Kaspersky SIEM

المستند التقني للمنتج

واجِهوا المستقبل بأمان kaspersky

المحتويات

سوق إدارة معلومات الأمان والأحداث

يواجه قادة الأمن الإلكتروني في المؤسسات العديد من التحديات، بما في ذلك العدد المتزايد من محاولات اختراق بنيتهم التحتية، ونقص موظفي الأمن الإلكتروني، والهجمات المعقدة بشكل متزايد.

علاوة على ذلك، يجب على المؤسسات الالتزام بالمتطلبات التنظيمية المتعلقة بالاحتفاظ بالبيانات والتدقيق والتحقيق في الحوادث، مما يؤثر على سوق إدارة معلومات الأمان والأحداث (SIEM) العالمي.

تتعرض المؤسسات أيضًا لضغوط لفصل تنبيهات الهجمات الإلكترونية حسب الأولوية وفرزها بشكل أكثر كفاءة نظرًا لنموها وتعقيدها المتزايد.

بالإضافة إلى ذلك، دفعت ظروف العمل عن بُعد الشركات إلى اعتماد تطبيقات البرامج كخدمة (SaaS) والسماح للموظفين بإحضار أجهزتهم الخاصة (BYOD)، مما يسلط الضوء على الحاجة إلى توسيع نطاق رؤية الشبكة خارج المحيط التقليدي.

أخيرًا، يمثل العثور على خبراء مؤهلين في مجال أمان المعلومات تحديًا في السوق اليوم. وتبحث الشركات عن طرق لتحسين مواردها وتحسين كفاءة الأمن الإلكتروني. وبالتالي، تريد المؤسسات الحصول على بيانات استخباراتية يسهل الوصول إليها وقابلة للتنفيذ لفرق مركز عمليات الأمان الخاصة بها.

وفقًا لتقرير Kaspersky Human Factor 360 Report

77%

من الشركات تعرضت لاختراق واحد على الأقل للأمن الإلكتروني، مع تعرض العديد منها لستة اختراقات في تلك الفترة

41%

من الشركات تشعر بأن لديها فجوات في البنية التحتية للأمن الإلكتروني وتخطط لزيادة الاستثمارات في هذا المجال من الآن فصاعدًا

معرفة المزيد

حول Kaspersky SIEM وبنيته

Kaspersky Unified Monitoring and Analysis Platform عبارة عن حل SIEM متكامل من الجيل التالي لإدارة بيانات وأحداث الأمان. ويتفوق في تلقي ومعالجة وتخزين أحداث معلومات الأمان، وتحليل البيانات الواردة وربطها. وتحتوي المنصة أيضًا على ميزة البحث، وتنشئ تنبيهات عند اكتشاف تهديدات محتملة، وتدعم الاستجابات التلقائية للتنبيهات التي تم إنشاؤها وتعقب التهديدات.

تسمح البنية المعيارية عالية الأداء بمعالجة مئات الآلاف من الأحداث في الثانية (EPS) في كل مثيل وتقليل التكلفة الإجمالية للملكية (TCO) عن طريق تحسين متطلبات النظام.

من خلال دمج منتجات الأطراف الخارجية ومنتجات Kaspersky في نظام مركزي لأمان المعلومات، يعد Kaspersky SIEM جزءًا أساسيًا من إستراتيجية دفاعية شاملة قادرة على تأمين البيئات المؤسسية والصناعية، بالإضافة إلى اكتشاف الهجمات الإلكترونية التي تبدأ في مجال تكنولوجيا المعلومات وتنتقل إلى أنظمة التكنولوجيا التشغيلية.

بفضل بنية الخدمات الصغيرة للحل، يستطيع المسؤولون إنشاء وتكوين الخدمات الصغيرة التي يحتاجون إليها لاستخدام Kaspersky SIEM كنظام لإدارة معلومات الأمان والأحداث (SIEM) كامل أو نظام لإدارة السجلات.

يستقبل الحل أحداث الأمان من مصادر مختلفة، بما في ذلك منتجات Kaspersky وأنظمة التشغيل وتطبيقات الأطراف الخارجية وأدوات الأمان وقواعد البيانات المختلفة، ويربط الأحداث مع بعضها البعض ويثريها بالبيانات من خلاصات معلومات التهديدات لتحديد الأنشطة المشبوهة في البنى التحتية لشبكة الشركة وتقديم الإخطار في الوقت المناسب عن حوادث الأمان.

من خلال جمع السجلات من كل عناصر التحكم الخاصة بالأمان وربط البيانات في الوقت الحقيقي، يجمع **Kaspersky SIEM ويوفر كل المعلومات اللازمة للتحقيق في الحوادث والاستجابة لها.**

علاوة على ذلك، يتيح Kaspersky SIEM لصائدي التهديدات اكتشاف التهديدات غير المعروفة سابقًا من خلال السماح للمشغلين بتحليل البيانات التاريخية وربطها، بالإضافة إلى إنشاء خطوط أساس إحصائية لتحديد الحالات الشاذة.

يحتوي Kaspersky Unified Monitoring and Analysis Platform على المكونات التالية

تم تزويد مكون **Core** بواجهة مستخدم رسومية مركزية للتحكم في إعدادات مكونات النظام ومراقبتها. ويمكن الوصول إلى المنصة من خلال حلول الجهات الخارجية باستخدام واجهة برمجة التطبيقات.

