Kaspersky Next XDR Expert

أكبر وأفضل وأسرع بكثير

kaspersky

هل هو حل يغير قواعد اللعبة، أو مجرد تغيير بسيط؟

XDR: الاكتشاف والاستجابة الموسعة

هو الاختصار الذي يدور على ألسنة الكثير من الناس، لكن على غرار جميع التقنيات الحديثة نسبيًا، لا يعرف الجميع بالضبط ما هو هذا الحل أو ما يمكن أن يفعله لأعمالهم. يوجد شيء واحد مؤكد، وهو أن حل XDR ينطوي على تحول إستراتيجي من التفاعل إلى الاستباقية، لأن مبدأ "الانتظار والترقب" لا ينطبق على الأمن الإلكتروني. وتنظر الأموال الذكية إلى حل XDR كإستراتيجية وليس مجرد منتج.

هل XDR مجرد أحدث صيحة تقنية تبحث عن إحداث تغيير بسيط، أو حل يغير قواعد اللعبة؟ من المؤكد أن المشاكل موجودة، بدءًا من النقص العالمي في المهارات، وموظفي أمان تقنية المعلومات المثقلين بالعمل، ومشهد التهديدات الذي لا يتوقف أبدًا، إلى التنبيه من الحمل الزائد، والأدوات المتباينة، وضعف معلومات التهديد، واتساع سطح الهجوم. وتقول شركة IDC إن حل XDR سيكون "قوة تغيير كبيرة تؤثر على مبيعات إدارة معلومات الأمان والأحداث (SIEM) ونقطة النهاية والاستجابة لها (EDR) والبنية الموجهة للخدمات (SOAR)، ومعلومات الشبكات، ومنصات تحليلات التهديدات، بالإضافة إلى مقدمي معلومات التهديدات الخارجية"[1]، وتعتقد شركة Forrester أن تقنية XDR المتميزة "ستحل محل اكتشاف نقطة النهاية و الاستجابة لها (EDR) على المدى القصير وستستولي على مكانة إدارة معلومات الأمان والأحداث (SIEM) على المدى الطويل"[2].

من المستهدف بحل XDR؟

حل مخصص للمؤسسات ذات XDR الوضع الأمني المتطور، التي تحتاج إلى منصة واحدة لمنحها صورة كاملة ومتسقة عما يحدث في بنيتها التحتية.

من المستهدف بحل XDR - وما التحديات التي يمكن أن يحلها؟

XDR حل مخصص للمؤسسات ذات الوضع الأمني المتطور، التي تحتاج إلى منصة واحدة لمنحها صورة كاملة ومتسقة عما يحدث في بنيتها التحتية.

تتسم تحديات الأمن الإلكتروني التي تواجهها هذه المؤسسات بالثبات والرسوخ. أجرت مؤسسة ESG Research استطلاعًا بين متخصصي تقنية المعلومات والأمن الإلكتروني[3] في المؤسسات التي تضم 100 موظف أو أكثر، حيث كان أكثر من 80% منهم يعملون في مؤسسات، عبر قطاعات متعددة. وفيما يلي بعض النتائج الرئيسية:

حل XDR سيكون قوة تغيير كبيرة – IDC

المزيد من الأجهزة، المزيد من التطبيقات، المزيد من حركة مرور الشبكة، المزيد من البيانات، المزيد من التهديدات...

صعوبات في مواكبة المتطلبات التشغيلية لتقنيات مركز عمليات الأمن (SOC)

أصبحت إدارة عمليات الأمان الآن أكثر صعوبة من أي وقت مضى خلال العامين الماضيين، والسبب في ذلك الصعوبات في مواكبة الاحتياجات التشغيلية لتقنيات مركز عمليات الأمن (SOC) - قابلية التوسع في تدفق البيانات، ومحركات معالجة موازنة الحمل، وإضافة سعة التخزين، وما إلى ذلك.

