أستكشاف أخطاء تحليل الملفات الإيجابية وإصلاحها في AMP لنقاط النهاية

المحتويات

المقدمة

يوضح هذا المستند كيفية تجميع تحليل ملف موجب زائف في "الحماية المتقدمة من البرامج الضارة" (AMP) لنقاط النهاية.

ساهم فيه يسوع خافيير مارتينيز، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- لوحة معلومات وحدة التحكم في AMP
- حساب بامتيازات المسؤول

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco AMP لإصدار نقاط النهاية 6.X.X والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يمكن أن يقوم AMP لنقاط النهاية بإنشاء تنبيهات مفرطة على خوارزمية تجزئة (SHA) 256 خاصة بالملف/العملية/الأمان. إذا كنت تشك في حدوث أي عمليات كشف إيجابية خاطئة في شبكتك، فيمكنك الاتصال بمركز المساعدة التقنية (TAC) من Cisco، فيواصل فريق التشخيص إجراء تحليل ملف أعمق. عندما يتصل أنت cisco TAC، أنت تحتاج أن يزود هذه معلومة:

·تجزئة الملف SHA 256
·نسخ نموذج الملف
·التقاط حدث التنبيه من وحدة تحكم AMP
·التقاط تفاصيل الحدث من وحدة تحكم AMP
·معلومات حول الملف (من أين تم الحصول عليه ولماذا يجب أن يكون في البيئة)
·شرح لماذا تعتقد أن الملف/العملية قد تكون إيجابية خاطئة

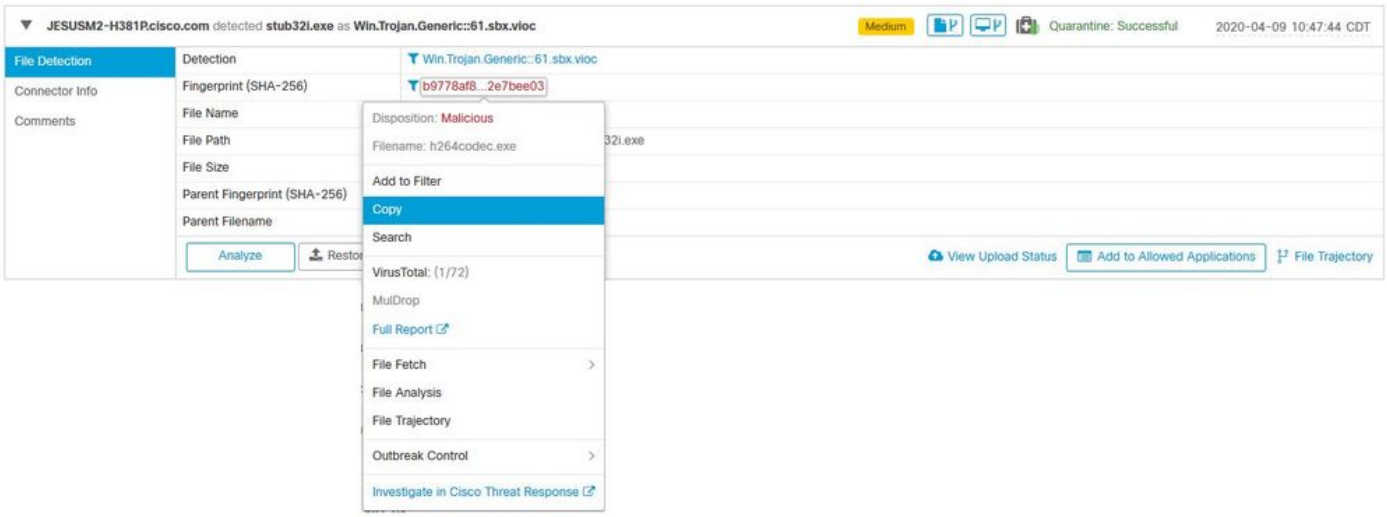
أستكشاف أخطاء تحليل الملف الإيجابي الخطأ وإصلاحها في AMP لنقاط النهاية

يزود هذه قسم معلومة أنت يستطيع استعملت أن يحصل كل التفاصيل يحتاج أن يفتح خطأ صحة ووية مع cisco TAC.

