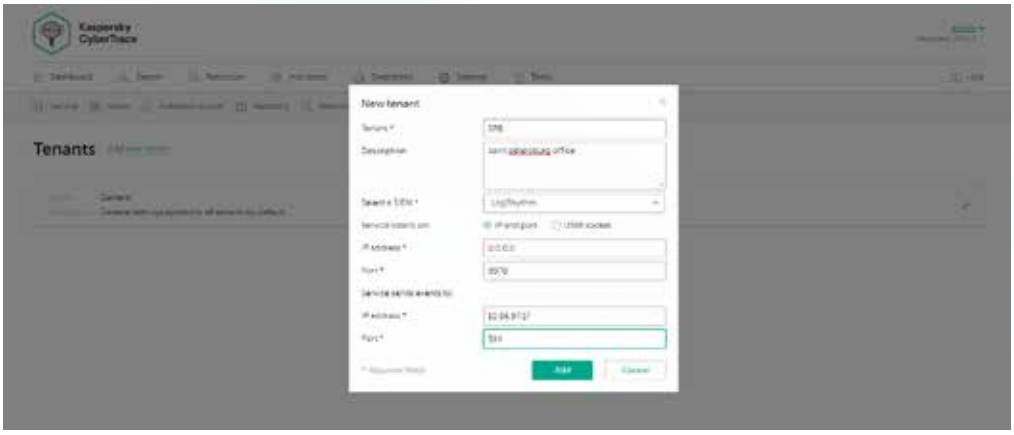
الشكل 4. مهمة تصدير المؤشرات

- 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. وبوسعنا كذلك فرز مؤشرات الاختراق وترشيحها بناءً على هذه العلامات وأوزانها.



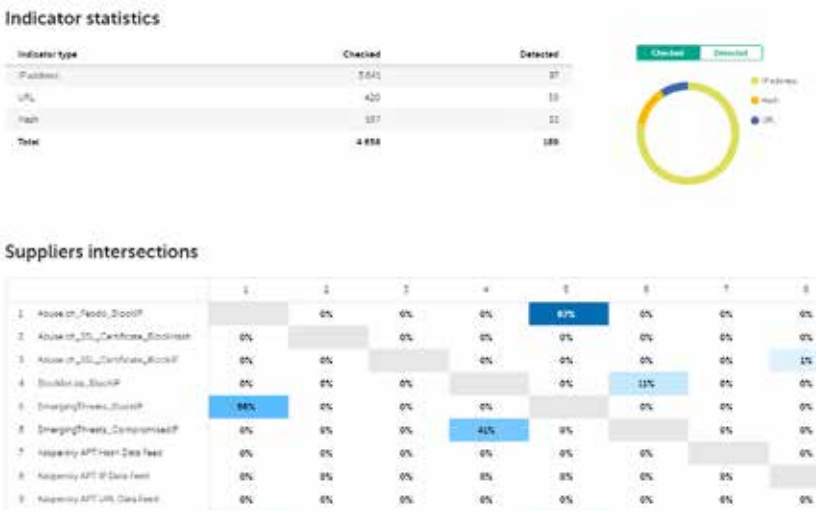
الصورة 5. علامات مؤشرات الاختراق

- 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. يتضمن التقرير عمليات الاكتشاف التاريخية كلها من أجل التحقيقات المستقبلية.
- يعمل عامل تصفية مخصص لإرسال أحداث عمليات الاكتشاف إلى حلول معلومات الأمن وإدارة الأحداث (SIEM) على تقليل الحمل عليها وعلى المحلل الذي يعاني إجهاد الإنذارات. ويسمح لك بإرسال أكثر عمليات الاكتشاف خطورة فقط، أي تلك التي يجب التعامل معها كحوادث، إلى أنظمة معلومات الأمن وإدارة الأحداث (SIEM). يتم حفظ عمليات الاكتشاف الأخرى كلها في قاعدة البيانات الداخلية ويمكن استخدامها أثناء تحليل السبب الجذري أو في تقصي أثر التهديدات.
- تقوم ميزة تعدد المستأجرين بدعم موفري خدمات الأمن المدارة أو حالات الاستخدام من قِبل المؤسسات الكبيرة عندما يحتاج مقدّم خدمة (مكتب مركزي) إلى التعامل مع أحداث من فروع مختلفة (مستأجرين) بشكل منفصل. يسمح ذلك باتصال عملية Kaspersky CyberTrace واحدة بحلول مختلفة لمعلومات الأمن وإدارة الأحداث (SIEM) من مستأجرين مختلفين، ويمكنك تكوين الموجزات التي تريد أن يتم استخدامها لكل مستأجر.



الشكل رقم 6. إنشاء مستأجر جديد

- تقوم إحصاءات استخدام الموجزات المُستعملة في قياس فعالية الموجزات المتكاملة ومصفوفة تقاطع الموجزات بالمساعدة في اختيار المزوّدين الأكثر أهمية للمعلومات المتعلقة بالتهديدات.



الشكل رقم 7. إحصاءات المؤشرات ومصفوفة تقاطع الموجزات

- تسمح لك HTTP RestAPI بالبحث عن معلومات متعلقة بالتهديدات وإدارتها. من خلال استخدام Rest API، يمكن دمج Kaspersky CyberTrace بسهولة في البيئات المعقدة للأتمتة والتوزيع.
- يتم دعم التكامل مع النظام الأساسي الموحد للمراقبة والتحليل من Kaspersky (KUMA)، بما في ذلك تكامل واجهة مستخدم الويب (واجهة مستخدم واحدة).

بالرغم من إمكانية استخدام أداة Kaspersky CyberTrace وموجزات البيانات المتعلقة بالتهديدات من Kaspersky بشكل منفصل، فإنها تقوي بشكل ملحوظ من قدرات اكتشاف التهديدات عند استخدامها معًا، ما يقوي عمليات الأمن لديك عبر تزويدها برؤية شاملة للتهديدات الإلكترونية. مع Kaspersky CyberTrace وموجزات البيانات المتعلقة بالتهديدات من Kaspersky، تتمكن المنظمات من:

- تنقيح التنبيهات الأمنية وتحديد أولوياتها بفعالية
- تقليل أعباء عمل المحللين ومنع إرهاقهم
- تحديد التحذيرات الخطيرة بشكل فوري واتخاذ قرارات مدروسة أكثر حول التحذيرات التي يجب تصعيدها إلى فرق الاستجابة للحوادث
- تشكيل آلية دفاعية استباقية ومبنية على المعلومات.

ميزات المنتج الأخرى:

- قابلية التكامل مع مختلف حلول معلومات الأمن وإدارة أحداثه لتصور وإدارة البيانات المتعلقة باكتشاف التهديدات
- بحث عن المؤشرات عند الطلب (التجزئات وعناوين IP والمجالات وروابط URL) لفحص مكثف للتهديدات
- تصفية متقدمة للموجزات
- فحص كميات كبيرة من السجلات والملفات
- واجهة سطر الأوامر لنظامي التشغيل Windows وLinux
- الوضع المستقل الذي تعمل فيه أداة Kaspersky CyberTrace على تلقي السجلات من مصادر مختلفة، مثل الأجهزة الشبكية، وتحليلها
- وغيرها الكثير

أخبار التهديدات الإلكترونية: www.securelist.com
أخبار أمن تكنولوجيا المعلومات: business.kaspersky.com
أخبار أمن تكنولوجيا المعلومات للشركات الصغيرة والمتوسطة الحجم: kaspersky.com/business
أخبار أمن تقنية المعلومات للمؤسسات الكبيرة: me.kaspersky.com/enterprise-security
بوابة Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com