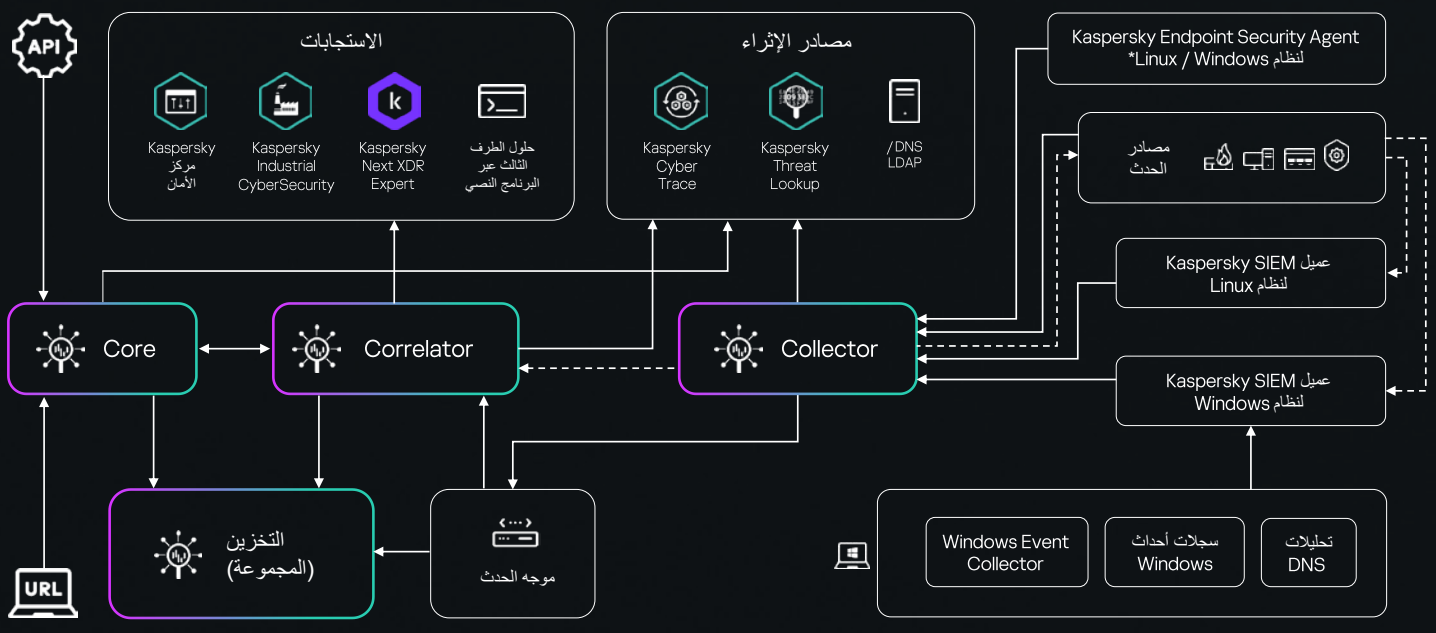
تُستخدم قواعد الارتباط لاكتشاف تسلسلات معينة من الأحداث التي تمت معالجتها واتخاذ إجراءات معينة بعد التعرف عليها، مثل إنشاء أحداث / تنبيهات الارتباط أو التفاعل مع قائمة نشطة. ويستخدم **Correlator** القوائم النشطة لتنفيذ الإجراءات المطلوبة بعد تحليل الأحداث الموحدة المستلمة من أدوات التجميع وينشئ تنبيهات بناءً على معايير الارتباط.

يتلقى مكون **Collector** واحد أو أكثر الأحداث من مصادر خارجية ويعالجها مسبقًا: توحيدها (التغيير إلى تنسيق واحد)، وتصفيتها، وتجميعها، وإثرائها ببيانات من مصادر خارجية باستخدام القواميس، والاستدعاءات إلى خدمة DNS، وأدوات أخرى.

يُستخدم مكون **Storage** لتخزين الأحداث الموحدة حتى يمكن الوصول إليها بسرعة وبشكل مستمر من إدارة معلومات الأمان والأحداث (SIEM) لاستخراج البيانات التحليلية.

يعيد مكون Agents توجيه الأحداث الأولية من محطات العمل والخوادم إلى جامعي إدارة معلومات الأمان والأحداث (SIEM). وأصبح من الممكن الآن إرسال أحداث سجل Windows مباشرة إلى أداة التجميع في Kaspersky Endpoint Security لنظام التشغيل Windows 12.6 أو Linux 12.2. ويؤدي هذا إلى تقليل حجم العمل اللازم لدمج مصادر الأحداث مع نظام Kaspersky SIEM بشكل كبير.

تقلل أجهزة توجيه الأحداث الحمل على الارتباطات وعدد المنافذ المفتوحة على جدران الحماية من خلال استقبال الأحداث بشكل ثابت دون تأخير عند تثبيت المجمعات في المكاتب البعيدة ذات النطاق الترددي المنخفض أو ارتباطات البيانات المشغولة بالفعل.



وظائف Kaspersky SIEM

مراقبة ومعالجة وتخزين المعلومات حول أحداث الأمان

يتلقى حل Kaspersky Unified Monitoring and Analysis Platform الأحداث من السجلات ويُوحد البيانات من مصادر الأحداث المختلفة لجعلها متسقة. وقد تتضمن أحداث أمان المعلومات هذه محاولات تسجيل الدخول، أو تفاعلات قاعدة البيانات، أو عمليات بث معلومات أداة الاستشعار، ويتم جمعها من خلال البنية التحتية لتكنولوجيا المعلومات المحمية بالكامل للشركة. على الرغم من أن الحدث الفردي قد لا يبدو مهمًا، إلا أن الأحداث الفردية المتعددة ترسم صورة أكبر للنشاط الخبيث الذي يمكن استخدامه لاكتشاف مشكلات الأمان.

يوفر نظام بحيرة البيانات، وهو مستودعنا المحلي المركزي المحلي، منصة لجمع وفهرسة وتحليل السجلات من مصادر مختلفة، بما في ذلك حلول الأمان (EPP وFW وIAM، وما إلى ذلك)، وأنظمة التشغيل، وتطبيقات الأعمال (أنظمة الموارد البشرية، والأدوات المكتبية)، وأنظمة الأمن المادي (أنظمة التحكم الآلي في الوصول)، وغيرها من الأجهزة.

يتم نقل الأحداث إلى أداة الترابط لتحليلها وتخزينها للاحتفاظ بها بمجرد تصفيتها وتجميعها. ولتحديد التنبيهات، تتلقى أداة الجمع الأحداث من المصادر، وتعالجها وتوجهها إلى خدمات التخزين و/أو الارتباط و/أو خدمات الأطراف الخارجية. وتتم إعادة توجيه الأحداث الأولية من محطات العمل والخوادم إلى أدوات جمع SIEM (في بعض الحالات بواسطة العملاء) ويمكن إرسالها إلى أنظمة أخرى لإجراء تحليل إضافي.