تجزئة الملف SHA 256

الخطوة 1. للحصول على تجزئة SHA 256، انتقل إلى **وحدة تحكم AMP > لوحة المعلومات > الأحداث.**

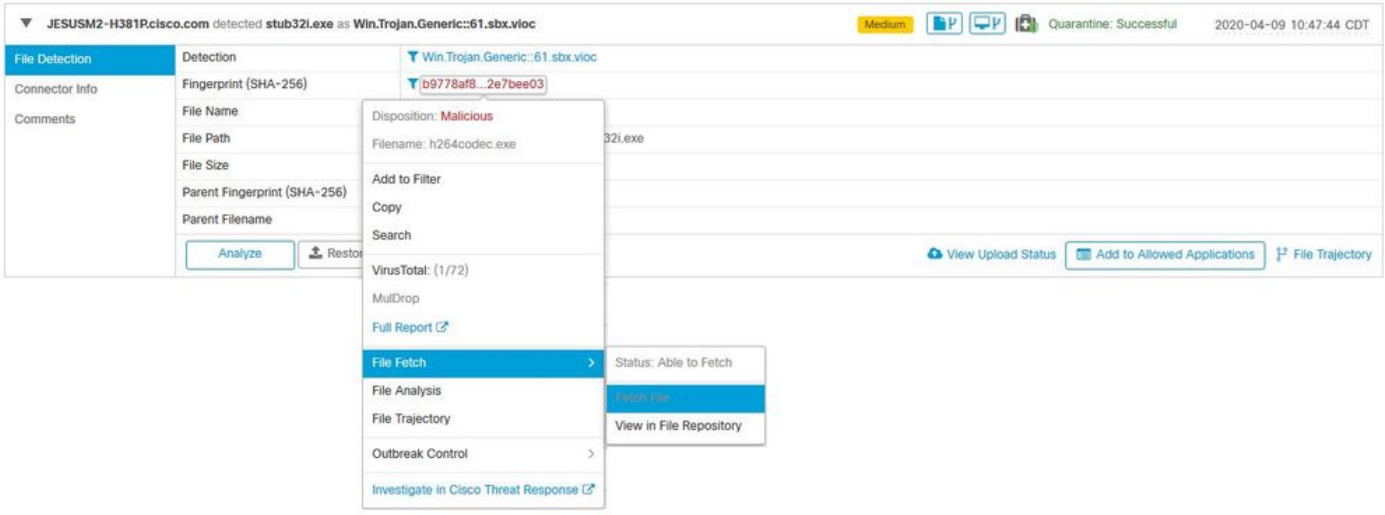
الخطوة 2. حدد **حدث التنبيه**، انقر على **SHA256** وحدد **نسخ** كما هو موضح في الصورة.



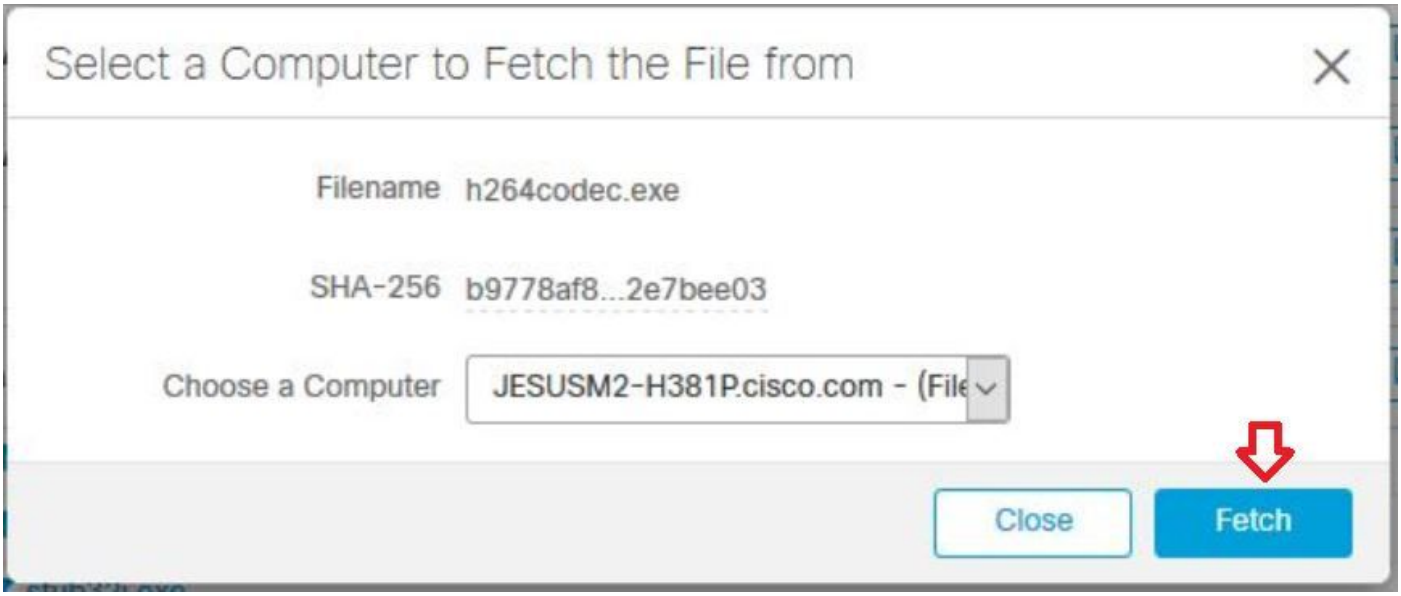
نسخ نموذج الملف

الخطوة 1. يمكنك الحصول على نموذج الملف من وحدة تحكم AMP، انتقل إلى **وحدة تحكم AMP > لوحة المعلومات > الأحداث.**

