تكوين الاستثناءات وإدارتها في Cisco Secure Endpoint Connector

المحتويات

المقدمة

يصف هذا المستند كيفية إنشاء الاستبعاد للمحركات المختلفة على وحدة تحكم نقطة النهاية الآمنة من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تعديل قائمة إستبعاد وتطبيقها على سياسة في وحدة تحكم نقطة النهاية الآمنة
- إتفاقية Windows CSIDL

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة تحكم نقطة النهاية الآمنة 5.4.20211013 من Cisco
- مرجع دليل مستخدم نقطة النهاية الآمنة 15 أكتوبر 2021

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 قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

سير عمل نقطة النهاية الآمنة

في مستوى عال من العمليات، تعمل نقطة النهاية الآمنة من Cisco على معالجة خوارزمية التجزئة الآمنة للملفات (SHA) بهذا الترتيب من خلال المكونات الرئيسية للموصل:

- الاستباعادات
- محرك تترا
- التحكم في التطبيق (قائمة السماح / قائمة الحظر)
- محرك SHA
- منع الاستغلال (ExPrev) / حماية النشاط الضار (MAP) / حماية عملية النظام / محرك الشبكة (رطب تدفق الجهاز)

ملاحظة: يعتمد إنشاء الاستباعاد أو السماح/حظر القائمة على المحرك الذي اكتشف الملف.

حافظت Cisco على الاستباعادات

يتم إنشاء الاستثناءات التي يتم صيانتها من Cisco وصيانتها بواسطة Cisco لتوفير توافق أفضل بين موصل نقطة النهاية الآمنة ومكافحة الفيروسات ومنتجات الأمان أو البرامج الأخرى.

تحتوي مجموعات الاستباعاد هذه على أنواع مختلفة من الاستباعادات لضمان التشغيل السليم.

يمكنك تعقب التغييرات التي تم إجراؤها على هذه الاستثناءات في الملاحق تغييرات قائمة الاستباعاد التي يتم صيانتها من Cisco لـ Cisco Secure Endpoint Console.

استباعادات مخصصة

محرك نقطة النهاية الآمنة

فحص الملفات (استخدام وحدة المعالجة المركزية (CPU) / اكتشاف الملفات) بواسطة محرك Tetra و SHA:

أستخدم هذه الأنواع من الاستباعادات لتجنب اكتشاف/عزل ملف أو تخفيف تأمين وحدة المعالجة المركزية (CPU) لنقطة النهاية.

يتم عرض الحدث الموجود على وحدة تحكم نقطة النهاية الآمنة كما هو موضح في الصورة.

ملاحظة: يمكن إستخدام CSIDL للاستبعادات، يرجى الرجوع إلى مستند Microsoft هذا للحصول على مزيد من المعلومات حول CSIDL.

إستثناء المسار

إستثناء Wildcard

ملاحظة: يتم إستخدام الخيار "تطبيق على جميع أحرف محرك الأقراص" لتطبيق الاستثناء أيضا على محركات الأقراص [من A إلى Z] المتصلة بالنظام.

إستثناء ملحق الملف

تحذير: أستخدم هذا النوع من الاستبعاد مع توخي الحذر لأنه يستبعد جميع الملفات ذات ملحق الملف من عمليات الفحص بغض النظر عن موقع المسار.

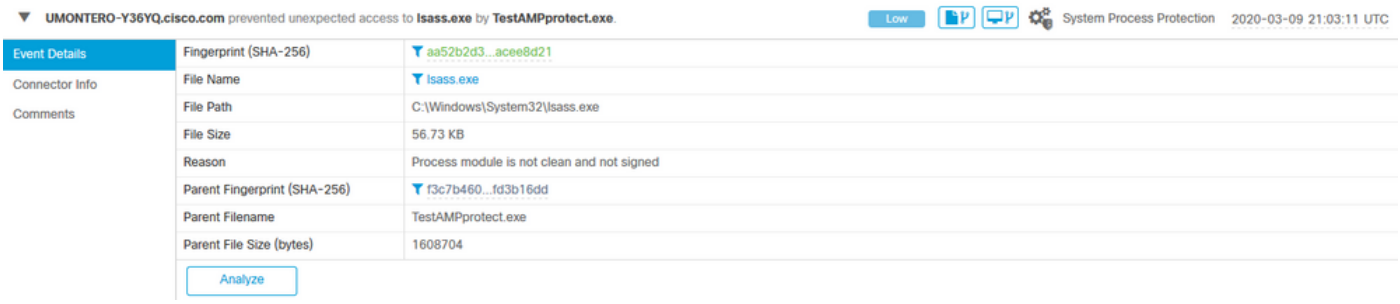
العملية: إستثناء مسح الملفات

حماية عملية النظام (SPP)

