kaspersky واجِهوا المستقبل بأمان

Kaspersky

Kaspersky Unified Monitoring and Analysis Platform

صفحة البيانات

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.

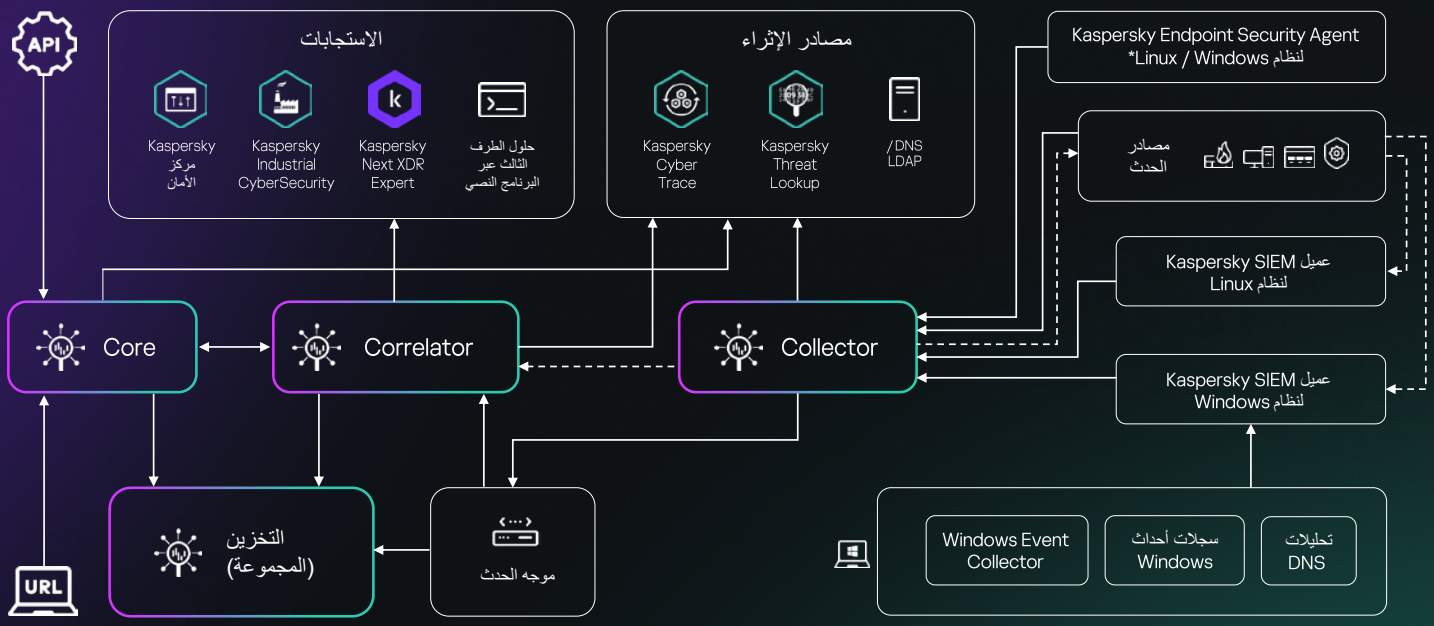
من خلال دمج منتجات الأطراف الخارجية ومنتجات Kaspersky في نظام مركزي لأمان المعلومات، يعد Kaspersky SIEM جزءًا أساسيًا من إستراتيجية دفاعية شاملة قادرة على تأمين البيئات المؤسسية والصناعية، بالإضافة إلى اكتشاف الهجمات الإلكترونية التي تبدأ في مجال تكنولوجيا المعلومات وتنتقل إلى أنظمة التكنولوجيا التشغيلية.

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.



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.

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

me.kaspersky.com

#kaspersky
#bringonthefuture

© 2024 AO Kaspersky Lab.
العلامات التجارية المسجلة وعلامات الخدمة مملوكة لأصحابها.