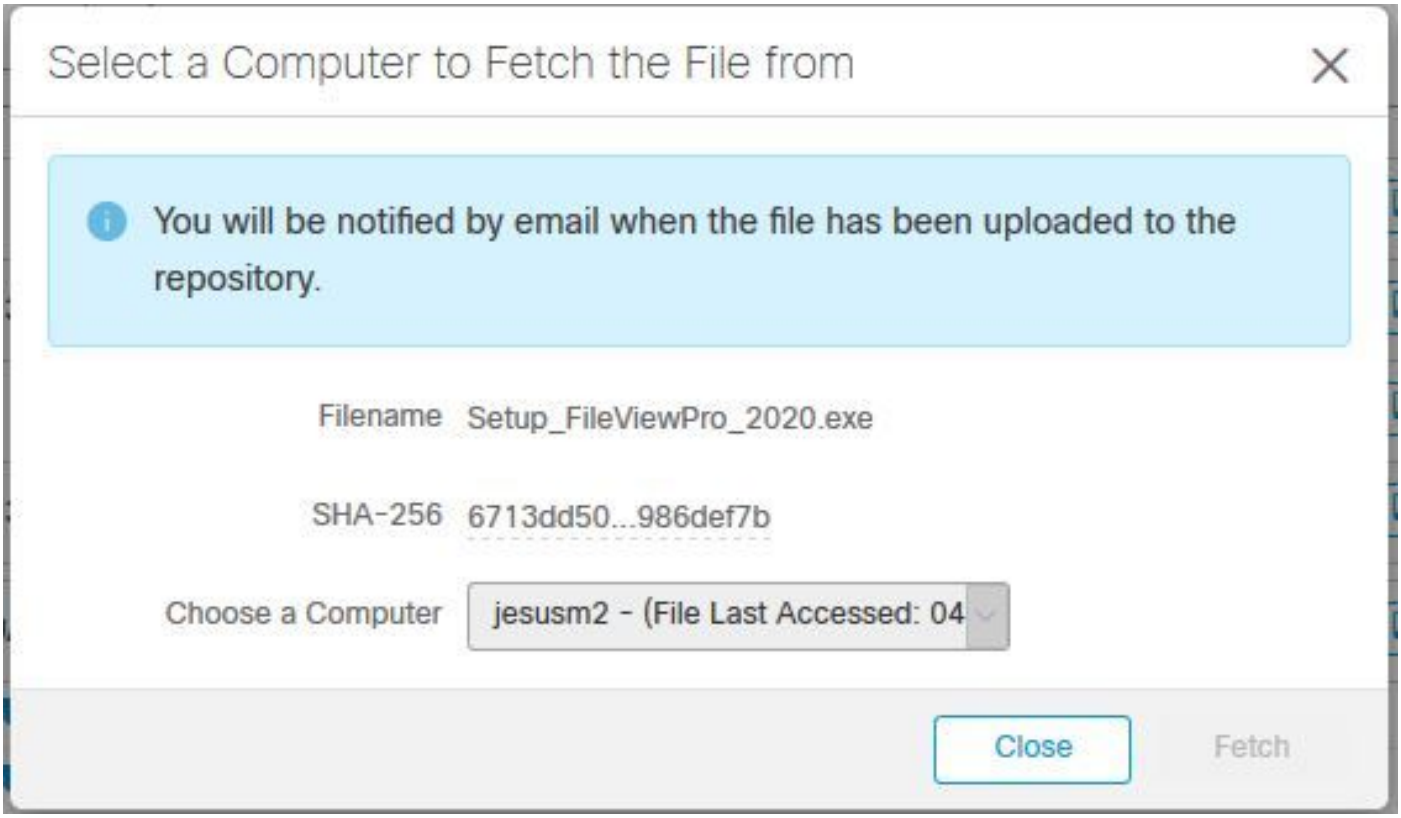
الخطوة 2. حدد **حدث التنبيه**، انقر على **SHA256** وانتقل إلى **إحضار الملف>إحضار الملف** كما هو موضح في الصورة.