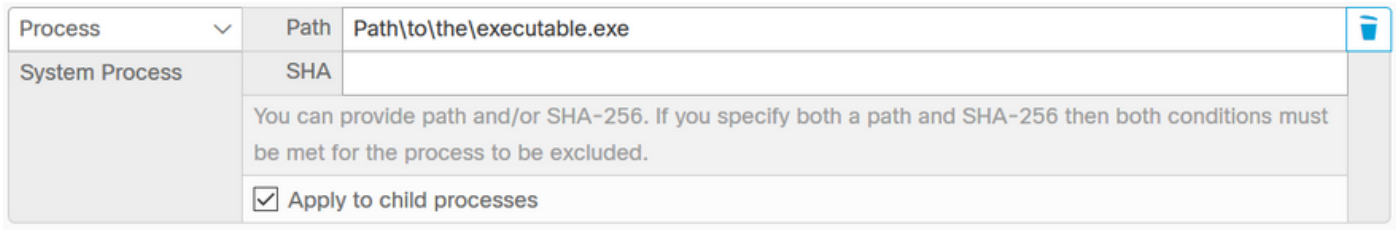
يتوفر محرك حماية عمليات النظام من الموصل الإصدار 6.0.5 ويقوم بحماية عمليات Windows التالية:

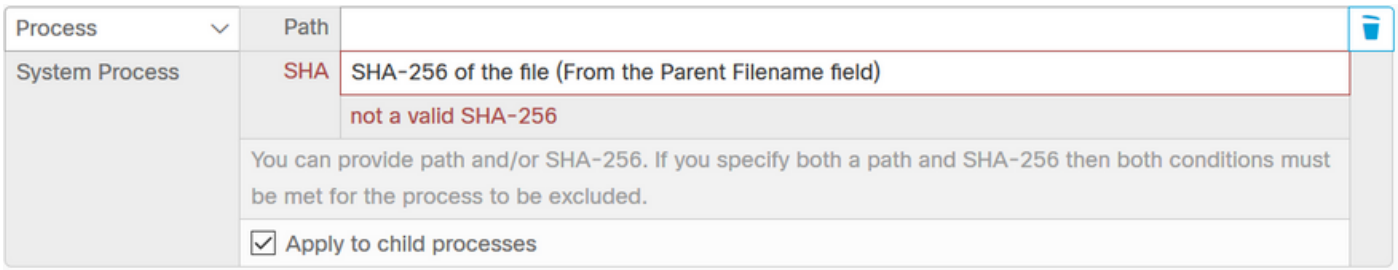
- النظام الفرعي لمدير جلسة العمل (smss.exe)
- النظام الفرعي لوقت تشغيل العميل/الخادم (csrss.exe)
- النظام الفرعي لسلطة الأمن المحلية (lsas.exe)
- تطبيق تسجيل الدخول إلى Windows (winlogon.exe)
- تطبيق بدء تشغيل Windows (wininit.exe)

تعرض هذه الصورة حدث SPP.