[1] المصدر: تحليل منتجات الأمان العالمية من IDC: من Power Point إلى Power Product، أين يوجد حل XDR الآن؟ (2022)

[2] المصدر: Forrester، الاكتشاف والاستجابة الموسعة (XDR) - معركة بين القديم والابتكار، آلي ميلين، كبير محللين، 2021

[3] المصدر: تقرير بحثي حول الممارسات البيئية والاجتماعية وحوكمة الشركات، وتحديث مركز عمليات الأمن (SOC) ودور الاكتشاف والاستجابة الموسعة، 2022

سطح الهجوم المتنامي والمتغير باستمرار ومشهد التهديد بشكل عام

المزيد من الأجهزة، المزيد من التطبيقات، المزيد من حركة مرور الشبكة، المزيد من البيانات، المزيد من التهديدات. لا يزال مشهد التهديدات قائمًا، وتتطور التهديدات الإلكترونية باستمرار من حيث الحجم والتعقيد مع انتشار الأدوات الجديدة. وفي الوقت نفسه، أصبح العائق أمام دخول المخترقين أقل من أي وقت مضى، حيث يتواجد في أحد الجانبين المشترون ذوو المهارات المنخفضة الذين يشترون التهديدات المجمعة الرخيصة على شبكة الويب المظلم، وفي الطرف الآخر المخترقون ذوو المهارات العالية والصبورون الذين يبنون هجمات معقدة على الجانب الآخر. ولا تنس التهديدات الداخلية والثغرات الأمنية في سلسلة التوريد.

العدد الكبير من العمليات اليدوية المطلوبة لإدارة الأمان

يوجد قدر أكبر من بيانات الأمان التي يتعين جمعها ومعالجتها، ومن غير الناجح ومن غير الفعال معالجتها يدويًا. ويتسبب هذا في عاصفة كاملة تؤثر على قابلية التوسع، وتؤدي إلى اعتماد مفرط على المشاركة البشرية المباشرة، وتقلل من فعالية التعامل مع التهديدات بشكل عام.

عدم القدرة على تطوير قواعد الاكتشاف

عدم القدرة على تطوير قواعد الاكتشاف وضبط عناصر التحكم في الأمان وتحديد التهديدات والتعامل معها بسرعة وكفاءة، بسبب نقص الوقت والموارد والمهارات. ولا تمتلك المؤسسات دائمًا المهارات أو الموظفين المناسبين لمواكبة التحليلات وعمليات الأمان. مما يقودنا مباشرة إلى المشكلة التالية...

النقص الحقيقي في المهارات العالمية

على الرغم من أن القوى العاملة العالمية في مجال الأمن الإلكتروني وصلت إلى أعلى مستوى لها على الإطلاق وهو 4.7 مليون متخصص، إلا أنه لا تزال هناك فجوة قدرها 3.4 مليون بحاجة إلى سدها - لكن لم يتم سدها. وتنمو هذه الفجوة بسرعة مضاعفة مقارنة بالقوى العاملة، مع زيادة بنسبة 26.2% على أساس سنوي.[4]

[4] المصدر: (ISC)²، دراسة القوى العاملة في مجال الأمن الإلكتروني، 2022

أدوات غير مناسبة للغرض

عندما تصبح الأدوات نفسها جزءًا من المشكلة، لا بد من تقديم شيء ما. وتعاني الأدوات الحالية في الغالب من صعوبة في اكتشاف التهديدات المتقدمة والتحقيق فيها، ومع ذلك لا تزال هناك حاجة إلى مهارات متخصصة لاستخدامها وإدارتها. ويُظهر البحث[5] أن الأدوات الحالية تفتقر في الغالب للفعالية في ربط التنبيهات، ويواجه موظفو أمان تقنية المعلومات صعوبة في التعامل مع العديد من الأدوات المنفصلة والمتباينة التي تتعامل مع البيانات المتباينة. وهذا أمر غير فعال ومرهق وفوضوي ومكلف. ويتمثل التحدي الآخر في افتقار الأدوات الحالية للقدرة على توسيع نطاقها للتعامل مع سطح الهجوم الموسع، وهناك فجوات كبيرة في قدرات الاكتشاف والاستجابة السحابية.[6]

تعاني الأدوات الحالية في الغالب

من صعوبة في اكتشاف التهديدات المتقدمة والتحقيق فيها، ومع ذلك لا تزال هناك حاجة إلى مهارات متخصصة لاستخدامها وإدارتها.