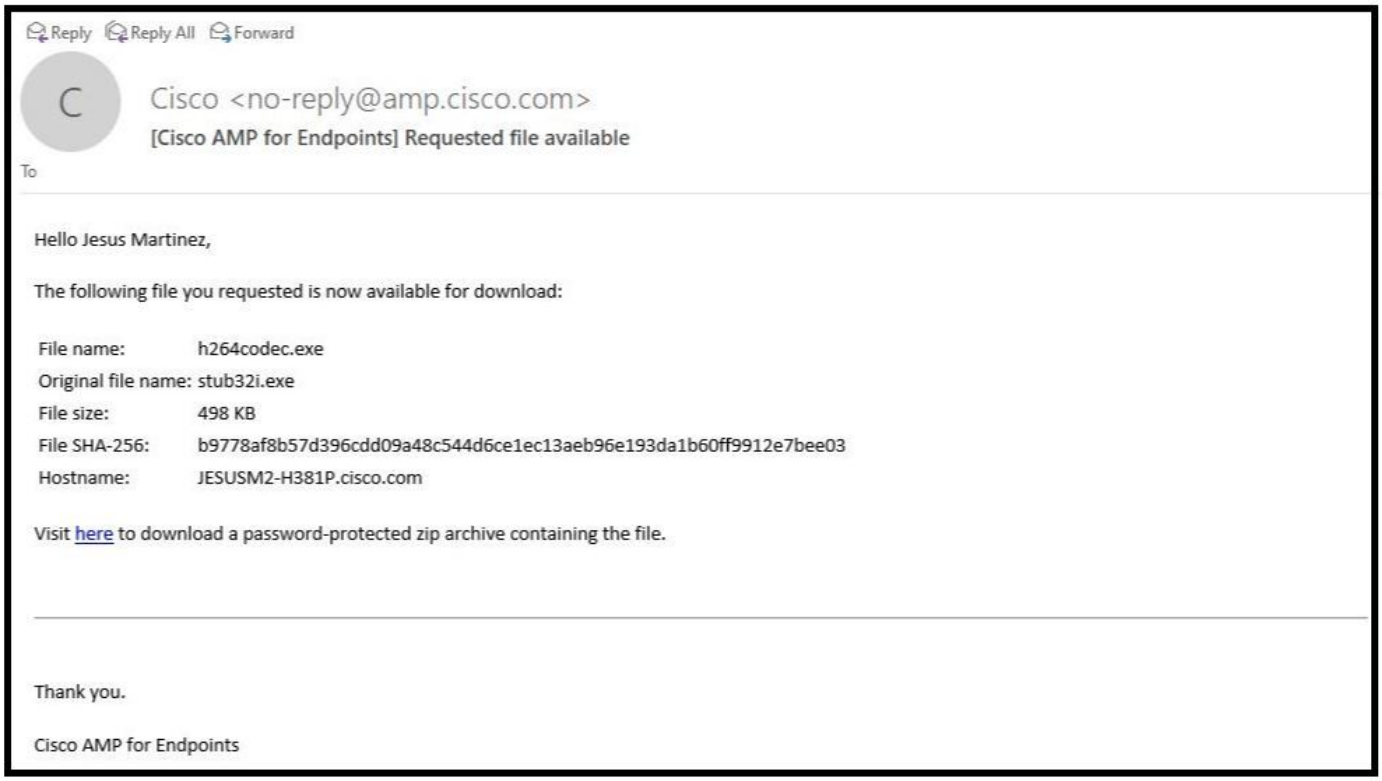
الخطوة 3. حدد الجهاز حيث تم الكشف عن الملف وانقر على **إحضار** كما هو موضح في الصورة (يجب تشغيل الجهاز) كما هو موضح في الصورة.



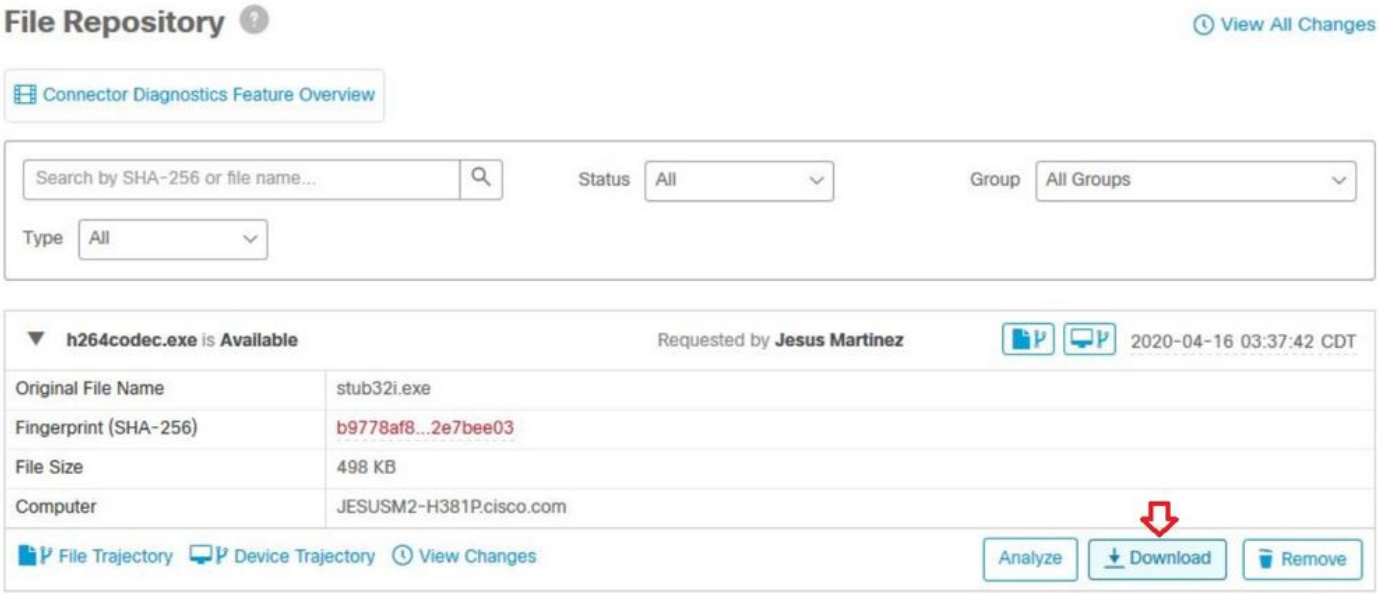
الخطوة 4. تتلقى الرسائل كما هو موضح في الصورة.



