أفضل ممارسات طلب تغطية نقاط النهاية الآمنة من Cisco

المحتويات

المقدمة

يصف هذا المستند العملية التي يجب إستخدامها عند طلب تغطية Talos لتهديد معروف تم تعريفه بالفعل ولكن لم يتم اكتشافه حاليا بواسطة نقطة نهاية آمنة.

مصادر مختلفة للمعلومات

يمكن أن تكون هناك مصادر متعددة يتم من خلالها التعرف على هذه التهديدات ونشرها، وإليكم بعض الأنظمة الأساسية الشائعة الاستخدام:

- Cisco CVE المنشور
- التعرف على نقاط الضعف وحالات التعرض الشائعة
- إستشارات Microsoft
- معلومات حول التهديدات الخاصة بجهة ثالثة

ترى Cisco التأكد من أن مصادر البيانات شرعية قبل أن نحصل على Talos لمراجعة المعلومات وتحديد التغطية ذات الصلة.

لمراجعة موقف Cisco وتغطيتها للتهديدات المعنية، لدينا مصادر مختلفة من Cisco/Talos يجب مراجعتها قبل طلب طلب تغطية جديد.

بوابة الثغرات من Cisco

بالنسبة لأي CVE متعلق بمنتجات Cisco، يرجى مراجعة هذا المدخل للحصول على مزيد من المعلومات: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

بوابة تالوس

يجب أن تكون بوابة Talos Intelligence هي النقطة المرجعية الأولى للمراجعة في حالة التحقيق في هذا التهديد أو أنه قيد التحقيق حاليا من قبل Talos: https://talosintelligence.com/

مدونات تالوس

كما توفر مدونات Cisco Talos معلومات حول التهديدات التي يتم تقييمها والتحقيق فيها بواسطة Talos: https://blog.talosintelligence.com/

وسنتمكن من العثور على معظم المعلومات ذات الصلة تحت عنوان "معلومات الضعف" التي

تتضمن أيضا جميع "توجيهات Microsoft" المنشورة.

التحقيق الإضافي باستخدام منتجات Cisco

توفر Cisco منتجات متعددة يمكن أن تساعد في مراجعة متجهات/تجزئة التهديد وتحديد ما إذا كانت نقطة النهاية الآمنة توفر تغطية للتهديدات.

التحقيق في الاستجابة لتهديدات Cisco SecureX (CTR)

يمكننا التحقيق في نواحي التهديد كجزء من تحقيقات فريق العمل المشترك، ويمكن إستعراض المزيد من المعلومات هنا: https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

أستكشاف Cisco XDR

توفر Cisco XDR قدرات محسنة للتحقق من متجهات التهديدات، ويمكن العثور على مزيد من المعلومات حول الوظائف هنا:
https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

مدونات Cisco المفيدة

يرجى مراجعة هذه المدونات أثناء إستعراض بعض الوظائف التي تمت مناقشتها في القسم السابق:

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-securex

الخطوات التالية

إذا لم نعثر على متجهات التهديدات التي يتم تغطيتها باستخدام الخطوات الواردة أعلاه، فيمكننا طلب تغطية Talos للتهديد من خلال تقديم طلب دعم TAC.

https://www.cisco.com/c/en/us/support/index.html

للإسراع بعملية التقييم والتحقيق الخاصة بطلب التغطية، كن نطلب الحصول على هذه المعلومات حول التهديد:

- مصدر معلومات التهديد (CVE/Advisory/تحقيقات/مذكرات/مدونات من طرف ثالث)
- تجزئة SHA256 المقترنة
- نموذج للملف (إذا كان متوفرا.)

وبمجرد توفر المعلومات، يقوم تالوس بمراجعة التقييم والتحقيق في الطلب وفقا لذلك.

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).