هل من الغريب أن يبدو مدير أمان المعلومات لديك مضغوطًا؟

الخبر السار هو أن تحسين عمليات الأمان يمثل أولوية، ويتم تمويله - سوف تنفق 88% من المؤسسات المزيد هذا العام، وتقول 66% إن توحيد الأدوات يمثل أولوية، كما أن تطوير التطبيقات الحديثة ونشرها قد زاد من السرعة، مما يتطلب مهارات جديدة.[7]

%88

من المؤسسات ستنفق أكثر هذا العام على تحسين عمليات الأمان

%66

يقولون إن دمج الأدوات يمثل أولوية

ماذا يفعل حل XDR

إليك كيف يستطيع حل XDR التغلب على هذه التحديات.

يكتشف حل XDR التهديدات المتقدمة بشكل أفضل

تمتد قدرات اكتشاف التهديدات في حل XDR إلى نقاط النهاية والشبكات والبيئات السحابية. ويستخدم خوارزميات التعلم الآلي والتحليلات السلوكية لتحديد التهديدات المعقدة، بما في ذلك البرامج الضارة وبرامج طلب الفدية والتهديدات المستمرة المتقدمة (APTs).

الاستجابة الآلية وإجراءات العلاج

يعمل حل XDR على أتمتة إجراءات الاستجابة والمعالجة، مما يُمكن المؤسسات من احتواء التهديدات بسرعة وتقليل أي ضرر محتمل. ويمكنه عزل نقاط النهاية المخترقة أو فصلها تلقائيًا، وحظر الأنشطة الضارة، ومعالجة الثغرات الأمنية، مما يقلل الجهد اليدوي ووقت الاستجابة.

يتكامل مع أدوات حماية نقطة النهاية

يمثل التكامل مع حماية نقطة النهاية مشكلة رئيسية، ويستفيد حل XDR من القياس عن بعد لنقطة النهاية والتحليلات السلوكية لتوفير رؤى عميقة حول أنشطة نقطة النهاية. ويستخدم خوارزميات التعلم الآلي المتقدمة لتحديد السلوك المريب ومؤشرات الهجمات (IOA)، مما يسهل الاكتشاف المبكر للتهديدات المعقدة.

[5] المصدر: تقرير بحثي حول الممارسات البيئية والاجتماعية وحوكمة الشركات، وتحديث مركز عمليات الأمن (SOC) ودور الاكتشاف والاستجابة الموسعة، مايو 2022

[6] المصدر: تقرير بحثي حول الممارسات البيئية والاجتماعية وحوكمة الشركات، وتحديث مركز عمليات الأمن (SOC) ودور الاكتشاف والاستجابة الموسعة، 2022

[7] المصدر: تقرير بحثي حول الممارسات البيئية والاجتماعية وحوكمة الشركات، وتحديث مركز عمليات الأمن (SOC) ودور الاكتشاف والاستجابة الموسعة، مايو 2022

أين يتناسب حل XDR مع النظام البيئي لنقطة النهاية والاستجابة لها (EDR) والاكتشاف والاستجابة المُدارة (MDR) والتنسيق الأمني والاستجابة الآلية (SOAR) وإدارة معلومات الأمان والأحداث (SIEM)

الدليل موجود في حرف X الذي يرمز إلى "موسع". يوسع حل XDR القدرات التي يوفرها التنسيق الأمني والاستجابة الآلية (SOAR) لاكتشاف التهديدات المعقدة بشكل استباقي عبر مستويات البنية التحتية المتعددة، والاستجابة تلقائيًا لهذه التهديدات ومواجهتها.