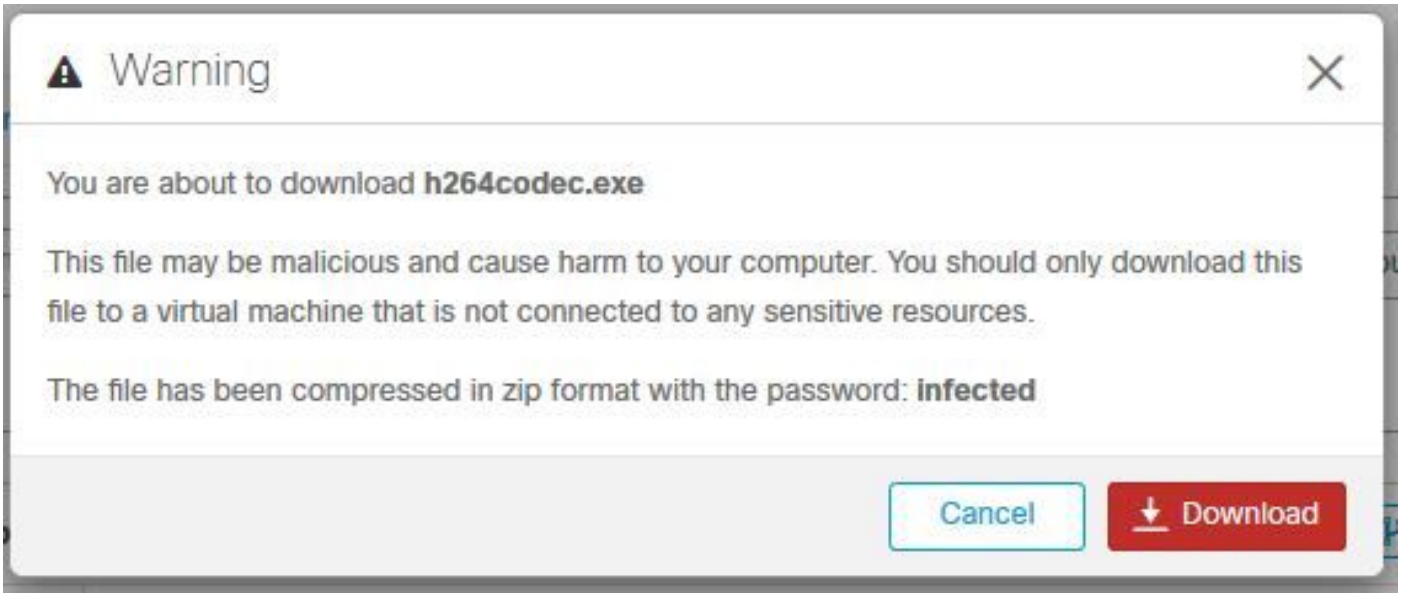
بعد بضع دقائق، تتلقى إخطارا بالبريد الإلكتروني عندما يكون الملف متاحا للتنزيل كما هو موضح في الصورة.



الخطوة 5. انتقل إلى **وحدة تحكم AMP > تحليل > مستودع الملفات** وحدد الملف وانقر فوق **تنزيل** كما هو موضح في الصورة.