إستثناء SPP

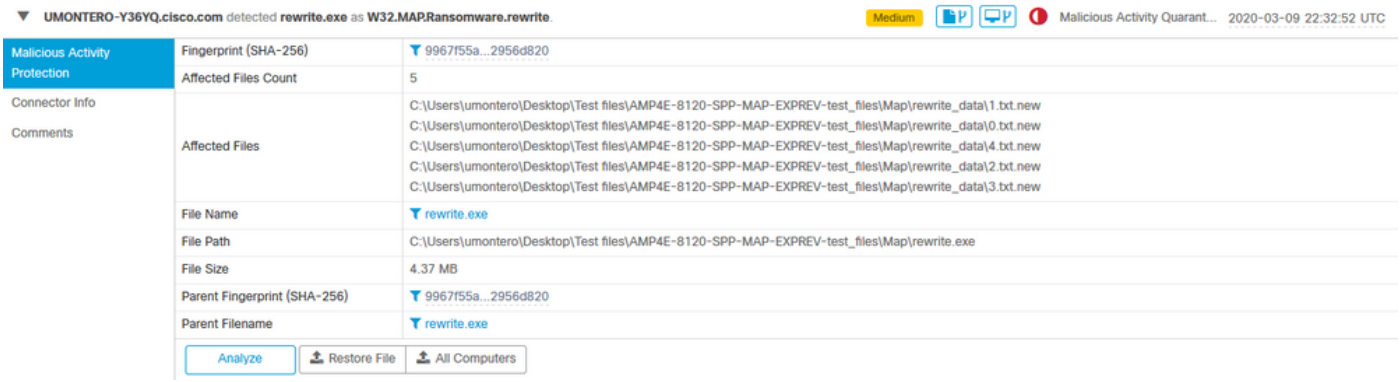




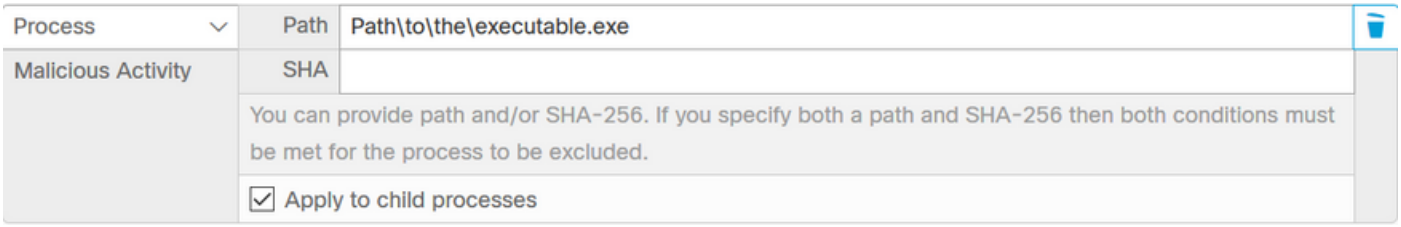
حماية الأنشطة الضارة (MAP)

محرك حماية الأنشطة الضارة (MAP)، يدافع عن نقطة النهاية الخاصة بك من هجوم برنامج الفدية. وهو يحدد الإجراءات أو العمليات الضارة عند تنفيذها، ويحمي بياناتك من التشفير.

يتم عرض حدث MAP في هذه الصورة.



إستثناء الخريطة

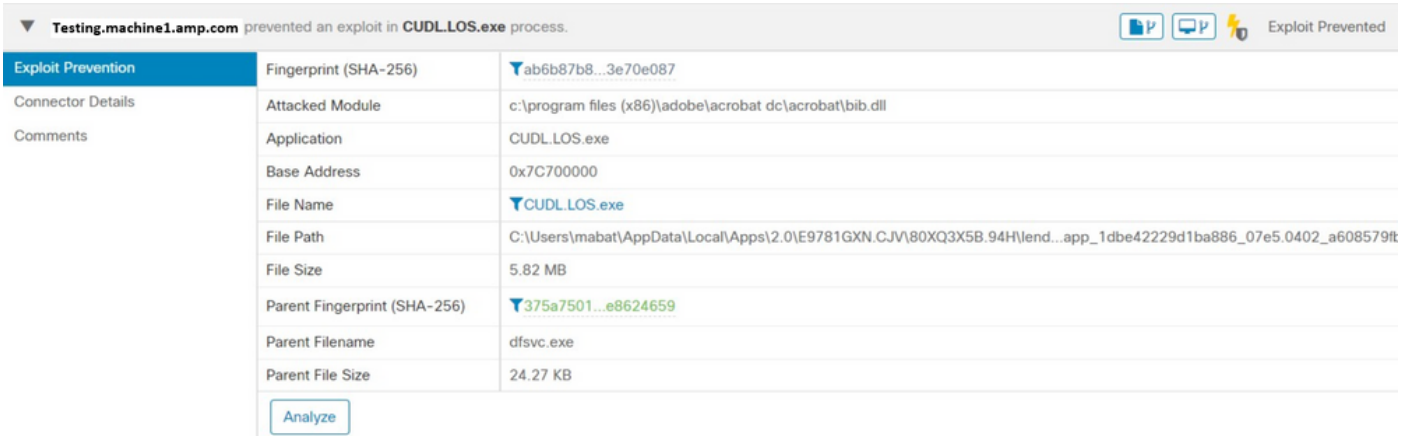


⚠ تحذير: أستخدم هذا النوع من الاستباعاد مع توخي الحذر وبعد التأكد من أن الكشف ليس ضارا بالفعل.

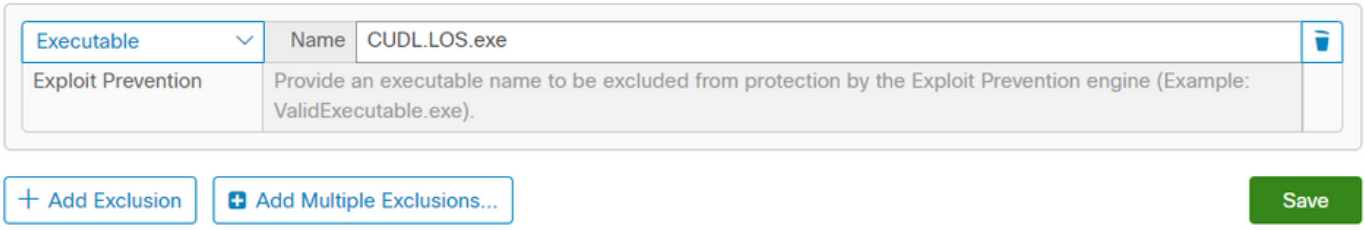
منع الاستغلال (EXPREV)

يقوم محرك منع الاستغلال بالدفاع عن نقاط النهاية الخاصة بك من هجمات حقن الذاكرة التي يتم إستخدامها بشكل شائع من قبل البرامج الضارة والهجمات الأخرى التي يتم تنفيذها في يوم صفر على البرامج التي لم يتم تصحيحها
مكامن الضعف. عندما يكتشف هجوم ضد عملية محمية، سيتم منعه ويولد حدثا، لكن لن يكون هناك حجز صحي.

