يعرض البحث الآمن عن نشاط الوصول أسماء قواعد غير معروفة

المحتويات

مسألة

أثناء إجراء "مظلة" لترحيل SSE، تعرض أحداث "بحث عن نشاط الوصول الآمن" اسم القاعدة "غير معروف" على أنه بدل من عرض قواعد السياسة المسماة. لوحظ هذا السلوك بالنسبة إلى أنواع حركة المرور المختلفة، بما في ذلك حركة المرور المموج بها مثل الطلبات إلى chatgpt.com. كان القلق هو ما إذا كانت إدخالات اسم القاعدة غير المعروفة هذه تشير إلى مشكلة في تكوين النهج أو مشكلة ترحيل تتطلب الإصلاح.

البيئة

- الوصول الآمن (SSE) من Cisco
- المؤسسة التي تخضع لعملية ترحيل SSE
- الإبلاغ عن البحث عن نشاط الوصول الآمن
- تم تصنيف حركة المرور كمجالات مرئية حديثا

قرار

السلوك غير المعروف لاسم القاعدة متوقع وعادي للأحداث التي تتم معالجتها بواسطة منطق نظام الوصول الآمن بدلا من القواعد التي تم إنشاؤها/تسميتها من قبل العميل. يحدث هذا بشكل عام لحركة المرور المصنفة كمجالات تم عرضها حديثا، حيث تم عرض المجال وأن نشاط البحث في تقارير النشاط على هذا النحو تم الإبلاغ عنه وتم الاستعلام عنه في وقت حديثا في الأمان.

ترجمة أحداث البحث عن النشاط باستخدام أسماء قواعد غير معروفة

عند مواجهة أحداث باسم القاعدة غير معروف، راجع حقول الحدث التالية لتحديد سبب الإنفاذ وتأكيد تطبيق السياسة المناسب:

- الإجراء - يعرض ما إذا كان قد تم السماح بحركة المرور أو منعها
- سبب منع الحدث / سبب الحظر - يقدم تفاصيل تنفيذ محددة
- الفئات - يعرض تصنيف المحتوى (مثل المجالات التي تم عرضها حديثا)
- مجال الوجهة/IP - هدف الطلب
- هوية المستخدم/المصدر - مصدر حركة المرور
- الطابع الزمني - عند حدوث الحدث

إذا عرض حقل الفئات المجالات التي تم عرضها حديثا، فإن UNKNOWN في حقل اسم القاعدة هو السلوك المتوقع ولا يشير إلى ترحيل فاشل أو تلف نهج.

خطوات التحقق من الصحة للسلوك غير المتوقع

إذا كان من المتوقع أن تتطابق حركة المرور مع قاعدة مسماة معينة ولكن تظهر UNKNOWN، قم بجمع هذه المعلومات للتحقق من مسار السياسة:

- 2-3 عينة من الطوابع الزمنية للحدث
- مجال الوجهة/IP لكل حدث
- هوية المستخدم/المصدر لكل حدث

يمكن إستخدام هذه المعلومات لمقارنة مسار السياسة المتوقع بسلوك الحدث الفعلي وتحديد ما إذا كان يتعين إجراء مزيد من التحقيق.

السبب

يظهر اسم قاعدة غير معروف عندما يقوم منطق نظام الوصول الآمن بمعالجة حركة مرور

البيانات بدلا من تطبيق قاعدة سياسة تم إنشاؤها/تسميتها من قبل العميل. هذا سلوك موثق لفئات معينة من فئات حركة المرور، وخاصة المجالات المرئية حديثا، حيث تكون آليات التصنيف والمعالجة المدمجة الأسبقية على القواعد المسماة أثناء التقييم الأولي للمجال.

المحتوى ذي الصلة

- تمكين أمان المجالات التي تم عرضها حديثا
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).