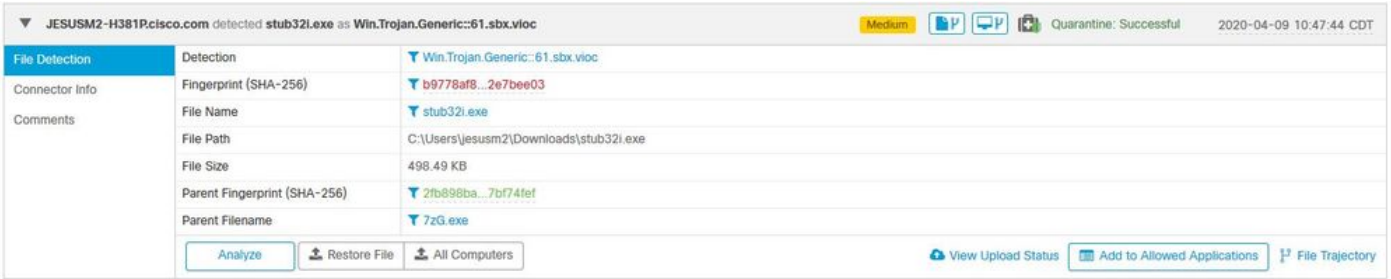
الخطوة 6. يظهر مربع الإعلام، انقر فوق **تنزيل**، كما هو موضح في الصورة، ويتم تنزيل الملف على ملف ZIP.



التقاط حدث التنبيه من وحدة تحكم AMP

الخطوة 1. انتقل إلى **وحدة تحكم AMP > لوحة المعلومات > الأحداث.**

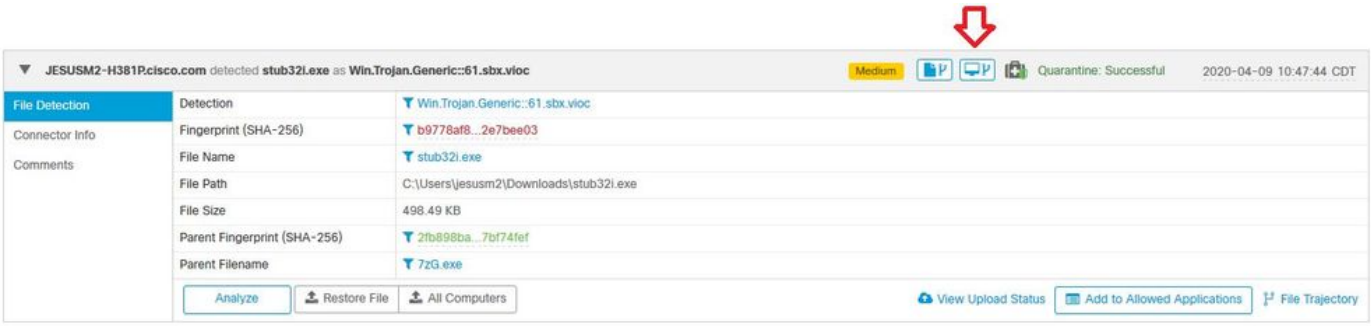
الخطوة 2. حدد **حدث التنبيه** والتقاط الالتقاط كما هو موضح في الصورة.



