تصدير قائمة بمعرفات أحداث Windows لنقطة النهاية الآمنة

المحتويات

المقدمة

يصف هذه المستند جميع معرفات الأحداث لنقطة النهاية الآمنة من Cisco، مما يساعد في المراقبة الفعالة والاستجابة للحوادث.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تسجيل أحداث Windows
- نقطة نهاية آمنة من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج التالية:

- Cisco Secure Endpoint 8.4.0.30201
- نظام التشغيل Windows Server 2019

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

المشكلة

تعد معرفات أحداث Windows لنقطة النهاية الآمنة من Cisco ضرورية للمراقبة الفعالة واستكشاف الأخطاء وإصلاحها. إن القدرة على الوصول إلى معرفات الحدث تلك هو أمر حيوي لتشخيص القضايا، وضمان الكفاءة العملياتية، وتعزيز الأمن بشكل عام.

الحل

افتح File Explorer، انتقل إلى C:\Program Files\Cisco\AMP\<version_number>\AMPEvents.man. يمكنك فتح هذا الملف في Notepad لعرض جميع المعلومات المتعلقة بأحداث Windows التي تم إنشاؤها بواسطة Cisco Secure Endpoint.

تم تصدير قائمة بمعرفات الأحداث من ملف AMPEvents.man:

معرف الحدث	حدث	المحرك/المهمة	م
100	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V1/V2/V3/V4	منع الاستغلال	ع
101	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V1/V2/V3/V4	منع الاستغلال	ع
102	EXPREV_ATTACK_WITHOUT_SUSPICIOUS_FILES_V3/V4_AUDIT	منع الاستغلال	ع
103	EXPREV_ATTACK_WITH_SUSPICIOUS_FILES_V3/V4_AUDIT	منع الاستغلال	ع
104	EXPREV_SCRIPT_CONTROL_ATTACK_V4	منع الاستغلال	ع
105	EXPREV_SCRIPT_CONTROL_ATTACK_V4_AUDIT	منع الاستغلال	ع
200	Malicious_activity_protection_v1/V2	MaliciousActivityProtection	ع
300	SD_BLOCK_PROCESS_ACTION_V1	حماية عملية النظام	ع
400	CCMS_JOB_START_V1	CCMS	ع
401	Janus_EVENT_V1		ع
500	ENDPOINT_ISOLATION_START_V1	عزل نقطة النهاية	ع
501	ENDPOINT_ISOLATION_STOP_V1	عزل نقطة النهاية	ع
502	ENDPOINT_ISOLATION_STARTFAILED_V1	عزل نقطة النهاية	ال
503	ENDPOINT_ISOLATION_STOPfailed_V1	عزل نقطة النهاية	ال
504	ENDPOINT_ISOLATION_UPDATED_V1	عزل نقطة النهاية	ع
505	ENDPOINT_ISOLATION_UPDATEFAILED_V1	عزل نقطة النهاية	ال
600	ORBITAL_INSTALL_SUCCESS_V1	مدار	ع
601	ORBITAL_INSTALL_FAILED_V1	مدار	ال
602	ORBITAL_UPDATE_SUCCESS_V1	مدار	ع
603	ORBITAL_UPDATE_FAILED_V1	مدار	ال
700	ENDPOINT_ISOLATION_BRUTE_FORCE_ATTEMPT	عزل نقطة النهاية	ت
800	SCRIPT_PROTECTION_DETECTION_V1	ScriptProtection	ع
801	SCRIPT_PROTECTION_QUARANTINE_V1	ScriptProtection	ع
900	ENGINE_DETECTION_HANDLED	الحماية السلوكية	ع
901	ENGINE_DETECTION_NOT_HANDLED	الحماية السلوكية	ال
902	Engine_DETECTION_AUDIT	الحماية السلوكية	ع
903	ENGINE_DETECTION_NO_ACTION	الحماية السلوكية	ع
904	ENGINE_CLEANUP_REQUIRED	الحماية السلوكية	ع
1248	SCAN_COMPLETED_CLEAN_V1	مسح	ع
1249	SCAN_COMPLETED_DIRTY_V1	مسح	ع
1250	SCAN_FAILED_V1	مسح	ال
1300	DETECTION_V1	اكتشاف	ع

1310	QUARANTINE_SUCCESS_V1	رجح	عم
1311	QUARANTINE_FAILED_V1	رجح	الج
1320	execution_block_v1	ExecutionBlock	عم
1321	execution_block_bad_parent_v1	ExecutionBlock	عم
1700	WMI_RECON_V1	نوك ريميو	عم

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).