دمج CTR وشبكة التهديدات

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لدمج الاستجابة لتهديدات Cisco (CTR) مع سحابة شبكة التهديدات (TG) من أجل إجراء تحقيقات CTR.

ساهم به يسوع خافيير مارتينيز، محرر من قبل يارادين سانشيز، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إستجابة تهديدات الحماية من Cisco
- شبكة تهديدات

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- وحدة تحكم CTR (حساب المستخدم مع حقوق المسؤول)
- وحدة تحكم شبكة التهديدات (حساب المستخدم مع حقوق المسؤول)

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 فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

شبكة تهديدات الحماية من Cisco هي عبارة عن نظام أساسي متطور وتلقائي لتحليل البرامج الضارة وتقنية المعلومات الاستخبارية حول تهديدات البرامج الضارة، حيث يمكن

تفجير الملفات المريبة أو وجهات الويب دون التأثير على بيئة المستخدم.

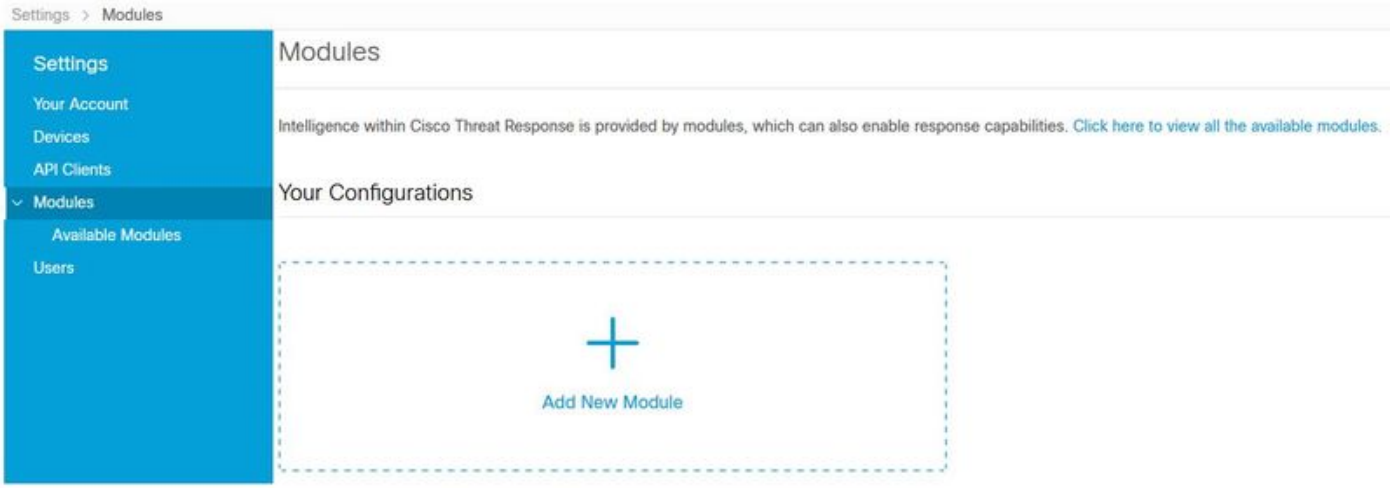
في الدمج مع Cisco Threat Response، تعد "شبكة التهديدات" وحدة مرجعية وتوفر القدرة على الدوران حول بوابة "شبكة التهديدات" لجمع معلومات إستخباراتية إضافية حول تجزئة الملفات و IPs والنطاقات و URLs في مخزن معارف شبكة التهديدات.

التكوين

وحدة التحكم CTR - تكوين الوحدة النمطية لشبكة التهديد

الخطوة 1. سجل الدخول إلى إستجابة تهديدات Cisco باستخدام بيانات اعتماد المسؤول.

الخطوة 2. انتقل إلى علامة التبويب وحدات نمطية، حدد **وحدات نمطية > إضافة وحدة نمطية جديدة**، كما هو موضح في الصورة.



الخطوة 3. في صفحة الوحدات النمطية المتاحة، حدد **إضافة وحدة نمطية جديدة** في جزء الوحدة النمطية لشبكة التهديد، كما هو موضح في الصورة.