يتم إنتاج أحداث الارتباط بواسطة الحل عند التعرف على حدث معين أو سلسلة من الأحداث ذات الصلة ويتم أيضًا تحليلها والاحتفاظ بها. وإذا أشار حدث أو تسلسل من الأحداث إلى وجود تهديد أمان محتمل، فإن Kaspersky SIEM يولد تنبيهًا يتضمن معلومات حول التهديد وأي معلومات أخرى ذات صلة يحتاج المتخصصون في مجال الأمن إلى أخذها بعين الاعتبار.

يتم استخدام بروتوكولات نقل موثوقة، مع تشفير اختياري، لنقل الأحداث بين المكونات. ويمكن للنظام استخدام صمام ثنائي للبيانات لجمع البيانات من الأجزاء المعزولة.

موصلات مدمجة ومخصصة لمئات المصادر من Kaspersky وموردي الجهات الخارجية مع تحديثات وتحسينات منتظمة.

تكامل مصادر الأحداث الخارجية مع إنشاء موصلات إضافية مجانًا بواسطة فريق Kaspersky Professional Services.

استعلامات بحث سريعة وتقارير جاهزة عن أحداث الأمان.

تخزين محلي آمن للسجلات للامتثال التنظيمي والتحقيق في الحوادث.

يدعم Kaspersky SIEM عمليات البحث عن الأحداث عبر وحدات تخزين متعددة لمساعدة المشغلين في العثور على الأحداث ذات الصلة في مجموعات التخزين الموزعة بشكل أسرع وأسهل.

يتيح Kaspersky SIEM الإدارة المركزية للأصول من خلال توفير مخزون كبير من الخوادم ومحطات العمل وأجهزة الشبكة. وتستطيع المنصة جمع البيانات عن الثغرات الأمنية في الأصول من مصادر مثل أدوات فحص الثغرات الأمنية وربطها ببيانات فئة الأصول لتحديد التهديدات. ويوفر هذا لفرق الأمن رؤية واضحة للمشهد الكامل للأصول.

الارتباط في الوقت الحقيقي والتاريخي لأحداث الأمان

ينفذ نظام Kaspersky SIEM ربطًا متبادلاً في الوقت الحقيقي تقريبًا باستخدام قواعد مخصصة لتحديد الهجمات والتهديدات ومئات القواعد المحددة مسبقًا التي طوّرها فريق Kaspersky SOC، أحد أكثر فرق البحث عن التهديدات النشطة نجاحًا وخبرة في هذا المجال. ويحمل خبراء Kaspersky SOC العديد من الشهادات التي تؤكد المستوى العالي من الخبرة والمعرفة.

يتم **ربط الأحداث في الوقت الحقيقي**. وتحلل أداة الترابط الأحداث الموحدة، وتنشئ تنبيهات وفقًا لقواعد الارتباط، وتتعامل مع جميع عمليات القائمة النشطة.

يعتمد مبدأ تشغيل أداة الارتباط على تحليل توقيع الحدث، مما يعني أنه يتم التعامل مع كل حدث وفقًا لقواعد الارتباط التي يحددها المستخدم. وينشئ البرنامج حدث ارتباط ويرسله إلى التخزين عندما يعثر على سلسلة من الأحداث التي تفي بمتطلبات قاعدة الارتباط. ويمكن للمستخدم تخصيص قواعد الارتباط ليتم تشغيلها من خلال نتائج تحليل سابق عن طريق إرسال حدث الارتباط إلى أداة الربط لإجراء تحليل إضافي. ويمكن استخدام نتائج قاعدة الارتباط بواسطة قواعد ارتباط أخرى. على سبيل المثال، يمكن أن تؤدي عدة تنبيهات ثانوية إلى إنشاء تنبيه أكبر (قد يتم تحليل عدة محاولات تخمين لاكتشاف حادث تخمين جماعي).

تستخدم المنصة البيانات التاريخية لتحديد الاتجاهات، والعثور على التهديدات التي لم يتم تحديدها من قبل، وتحديد الهجمات التي تم التغاضي عنها بواسطة عناصر أمان معينة، ويعمل كل ذلك على تحسين الاكتشاف الشامل للتهديدات.

تتولى حلول الجهات الخارجية أو المنتجات المدمجة مثل **Kaspersky Endpoint Detection and Response** تنفيذ عملية الاكتشاف في جانب أداة الاستشعار. ومن خلال ضبط إعدادات المنتج، يستطيع المستخدمون التحكم في هذه العملية والحصول على الأحداث والقياس عن بعد التي قامت هذه المنتجات بمعالجتها بالفعل من خلال منطق الكشف الخاص بها.

يشتمل محرك الارتباط الخاص بالحل على الاكتشاف في جانب المنصة. وبفضل محرك الارتباط القوي للمنصة، يمكن للمستخدمين إنشاء قواعد ارتباط قابلة للتكيف. وتتوفر أيضًا القواعد الجاهزة وحزم أداة التوحيد لدعم منتجات الأطراف الخارجية التي يمكن الوصول إليها تجاريًا والتي يتم توسيعها وتحديثها باستمرار.

لدعم المحللين، يتم عرض تغطية مصفوفة MITRE ATT&CK حسب القواعد لتقييم مستوى الأمان بشكل أفضل.

أكثر من 650 قاعدة ارتباط تم تكوينها مسبقًا لاكتشاف سيناريوهات الهجوم، ويتم تحديثها بانتظام بواسطة خوادم Kaspersky باستخدام التعيين بواسطة MITRE وتوصيات الاستجابة.

تحسين ملاءمة البيانات من خلال إثرائها بالبيانات التحليلية المجمعة من Kaspersky Threat Intelligence Portal (باستخدام Kaspersky Threat Lookup Kaspersky CyberTraceg).

يتم جمع البيانات حول الأصول والبنية التحتية من Kaspersky Security Center ومصادر خارجية.