النهج المتكامل هو المفتاح

من خلال دمج العديد من الأدوات وتطبيقات الأمان، ومراقبة البيانات على نقاط النهاية والشبكات والسحابة وخوادم الويب وخوادم البريد وغيرها، يفعل حل XDR المزيد لاكتشاف التهديدات والقضاء عليها مع تبسيط إدارة أمان المعلومات في الوقت نفسه من خلال أتمتة التفاعل عبر المنتجات.

تعتقد Forrester أنه في معظم الحالات، لن يستبدل حل XDR منصات تحليلات الأمان بشكل مباشر، مشيرة إلى أن "حل XDR في رحلة، ونتوقع أنه على مدى السنوات الخمس المقبلة، ستتصادم منصات تحليلات الأمان وXDR".

تتضمن إدارة معلومات الأمان والأحداث (SIEM) حالات استخدام مفيدة تتجاوز اكتشاف التهديدات، وقابلية تخصيص التنسيق الأمني والاستجابة الآلية (SOAR)، لكن عندما يتعلق الأمر باكتشاف التهديدات والاستجابة لها، تعد التحليلات المتقدمة للحماية المحسنة لحل XDR لا مثيل لها.

يوفر الرؤية في الوقت الحقيقي

يوفر حل XDR الرؤية في الوقت الحقيقي للوضع الأمني لمؤسستك. ويجمع البيانات ويحللها من مصادر مختلفة، مثل نقاط النهاية والخوادم وجدران الحماية والمنصات السحابية، لتقديم رؤى شاملة حول التهديدات المستمرة والأنشطة المشكوك فيها في وحدة تحكم واحدة. وهذا ما يجعله حلاً استباقيًا حقًا - البحث الاستباقي عن التهديدات والاستجابة الأسرع للحوادث. وتساعد النظرة الشاملة فرق الأمان على تحديد الأنشطة المشكوك فيها وحوادث الأمان المحتملة بشكل أكثر كفاءة.

تحديد سياق البيانات ومعلومات التهديدات

عندما يستفيد حل XDR من معلومات التهديدات عالية الجودة وقاعدة بيانات شاملة لمعلومات التهديدات، يوفر معلومات سياقية مفيدة للغاية حول التهديدات والمهاجمين. وتُبسط هذه المعلومات الذكية الغنية عن التهديدات تنبيهات التحقيق والتعامل مع الحوادث، وتساعد فرق الأمان على فهم أساليب وتقنيات ودوافع أطراف التهديد، مما يسهل الاستجابة الأكثر فعالية للحوادث وتدابير الدفاع الوقائي.

تمكين عمليات الأمان المبسطة

عند دمج أفضل الحلول بشكل صحيح فإنها ستتكامل مع بنيتك التحتية الحالية لتقديم أفضل النتائج من الأتمتة، وتعطي رؤية ووعيًا كاملين دون الحاجة إلى استبدال حلول الأمان من الأطراف الأخرى المستخدمة بالفعل. ولا تنس أنه من خلال توفير رؤية شاملة لحوادث الأمان وسلوك المستخدم، فإن التكامل يدعم الامتثال.

من الواضح أن حل XDR يمكنه تقديم التالي: التحكم والاستقرار وهذه الميزة بالغة الأهمية. لكن لا يتم إنشاء جميع عروض XDR على قدم المساواة ... كيف تختار العرض المناسب لك؟

5 أشياء أساسية يجب مراعاتها عند مقارنة بائعي XDR وحلول

إليك كيف يستطيع حل XDR التغلب على هذه التحديات.