يتم عرض حدث Exprev في هذه الصورة.



إستباعاد Exprev

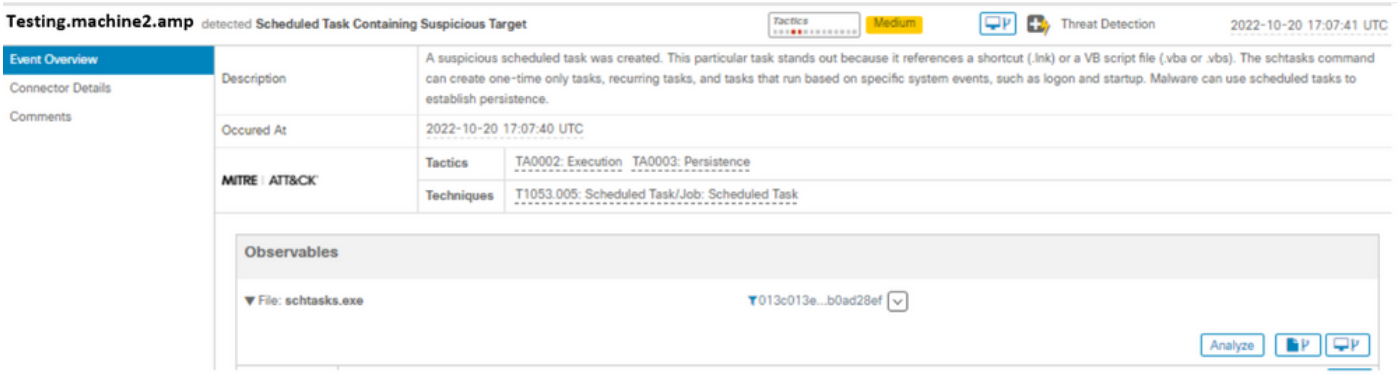


⚠ تحذير: أستخدم هذا الاستبعاد كلما كنت تثق في النشاط على الوحدة النمطية/التطبيق المتأثر.

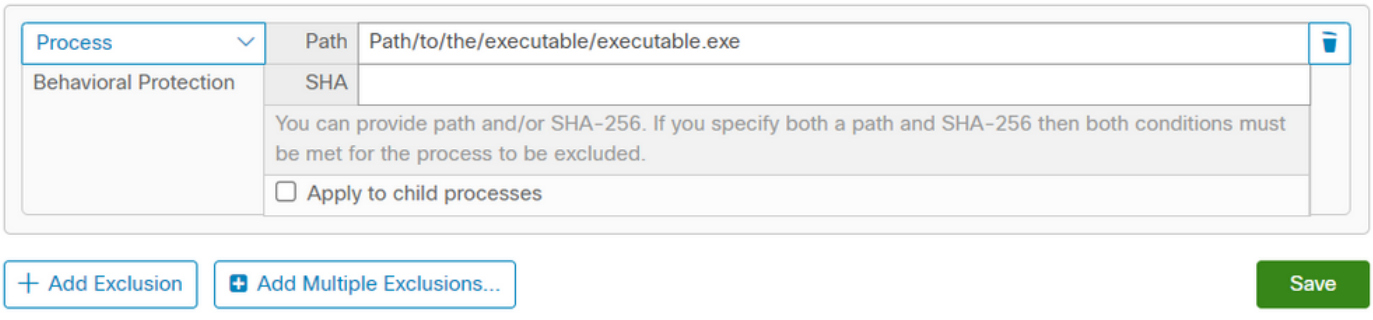
الحماية السلوكية (BP)

يعزز محرك الحماية السلوكية القدرة على اكتشاف التهديدات وإيقافها سلوكيا. وتعمق القدرة على اكتشاف الهجمات "التي تتم خارج الأراضي" وتوفر
إستجابة أسرع للتغيرات في بيئة التهديد من خلال تحديث التوقيع.

يتم عرض حدث BP في هذه الصورة.



إستثناء BP



معلومات ذات صلة

- لمزيد من المعلومات حول تكوين النهج، انتقل إلى دليل المستخدم
- إنشاء إستثناءات في فيديو Cisco Secure Endpoint Connector
- الدعم التقني والمستندات - Cisco Systems

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).