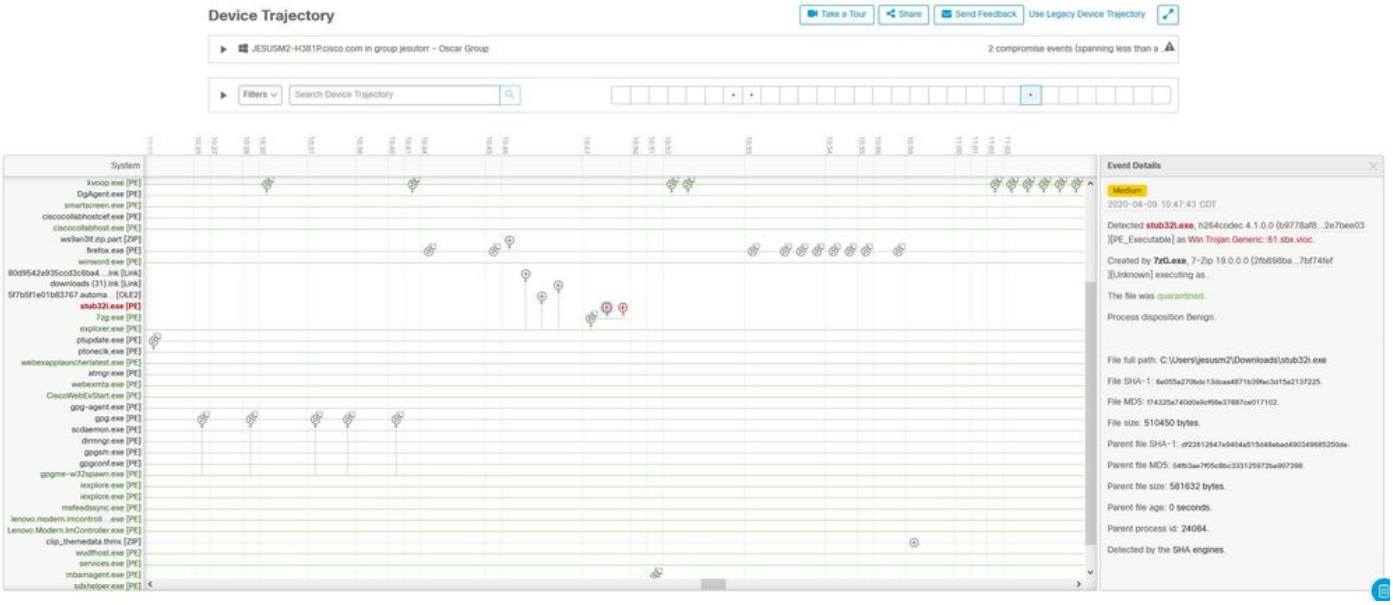
التقاط تفاصيل الحدث من وحدة تحكم AMP

الخطوة 1. انتقل إلى **وحدة تحكم AMP > لوحة المعلومات > الأحداث.**

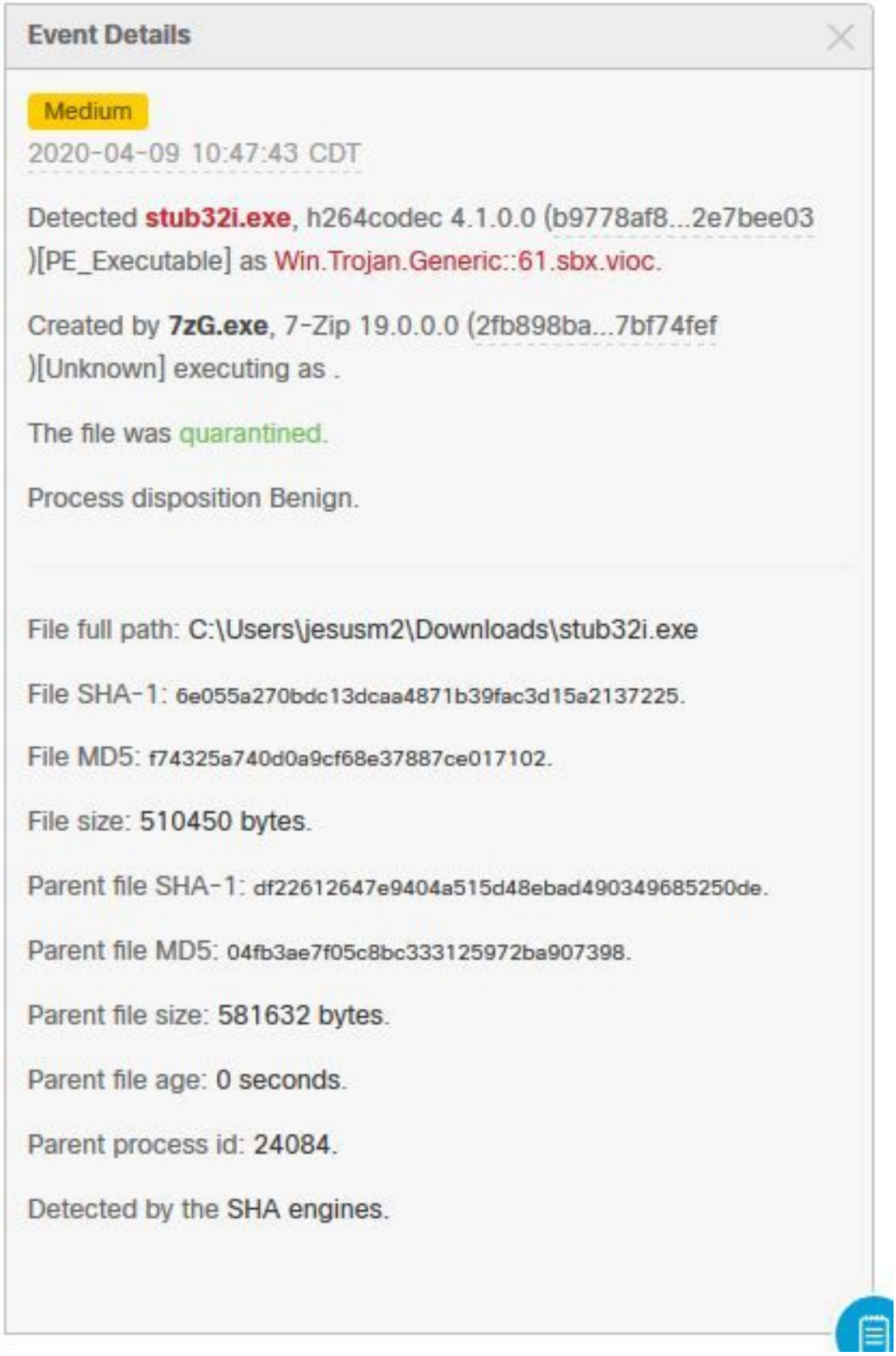
الخطوة 2. حدد حدث التنبيه وانقر على خيار **مسار الجاز** كما هو موضح في الصورة.