يستطيع المستخدمون مقارنة حدث ما بقيم مجمعة ومتراكمة ومتوسطة وقصوى ودنيا لفترة زمنية محددة باستخدام وظيفة استخراج البيانات ClickHouse. ويؤدي هذا إلى توسيع قدرات منطق الاكتشاف بشكل كبير دون الحاجة إلى إنشاء العديد من قواعد الخدمة.

لتسهيل إنشاء المحتوى وتحريره، نسمح للمستخدمين بمعرفة قواعد الارتباط التي سيتم تطبيق التغيير المقصود عليها مسبقًا قبل إجراء أي تغييرات على معايير التصفية.

يعتمد مبدأ تشغيل أداة الارتباط على تحليل توقيع الحدث، مما يعني أنه يتم التعامل مع كل حدث وفقًا لقواعد الارتباط التي يحددها المستخدم. وينشئ البرنامج حدث ارتباط ويرسله إلى التخزين عندما يعثر على سلسلة من الأحداث التي تفي بمتطلبات قاعدة الارتباط.

تعقب التهديدات لاكتشاف التهديدات التي لم تكن معروفة من قبل من خلال السماح للمشغلين بتحليل البيانات التاريخية وربطها باستخدام قاعدة بيانات قوية موجهة نحو الأعمدة.

يستطيع المستخدمون بسهولة تحديد موقع عوامل التصفية والقواميس والقواعد التي يتم توحيدها جميعًا بعلامة واحدة باستخدام وظيفة البحث المستندة إلى العلامة. ويتيح تخزين سجل استعلامات البحث للمستخدم إمكانية الوصول إلى الاستفسارات السابقة بسهولة.

يمكن للمنصة تخزين البيانات لفترة طويلة دون تجاوز الميزانية المخصصة لأجهزة التخزين باهظة الثمن بفضل خيارات التخزين المتصلة بالشبكة وغير المتصلة بالشبكة باستخدام ClickHouse ونظام الملفات الموزعة (Hadoop (HDFS أو الأقراص المحلية.

يمكن للمسؤولين منع مشكلات المساحة في النظام الفرعي للقرص باستخدام إعدادات مرنة: يمكن ضبط عمق تخزين الأحداث بالجيجابايت كنسبة مئوية من مساحة القرص، بالإضافة إلى الأيام.

تخزين بيانات أحداث الأمان

يتم استخدام مكون التخزين في Kaspersky SIEM لتخزين الأحداث الموحدة للوصول إلى البيانات التحليلية بسرعة وبشكل مستمر من **Kaspersky Unified Monitoring and Analysis Platform**.

يضمن ClickHouse الاستمرارية وسرعة الوصول. ويتم توصيل التخزين بخدمة تخزين Kaspersky SIEM عبر مجموعة ClickHouse. ويمكن أيضًا إضافة أقراص التخزين غير الموصلة بالشبكة إلى مجموعات ClickHouse.

يستطيع المستخدمون إضافة مساحة في المستودعات لتجميع الأحداث المخزنة بناءً على سمة محددة. ويتيح ذلك للمسؤولين تعيين أوقات تخزين مختلفة للأحداث بناءً على خصائصها المحددة.

ويتعامل نظام Kaspersky Unified Monitoring and Analysis Platform أيضًا مع ضغط البيانات لتقليل استخدام مساحة القرص بشكل كبير دون المساس باسترجاع البيانات. ويدعم حل Kaspersky منطقتين: واحدة لاسترجاع البيانات بسرعة والأخرى لتخزين كمية كبيرة من البيانات.

تحتوي المنصة على قسمين متميزين: أحدهما للتخزين دون الاتصال بالشبكة الذي يمكن تحقيقه على نظام الملفات الموزعة Hadoop أو الأقراص المحلية، والآخر للتخزين التشغيلي باستخدام ClickHouse. ويكون هذا الفصل شفافًا بالنسبة للمستخدمين.

يمكن للمشغلين، بدون الاضطرار إلى التنقل بين الأرشيفات، إنشاء استعلامات بحث في واجهة واحدة وتركيز جهدهم الكامل على التحقيق. و**يقلل هذا من تكلفة ملكية النظام** مع الحفاظ على تجربة مستخدم ممتازة. وتدعم المنصة عمليات البحث عن الأحداث عبر وحدات تخزين متعددة لمساعدة المشغلين في العثور على الأحداث ذات الصلة في مجموعات التخزين الموزعة بشكل أسرع وأسهل.

يمكن للمؤسسات أن تظل متوافقة مع المتطلبات التنظيمية للاحتفاظ بالبيانات والتدقيق والتحقيق في الحوادث من خلال جمع السجلات وتخزينها بشكل آمن من مجموعة متنوعة من المصادر. بالإضافة إلى ذلك، يسهل التخزين المركزي والمنظم على الشركات استرداد السجلات وتحليلها حسب الحاجة.

قدرات الاستجابة المتكاملة

تعمل وظيفة الاستجابة المضمنة باستخدام منتجات Kaspersky على زيادة كفاءة الأمان. على سبيل المثال، لتوسيع قدرات الاستجابة لنقطة النهاية، يمكن دمج Kaspersky SIEM مع Kaspersky Endpoint Detection and Response لإدارة عزل الشبكة للأصول وقواعد الوقاية أو تنفيذ التطبيقات والبرامج النصية. ويمكن تنفيذ إجراءات الاستجابة هذه يدويًا أو تلقائيًا على الأصول باستخدام عميل Kaspersky Endpoint Security.

يمكن أن يساعد جمع معلومات المخزون الآلي (البرمجيات المثبتة، والثغرات الأمنية، والمعدات، ومالكو الأصول، وما إلى ذلك) في وضع أحداث أمان المعلومات في سياقها والمساعدة في التحقيقات في الحوادث.

يستفيد Kaspersky SIEM من منصة Kaspersky CyberTrace، وهي منصة متكاملة المزايا لمعلومات التهديدات تدعم العشرات من موجزات بيانات التهديدات الجاهزة (التجارية والعامة) لإثراء الأحداث تلقائيًا في الوقت الحقيقي بمعلومات سياقية حول مؤشرات الاختراق.