1

توجد صلة مباشرة بين جودة حل XDR والتآزر بين حماية نقطة النهاية (EPP) ونقطة النهاية والاستجابة لها (EDR) الخاص بالبائع

يعد حل EDR للاكتشاف المتقدم والاستجابة للتهديدات الإلكترونية المتطورة على مستوى نقطة النهاية عنصرًا أساسيًا في حل XDR. وفي الوقت نفسه، يحتاج EDR إلى منصة قوية لحماية نقطة النهاية (EPP) لفرز الأعداد الهائلة من التهديدات الجماعية تلقائيًا. ومن الهام النظر بعناية في ميزات حماية نقطة النهاية، والتحقق من وجود دعم لكل أنواع نقاط النهاية - أجهزة الكمبيوتر الشخصية وأجهزة الكمبيوتر المحمولة والأجهزة الافتراضية والأجهزة المحمولة وأنظمة التشغيل المختلفة.

2

معلومات التهديدات الحديثة والرؤية الكاملة لأساليب وتقنيات مجرمي الإنترنت ضرورية لمواجهة التهديدات الإلكترونية

ليس الأمر صعبًا - أي حل XDR يستحق كل هذا العناء سيوفر كلا القدرتين، جنبًا إلى جنب مع سياق إضافي لتحسين وتسريع التحقيق في الحوادث والاستجابة لها.

3

التكامل مع حلول الأطراف الخارجية أكثر استدامة وفعالية من حيث التكلفة

يعد مدى تكامل حل XDR مع الأطراف الخارجية مشكلة أخرى بالغة الأهمية، لأن قابلية التشغيل البيني تجعل الشراء استثمارًا أكثر استدامة منذ البداية. وسيجمع حل XDR الذي يوفر العديد من خيارات التكامل الحقيقية المزيد من مصادر البيانات ويقدم صورة أكثر اكتمالاً لما يحدث في بنيتك التحتية.

4

المراجعات المستقلة والاعتراف العالمي ونتائج الاختبارات المستقلة مهمة

عندما تستثمر في شيء هام لعملك مثل الأمن الإلكتروني، لا تغفل التقييمات المستقلة. واسأل عن نتائج الاختبارات المستقلة. وتحقق من الاعتراف الدولي من شركات مثل Forrester وIDC وغيرها. وهل يتم تنفيذ الحلول على مستوى العالم؟ اسأل عن دراسات الحالة.

5

هل استثمارك متوافق مع التقنيات المستقبلة؟

لا تقف التقنية مكتوفة الأيدي، خاصة لحل مثل XDR، الذي لا يزال تقنية حديثة نسبيًا، ويجب عليك معرفة كيف تبدو خريطة طريق البائع للتطوير المستمر.

لماذا Kaspersky

خاضعة لأكبر عدد من الاختبارات. حائزة على أكبر عدد من الجوائز. حماية Kaspersky.

Kaspersky شركة عالمية راسخة في مجال الأمن الإلكتروني وتتمتع بسجل حافل من الخبرة الأمنية. وقد وفرنا الحماية للمؤسسات في جميع أنحاء العالم لأكثر من 25 عامًا وحصلنا على عدد لا يحصى من الجوائز والأوسمة لمنتجاتنا وخدماتنا. بين عامي 2013 و2022، حصلت منتجات Kaspersky على ما يلي:

587

حققت المركز الأول 587 مرة

685

حققت أحد المراكز الثلاثة الأولى 685 مرة

827

شاركت في 827 اختبارًا ومراجعة مستقلة

في عام 2023، حصلت Kaspersky على لقب الشركة الرائدة في سوق حلول XDR من قبل شركة ISG العالمية الرائدة في مجال الأبحاث والاستشارات التقنية. وتُعرّف ISG "الرواد" بأنهم من يمتلكون عرضًا شاملاً للمنتجات والخدمات ويمثلون قوة مبتكرة واستقرارًا تنافسيًا. معرفة المزيد:

معرفة المزيد

Kaspersky Extended Detection and Response

معرفة المزيد

#kaspersky
#bringonthefuture

me.kaspersky.com