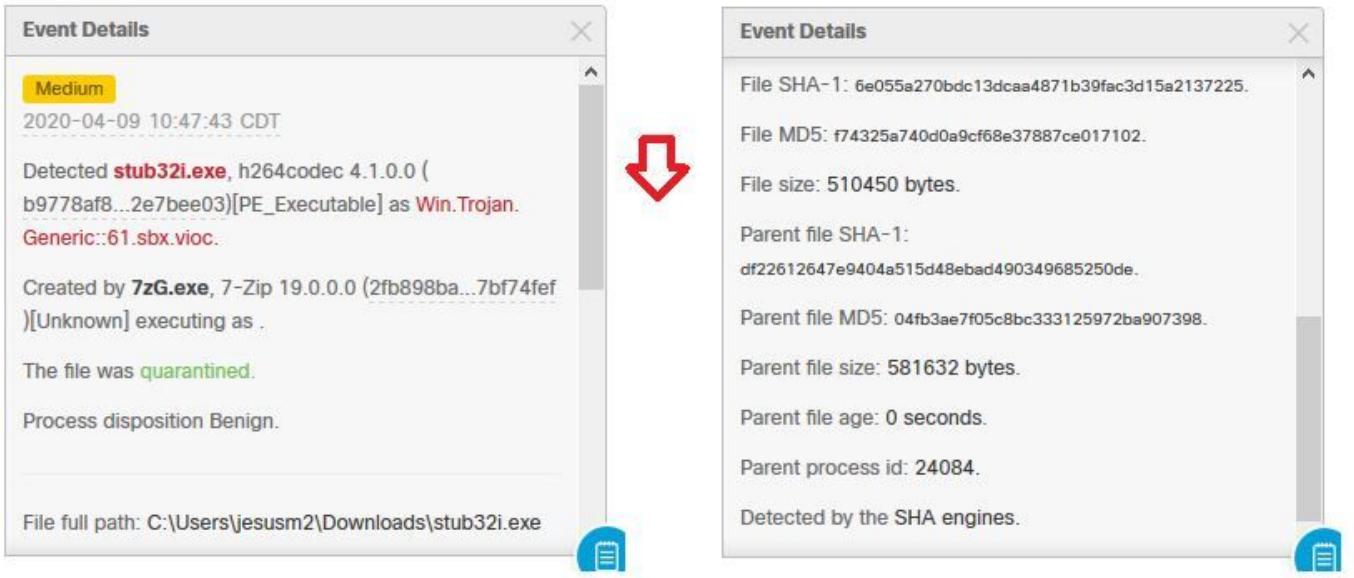
إنه يعيد التوجيه إلى **تفاصيل مسار الجاز** كما هو موضح في الصورة.



الخطوة 3. التقاط مربع **تفاصيل الحدث** كما هو موضح في الصورة.



الخطوة 4. إذا كان من الضروري، انزلق لأسفل والتقاط بعض الالتقاط للحصول على معلومات **تفاصيل** جميع **الأحداث** كما هو موضح في الصورة.



معلومات حول الملف

- معلومات حول مصدر الملف.
- إذا جاء الملف من موقع ويب، فقم بمشاركة عنوان URL للويب.
- شارك وصفا صغيرا للملف وقم بشرح وظيفة الملف.

الشرح

- لماذا تعتقد أن عملية الملف يمكن أن تكون إيجابية خاطئة؟
- شارك الأسباب التي تثق بها في الملف.

توفير المعلومات

- بمجرد تجميع جميع التفاصيل، قم بتحميل جميع المعلومات المطلوبة إلى موقع https://cway.cisco.com/csc/.
- تأكد من الإشارة إلى رقم طلب الخدمة.

القرار

تسعى Cisco دائما إلى تحسين ذكاء التهديد الخاص بتقنية AMP لنقاط النهاية وتوسيعه، ومع ذلك، إذا قام حل AMP for Endpoints لديك بتشغيل تنبيه بشكل غير صحيح، فيمكنك إتخاذ بعض الإجراءات لمنع أي تأثير إضافي على بيئتك. يقدم هذا وثيقة guidelines أن يحصل كل التفاصيل المطلوبة أن يفتح حالة مع cisco TAC فيما يتعلق مسألة إيجابية خاطئة. استنادا إلى تحليل ملف "فريق التشخيص"، يمكن تغيير مصير الملف لإيقاف أحداث التنبيه التي تم تشغيلها على وحدة تحكم AMP أو يمكن أن يوفر Cisco TAC الإصلاح المناسب للسماح بتشغيل الملف/العملية دون حدوث مشاكل في بيئتك.

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).