سجلات أحداث ملف الوصول الآمن مفقودة من SIEM بعد تغيير الترخيص

المحتويات

مسألة

توقف إستلام سجلات أحداث الملفات بواسطة SIEM من تخزين AWS S3 بينما إستمرت سجلات DNS في التسليم بنجاح. عرضت موصلات بيانات حدث الملف رمز "غير متصل" في واجهة SIEM. تم تعريف السجلات التي توقفت عن الظهور كسجلات أحداث ملفات مرتبطة بـ DLP/IPS. ظلت سجلات طبقة DNS تعمل طوال فترة المشكلة.

كانت البيئة تستخدم كل من Umbrella و Secure Access أثناء الترحيل، مع إرسال السجلات إلى نفس مستودع AWS. وقد جرى تدوير المفاتيح وتأكد أنها تعمل بشكل صحيح. تمت ملاحظة أن إصدار المخطط موجود في الإصدار 10 أثناء توفر الإصدار 16.

البيئة

- مؤسسة الوصول الآمن من Cisco مع تكوينات الوصول الآمن والمظلة
- تكامل تخزين AWS S3 لتصدير السجل
- Microsoft Sentinel SIEM لنظام الأساسي
- (الإصدار 16 متوفر) قيد الاستخدام المخطط من الإصدار 10
- 2026 يونيو 23 في Essentials إلى Advantage من Secure Access ترخيص تغيير تم
- 2026 يونيو 24 في الملف حدث سجلات ملاحظة فيها تم مرة آخر

قرار

كشف التحقيق عن أن سجلات أحداث الملف كانت مرتبطة بوظيفة DLP/IPS، والتي تتطلب ميزات ترخيص محددة. وقد تم تحديد السبب الجذري من خلال التحليل التالي.

الخطوة 1: تحليل حركة المرور

تحقق من البحث عن النشاط في الوصول الآمن لتأكيد أنماط حركة المرور:

1.- انتقل إلى البحث عن النشاط ومرشح حركة مرور الويب وأحداث المصير النهائي الضارة. لمدة 30 يوم الماضي، لكن لم تظهر أي أحداث حركة مرور DNS وأظهر التحليل وجود حركة مرور ويب. تم تمكين فحص الملف بها، ولم يتم تحديد أي قواعد تم تكوينها مؤخرًا.
2.- تدفق حركة المرور > السجلات الموجودة على تقرير CSA > S3 bucket - SIEM.

الخطوة 2: مراجعة سجل الترخيص

1.- مراجعة سجل الترخيص في Secure Access لتحديد أي تغييرات تتوافق مع توقيت إيقاف سجل حدث الملف.

2.- انتقل إلى Secure Access (الوصول الآمن) > Admin > Subscription لعرض مستوى الترخيص الحالي وملخص الميزات.

أظهر التحقيق أن ترخيص Secure Access تغير من ميزة Secure Access إلى أساسيات Secure Access في 23 يونيو 2026، وهو ما يتوافق مع التوقيت الذي توقفت فيه سجلات أحداث الملفات عن الظهور.

الخطوة 3: التحقق من الميزة

تحقق من الميزات المضمنة في مستوى الترخيص الحالي. الـ DLP و IPS، التي تقوم بإنشاء سجلات أحداث الملفات، في طبقة ترخيص Secure Access Essentials.

الخطوة 4: سبب التأكيد والجذر

ونظرا لأن "حدث الملف" سجلات ظهور توقف عند تمامًا التخيص تغيير توقيت ويتطابق تم، حل الحالة على أساس أن سجلات DNS طبقة تسجيل يعمل وكان المتطلب الأساسي Essentials الحالي ترخيص بموجب متوفرة تكون لن الملفات أحداث.

السبب

تم إيقاف إنشاء سجلات أحداث الملف بسبب تغيير الترخيص من ميزة Secure Access إلى DLP و Secure Access في 23 يونيو 2026. تقترن سجلات أحداث الملفات بوظائف أساسيات IPS، والتي لا يتم تضمينها في طبقة ترخيص Essentials. قام خفض درجة الترخيص بإزالة الوصول إلى إمكانيات فحص الملفات التي تقوم بإنشاء أنواع السجلات المحددة هذه.

المحتوى ذي الصلة

- [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).