تتيح مكونات الذكاء الاصطناعي في Kaspersky SIEM الاكتشاف السريع للأنشطة المشبوهة في البنية التحتية

أدوات الذكاء الاصطناعي والتعلم الآلي

تستخدم Kaspersky خوارزميات تنبؤية وتقنيات التجميع والشبكات العصبية وتقنيات النمذجة الإحصائية والخوارزميات المتخصصة لزيادة فعالية منتجاتنا في اكتشاف التهديدات بشكل أسرع وتحديد أولويات الاكتشافات بدقة.

يمكن لفرق المراقبة والاستجابة إعطاء الأولوية للتنبيهات والتركيز على منع الأضرار المحتملة، والتحقق منها من خلال البيانات الضخمة وأنظمة الذكاء الاصطناعي. وتساعد وحدة الذكاء الاصطناعي في الفرز من خلال تحليل البيانات التاريخية، وتحديد أولويات التنبيهات الواردة وتوفير درجات المخاطر المستندة إلى الذكاء الاصطناعي للأصول. ويساعد هذا الأسلوب في إنشاء فرضيات قيمة يمكن استخدامها في عمليات البحث الاستباقية.

تستخدم المنصة قواعد الارتباط المحددة من قبل المستخدم لربط الأحداث في الوقت الحقيقي. وتطبق وحدة الارتباط الخاصة بها خوارزميات الذكاء الاصطناعي لاكتشاف الأنشطة الشاذة مثل الارتفاع المفاجئ في حركة المرور أو الوصول المتعدد للخدمة مما يشير إلى وقوع حادث محتمل، مما يسمح بالاكتشاف المبكر قبل حدوث الضرر.

يتضمن Kaspersky SIEM أيضًا بيانات من Kaspersky Threat Intelligence، والتي تم إنشاؤها باستخدام تقنيات الذكاء الاصطناعي والبيانات الضخمة. ويتم إثراء قاعدة البيانات بشكل مستمر بنتائج التحليل اليدوي للتهديدات المستمرة المتقدمة (APT)، والبيانات التشغيلية للويب المظلم، والمعلومات من Kaspersky Security Network، والرؤى المستمدة من التحليل المنتظم للبرامج الضارة الجديدة.

تساعد كل هذه التقنيات المستخدمين على تقليل الضرر المحتمل الناجم عن الحوادث الإلكترونية، وزيادة متوسط الوقت للاكتشاف (MTTD) ومتوسط الوقت للإصلاح (MTTR).

يقدم التصور المتميز مع لوحات المعلومات والتقارير البيانات بالتنسيقات الأكثر استخدامًا لتحديد الاتجاهات والأنماط والأحداث الشاذة.

بفضل الأدوات المصغّرة القابلة للتخصيص لتصور المؤشرات وعرضها بسهولة، يمكن للمحللين تحديد أولويات الحوادث وتحديد الأسباب الجذرية والاستجابة للتهديدات بشكل أكثر كفاءة، بينما يمكن للمؤسسات تتبع فعالية عملياتها الأمنية وتحديد الاتجاهات وتقييم السلامة العامة لنظامها الأمني.

يستطيع المستخدمون إثراء بيانات حقل الحدث بمحتويات القواميس والجداول والأصول وسمات الحساب واستخدام هذه البيانات للبحث والتصور. ويساعد ذلك في إنشاء لوحات معلومات وتقارير تحتوي على المزيد من البيانات السياقية.

يساعد هذا الحل المستخدمين على إنشاء عناصر واجهة المستخدم الخاصة بهم باستخدام إعدادات قابلة للتعديل، بالإضافة إلى تخطيطات مع **مجموعات عناصر واجهة مستخدم مختلفة:**

مقاييس التنبيه الرئيسية
(الخطورة والأولوية والحالة)

- الأصول المتضررة
- الإخطارات الأخيرة
- أهم مصادر البيانات التي تحتوي على أكبر عدد من التنبيهات
- التنبيهات المخصصة لمشغلين محددين
- المستخدمون و/أو الأجهزة المتضررة
- التنبيهات بواسطة السياسة

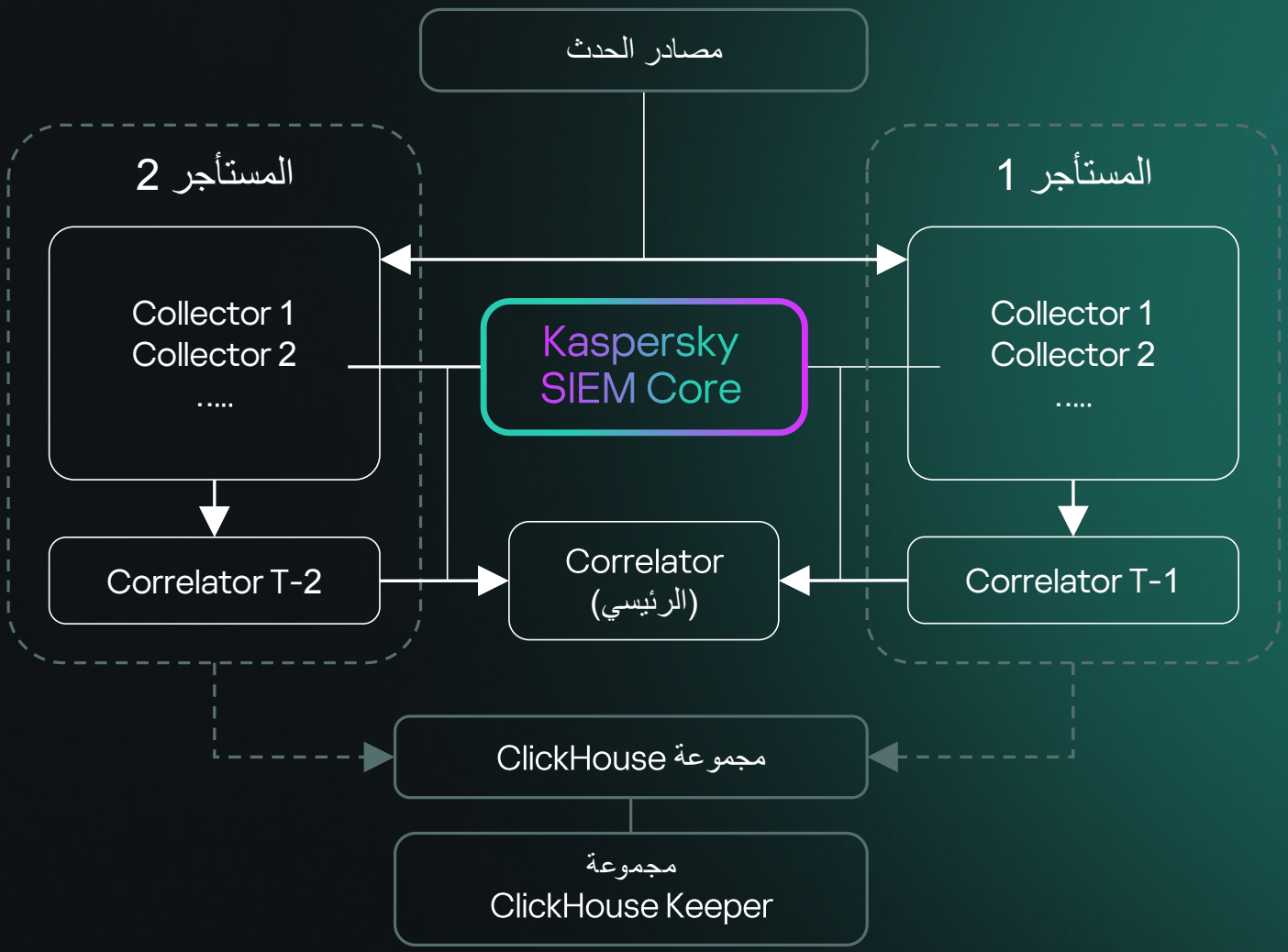
مؤشرات الحادث الرئيسي
(الشدة والتخصيص)

