kaspersky

XDR مقابل MDR مقابل EDR

XDR
Extended Detection and Response

يكتشف بشكل استباقي التهديدات المعقدة عبر مستويات البنية التحتية المتعددة، ويستجيب تلقائيًا لهذه التهديدات ويواجهها

MDR
خدمة الاكتشاف و الاستجابة المدارة

يوفر حماية مُدارة ومستمرة حتى ضد التهديدات غير الضارة الأكثر تعقيدًا وابتكارًا

EDR
Endpoint Detection and Response

يتعرف على التهديدات الجديدة وغير المعروفة والمراوغة التي تتجاوز حماية نقطة النهاية، وينفذ أتمتة مهام الأمان الروتينية

طريقة العمل

- يتيح الاكتشاف المتقدم ومطاردة التهديدات التي تتجاوز آليات الوقاية
- يعزز رؤية التهديد وتصوره
- يُبسط تحليل السبب الجذري
- يوفر استجابة مركزية وآلية

- يجمع القياس عن بعد من منتجات الأمان، ويحلل البيانات التعريفية لنشاط النظام بشكل استباقي للبحث عن أي علامات على وجود هجوم نشط أو وشيك، ويوفر استجابة مُدارة أو موجهة

- يدمج أدوات متعددة وتطبيقات الأمان
- يراقب البيانات الموجودة على نقاط النهاية والشبكات والسحابات وخوادم الويب وخوادم البريد، وما إلى ذلك، لاكتشاف التهديدات المعقدة والقضاء عليها
- يُبسط إدارة أمان المعلومات من خلال أتمتة التفاعل بين المنتجات

ما المؤسسات التي يناسبها؟

- الشركات التي تضم فريقًا داخليًا لأمان تقنية المعلومات التي تتطلب رؤية دقيقة لنقطة النهاية واستجابة مركزية لتقليل مهام المعالجة اليدوية

- الشركات التي تسعى إلى توسيع القدرة الداخلية لأمان تقنية المعلومات من خلال رفع عبء مهام الاكتشاف والاستجابة الرئيسية
- المؤسسات التي قد لا تمتلك الميزانية أو الموظفين المتخصصين المتاحين لبناء مركز عمليات الأمن الداخلي الخاص بها

المؤسسات الناضجة من حيث الأمان التي ترغب في الحصول على منصة واحدة تقدم ما يلي:

- صورة متماسكة لما يحدث في كل أرجاء البنية التحتية لديهم
- مدمج في صيد التهديدات ومعلومات التهديدات
- تحديد أولويات عليا للحوادث وعدد أقل من التنبيهات الإيجابية الكاذبة

قيمة الأعمال

- يمنح العاملين في مجال الأمان الرؤية الموحدة والتحكم الذي يحتاجون إليه للبحث عن التهديدات بشكل فعال بدلاً من انتظار التنبيهات
- يعمل على تعظيم قدرات فرق أمان تقنية المعلومات الحالية من خلال أتمتة مجموعة من عمليات التحليل والتحقيق والاستجابة
- يعزز كفاءة التكلفة من خلال تمكين فرق أمان تقنية المعلومات من العمل بشكل أكثر فعالية دون الحاجة إلى التوفيق بين أدوات ووحدات تحكم متعددة

- يحل أزمة الكفاءة في مجال الأمن الإلكتروني مما يضمن الحماية الفورية ضد التهديدات المعقدة
- يتيح الاستعانة بمصادر خارجية لتنفيذ عمليات إدارة الحوادث لتركيز المصادر الداخلية المحدودة والمكلفة بشكل أفضل على النتائج المهمة التي يتم تحقيقها
- يقلل من تكاليف الأمان الإجمالية دون الحاجة إلى نشر حلول أمنية معقدة وتوظيف مجموعة من المتخصصين في مجال الأمان الداخلي

- يوفر حماية شاملة ضد مشهد التهديدات المتطور
- يزيد نهج النظام البيئي كفاءة أدوات الأمن الإلكتروني المعنية ويوفر في الموارد ويقلل من المخاطر
- يُبسط عمل متخصصي أمان تكنولوجيا المعلومات ويمنحهم السياق الإضافي اللازم للتحقيق في الهجمات متعددة المتجهات
- يقلل من متوسط الوقت للاكتشاف (MTTD) ومتوسط الوقت للإصلاح (MTTR) - وهو أمر ضروري في مكافحة التهديدات المعقدة والهجمات المستهدفة
- يتيح الاستجابة المركزية والآلية عبر مجموعة تقنيات الأمان بأكملها

إذا كانت مؤسستك مؤسسة ناضجة من حيث الأمان تتطلع إلى الاستفادة من إمكانات XDR، تفضل بإلقاء نظرة على

Kaspersky Expert Security

معرفة المزيد