- الأجهزة المتضررة
- أعلى عناوين IP داخلية وخارجية حسب حجم حركة مرور NetFlow (Bytesln)
- أعلى عقد للإدارة عن بعد
- (منافذ 3389، 22)
- إجمالي بايت NetFlow للمنافذ الداخلية
- أهم المصادر بناءً على عدد الأحداث والفئات والأصول والمستخدمين

بنية تعدد الإيجارات

يوفر Kaspersky SIEM دعمًا كاملاً متعدد المستأجرين، مما يعني أن المستخدمين لدى أحد المستأجرين لا يمكنهم رؤية البيانات (الأحداث، والتنبيهات، والحوادث، وما إلى ذلك) الخاصة بمستأجر آخر. وفي وضع تعدد الإيجارات، يتيح مثيل واحد لتطبيق Kaspersky SIEM الذي تم نشره في المؤسسة الرئيسية عزل الفروع بحيث تتلقى الأحداث الخاصة بها وتعالجها.

تتم إدارة النظام مركزيًا عبر الواجهة الرئيسية، ويعمل المستأجرون بشكل مستقل مع إمكانية الوصول فقط إلى الموارد والخدمات والإعدادات الخاصة بهم. ويتم تخزين الأحداث المتعلقة بالمستأجر بشكل منفصل. ويمكن للمستخدمين الوصول إلى العديد من المستأجرين في وقت واحد. ويمكن للمسؤول العام أيضًا تحديد بيانات المستأجر التي سيتم عرضها في أجزاء مختلفة من واجهة الويب.



توفر المنصة نظامًا قائمًا على التصفية لتوزيع الأحداث على المساحات. وتم الآن تعيين وصول المستخدم إلى الأحداث على مستوى المساحة. ويتيح ذلك التحكم الدقيق في الوصول إلى الأحداث داخل مستأجر واحد.

تتم إدارة النظام مركزيًا من خلال الواجهة الرئيسية بينما يعمل المستأجرون بشكل مستقل عن بعضهم البعض ولا يمكنهم الوصول إلا إلى الموارد والخدمات والإعدادات الخاصة بهم. ويتم تخزين أحداث المستأجرين بشكل منفصل.

مجموعة واسعة من عمليات التكامل الجاهزة

تم دمج Kaspersky Unified Monitoring and Analysis Platform بشكل كامل مع حلول وتقنيات Kaspersky للاستخدام المنسق للمنتجات بكفاءة محسنة. ولا يمكن لموردي الجهات الخارجية مطابقة مستوى التكامل السلس الخاص بنا مع منتجاتنا الخاصة، التي تتضمن واجهة واحدة لتكامل معلومات التهديدات، والقدرة على استخدام مستشعرات نقطة النهاية الخاصة بنا كعملاء لإدارة معلومات الأمان والأحداث (SIEM)، وغير ذلك الكثير.

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response *

Kaspersky Security Center

Kaspersky Secure Mail Gateway

Kaspersky Web Traffic Security

Kaspersky Threat Lookup

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Automated Security Awareness Platform

وغير ذلك

يساعد التكامل مع المجموعة الغنية من خدمات **Kaspersky Threat Intelligence** في تحديد التهديدات وترتيب أولوياتها والوصول السريع إلى المعلومات السياقية حول الهجمات الجديدة ومؤشرات الاختراق وتكتيكات المهاجمين وتقنياتهم.

* يتضمن عمليات تكامل محتملة مع Kaspersky Endpoint Detection and Response Expert وKaspersky Endpoint Detection and Response Optimum وKaspersky Next EDR Foundations وKaspersky Next EDR Optimum وKaspersky Next EDR Expert.

يتفوق Kaspersky SIEM في تلقي البيانات (السجلات) من الأنظمة والأجهزة الأخرى. ولتسهيل التنفيذ السريع دون النفقات الإضافية لإعداد قواعد تحليل المصدر، تأتي المنصة مزوّدة بمجموعة واسعة من عمليات التكامل الجاهزة لمنتجات Kaspersky ومنتجات الجهات الخارجية:

حسب مجال الأمان

- حماية نقطة النهاية (حلول EDR و EPP)
- حماية البريد الإلكتروني وحركة مرور الويب (حماية البريد الإلكتروني، NDR، FW / NGFW، UTM، IDS)
- الوعي الأمني
- عبء العمل السحابي (CASB، CWPP)
- معلومات التهديدات (CTI)
- أمان الهوية (IAM، PAM)
- أمان التكنولوجيا التشغيلية / إنترنت الأشياء
- منع فقدان البيانات (DLP)

حسب نوع البيانات

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- Key-Value
- RegExp
- NetFlow v5
- NetFlow v9
- IPFIX

حسب نوع النقل

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL (SQLite، MSSQL، MySQL، PostgreSQL، Cockroach، Oracle، Firebird، ClickHouse، Elasticsearch)
- File
- Diode
- FTP
- NFS
- WMI
- WEC
- ETW (تحليلات DNS)
- SNMP
- SNMP Traps
- VMware API
- MS Office 365

حسب البائع

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMware
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- وما إلى ذلك

يمكن تطوير عمليات تكامل إضافية بواسطة فريق Kaspersky Professional Services أو شركائه، بما في ذلك استخدام واجهات برمجة التطبيقات (APIs) الخاصة بالمنتجات القابلة للاتصال. تفضل بالاطلاع على القائمة الكاملة لمصادر الأحداث المدعومة.

القائمة الكاملة

الدعم المتميز لحل Kaspersky SIEM

يأتي الدعم المتميز من Kaspersky Premium Support لحل Kaspersky SIEM مزودًا بترخيصي Premium وPremium Plus، مما يضمن الاستجابة السريعة والمساعدة عالية الجودة لأية مشكلات للحفاظ على تشغيل Kaspersky SIEM بسلاسة

Kaspersky Premium Support

	الدعم القياسي	ترخيص Premium	ترخيص Premium Plus
الاتصالات			
حساب الشركة (بوابة الويب)	●	●	●
الهاتف		●	●
البريد الإلكتروني		●	●
الخدمة			
أدوات التحليل المخصصة لحل Kaspersky SIEM		5	10
المساعدة عن بعد لتشخيص المشاكل		●	●
أولوية تصعيد طلبات الدعم		عالي	الأعلى
التصحيح الخاص			●
مدير حساب فني مخصص (TAM)			●
تقارير الحالة من مدير الحساب الفني المخصص			تقرير ربع سنوي
أوقات الاستجابة			
المشاكل الحرجة	لا توجد اتفاقية مستوى الخدمة	ساعتان (على مدار الساعة)	30 دقيقة (على مدار الساعة)
المشكلات عالية المستوى	لا توجد اتفاقية مستوى الخدمة	6 ساعات (أوقات العمل في أيام العمل)	4 ساعات (على مدار الساعة)
المشكلات متوسطة المستوى	لا توجد اتفاقية مستوى الخدمة	8 ساعات (أوقات العمل في أيام العمل)	6 ساعات (أوقات العمل في أيام العمل)
المشكلات منخفضة المستوى	لا توجد اتفاقية مستوى الخدمة	10 ساعات (أوقات العمل في أيام العمل)	8 ساعات (أوقات العمل في أيام العمل)

استجابة سريعة

يتم تحديد أولويات الطلبات من خلال اتفاقيات مستوى الخدمة الصارمة لحل المشكلات بشكل أسرع وموثوق

أدوات تحليل مخصصة

تقوم أدوات التحليل المخصصة بتمكين إدارة معلومات الأمان والأحداث (SIEM) من معالجة تنسيقات السجل الفريدة من مصادر البيانات المحددة الخاصة بك

مدير حساب فني مخصص

باستخدام ترخيص Premium Plus، يدير مدير الحساب الفني المخصص جميع المشكلات بمسؤولية عالية

تصحيحات خاصة

احصل على إصلاحات وتصحيحات مخصصة، مصممة لمشاكل محددة، مع ترخيص Premium Plus

لماذا تختارنا؟

وفّر ما يصل إلى 50% من متطلبات تثبيت الأجهزة أو المحاكاة الافتراضية واخفض التكلفة الإجمالية للملكية مع حل معياري عالي الأداء يتفوق باستمرار على موردي حلول إدارة معلومات الأمان والأحداث (SIEM) القدامى من حيث كفاءة التكلفة ويمكنه التعامل مع مئات الآلاف من الأحداث في الثانية في كل مثيل.

حافظ على المرونة مع خيارات الترخيص الخاصة بنا. ونتتبع متوسط تدفق الأحداث في الثانية في اليوم بعد التجميع والتصفية للحد من التجاوزات وعدم تقييد الوصول إلى Kaspersky SIEM في حالة حدوثها.

استفد من مجموعة واسعة من عمليات التكامل مع كل من حلول Kaspersky والأطراف الخارجية مع خيارات الاستجابة المضمنة. ولا يمكن للموردين الآخرين مطابقة مستوى التكامل السلس الخاص بنا مع منتجاتنا الخاصة، التي تتضمن واجهة واحدة لتكامل معلومات التهديدات، والقدرة على استخدام مستشعرات نقطة النهاية الخاصة بنا كعملاء لإدارة معلومات الأمان والأحداث (SIEM)، وغير ذلك الكثير.

يمكنك تخزين البيانات محليًا بتكلفة منخفضة وبدون تجاوز الميزانية لفترة طويلة باستخدام خيارات التخزين المتصلة بالشبكة وغير المتصلة بالشبكة باستخدام ClickHouse ونظام الملفات الموزعة (HDFS Hadoop) أو الأقراص المحلية، مع القدرة على البحث بسرعة عبر كلا المنطقتين في وقت واحد.

تحسين ملاءمة البيانات وتسريع الاكتشاف والفرز بفضل الإثراء بمعلومات التهديدات التكتيكية والتشغيلية والإستراتيجية التي يوفرها فريق الباحثين والمحللين الرائد عالميًا عبر Kaspersky Threat Intelligence Portal.

استفد من تعدد الإيجارات المضمن باستخدام مزود خدمة الأمن المدارة (MSSP) والحل الجاهز للمؤسسات الكبيرة الذي يوفر دعمًا أصليًا لتعدد الإيجارات حيث يتيح تثبيت حل واحد لإدارة معلومات الأمان والأحداث (SIEM) في البنية التحتية الرئيسية للمؤسسات إنشاء حل معزول لإدارة معلومات الأمان والأحداث (SIEM) للمستأجرين الذين يتلقون الأحداث الخاصة بهم ويعالجونها.

استخدمت Kaspersky حل إدارة معلومات الأمان والأحداث (SIEM) الخاص بها لاكتشاف البرامج الضارة غير معروفة سابقًا التي تستهدف أجهزة iOS

أثناء مراقبة حركة مرور الشبكة لشبكة Wi-Fi الخاصة بشركتنا والمخصصة للأجهزة المحمولة باستخدام Kaspersky Unified Monitoring and Analysis Platform، اكتشفنا نشاطًا مشبوهًا مصدره هواتف متعددة تعمل بنظام iOS.

نظرًا لأنه من المستحيل فحص أجهزة iOS الحديثة من الداخل، فقد أنشأنا نسخًا احتياطية دون اتصال بالإنترنت للأجهزة المعنية، وقمنا بفحصها باستخدام mvt-ios الخاص بمجموعة أدوات التحقق من الأجهزة المحمولة واكتشفنا آثار الاختراق.

استجابت شركة Apple بإصدار تحديثات أمنية لمعالجة أربع ثغرات أمنية فورية حددها باحثون في Kaspersky:

CVE-2023-32434، CVE-2023-32435، CVE-2023-38606، CVE-2023-41990

تؤثر هذه الثغرات الأمنية على مجموعة واسعة من منتجات Apple، بما في ذلك أجهزة iPhone iPodg iPadg وأجهزة macOS وأجهزة Apple TV وساعات Apple. أبلغت Kaspersky شركة Apple باستغلال إحدى ميزات الأجهزة، والتي قامت الشركة بتخفيفها لاحقًا.

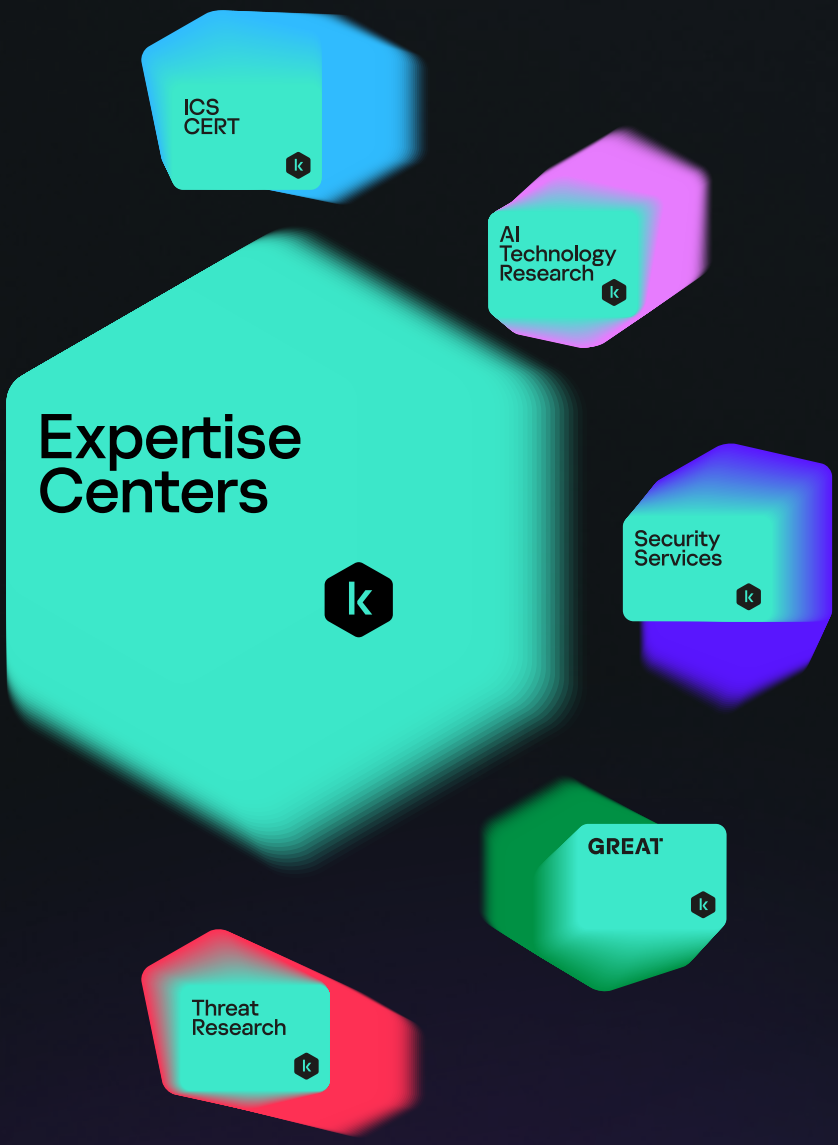
تعتمد الشركات في جميع أنحاء العالم على إدارة معلومات الأمان والأحداث (SIEM) لتطوير عمليات شاملة لأمان المعلومات تعزز كفاءة الأمن الإلكتروني.

معرفة المزيد

لماذا Kaspersky؟

يستفيد Kaspersky SIEM من سنوات من المعرفة المتراكمة والمهارات المحسنة لمراكز الخبرة الخمسة.

معرفة المزيد



27

منذ **أكثر من 27 عامًا** نبني الأدوات ونقدم الخدمات للحفاظ على سلامتك من خلال تقنياتنا الأكثر اختبارًا والأكثر حصدًا للجوائز.

معرفة المزيد

نحن **شركة عالمية خاصة للأمن الإلكتروني** ولدينا آلاف العملاء والشركاء حول العالم، وملتزمون بالشفافية والاستقلالية.

معرفة المزيد

Kaspersky Unified Monitoring and Analysis Platform

معرفة المزيد

#kaspersky
#bringonthefuture

me.kaspersky.com