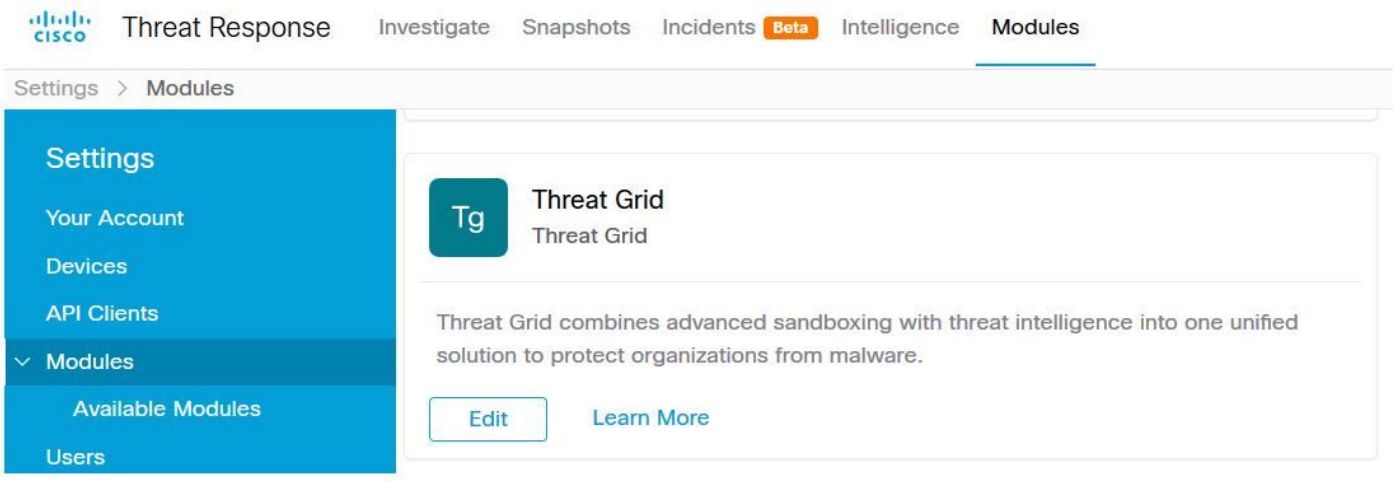
الخطوة 4. يفتح نموذج **إضافة وحدة نمطية جديدة**. أكمل النموذج كما هو موضح في الصورة.

- **اسم الوحدة النمطية** - أترك الاسم الافتراضي أو أدخل اسما ذا معنى لك.
- **URL** - من القائمة المنسدلة، أختر URL المناسب للموقع الذي يستند إليه حساب شبكة التهديدات (أمريكا الشمالية أو أوروبا). تجاهل الخيار **الآخر** في الوقت الحالي.

الخطوة 5. حدد **حفظ** لإكمال تكوين الوحدة النمطية لشبكة التهديدات.

الخطوة 6. يتم عرض "شبكة التهديدات" الآن أسفل التكوينات الخاصة بك في صفحة **الوحدات النمطية** كما هو موضح في الصورة.

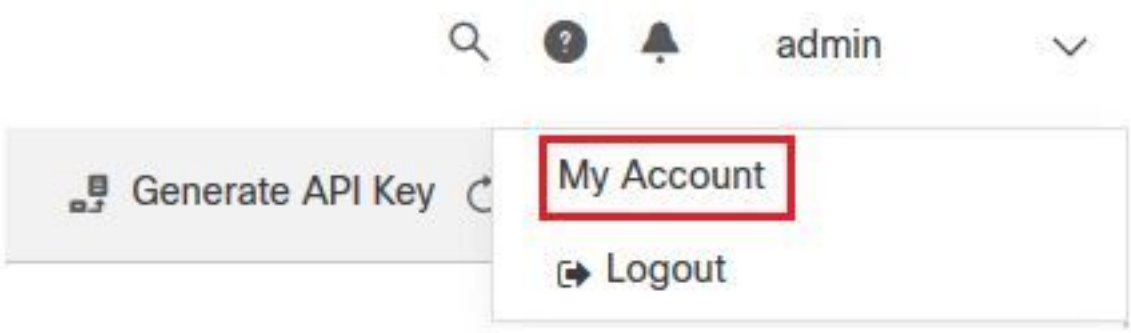
(يتوفر TG من قوائم المحور وفي دفاتر الحالة لتحسين التحقيق في التهديدات).



وحدة التحكم في شبكة التهديدات - السماح لشبكة التهديدات بالوصول إلى الاستجابة للتهديدات

الخطوة 1. سجل الدخول إلى شبكة التهديد باستخدام بيانات اعتماد المسؤول.

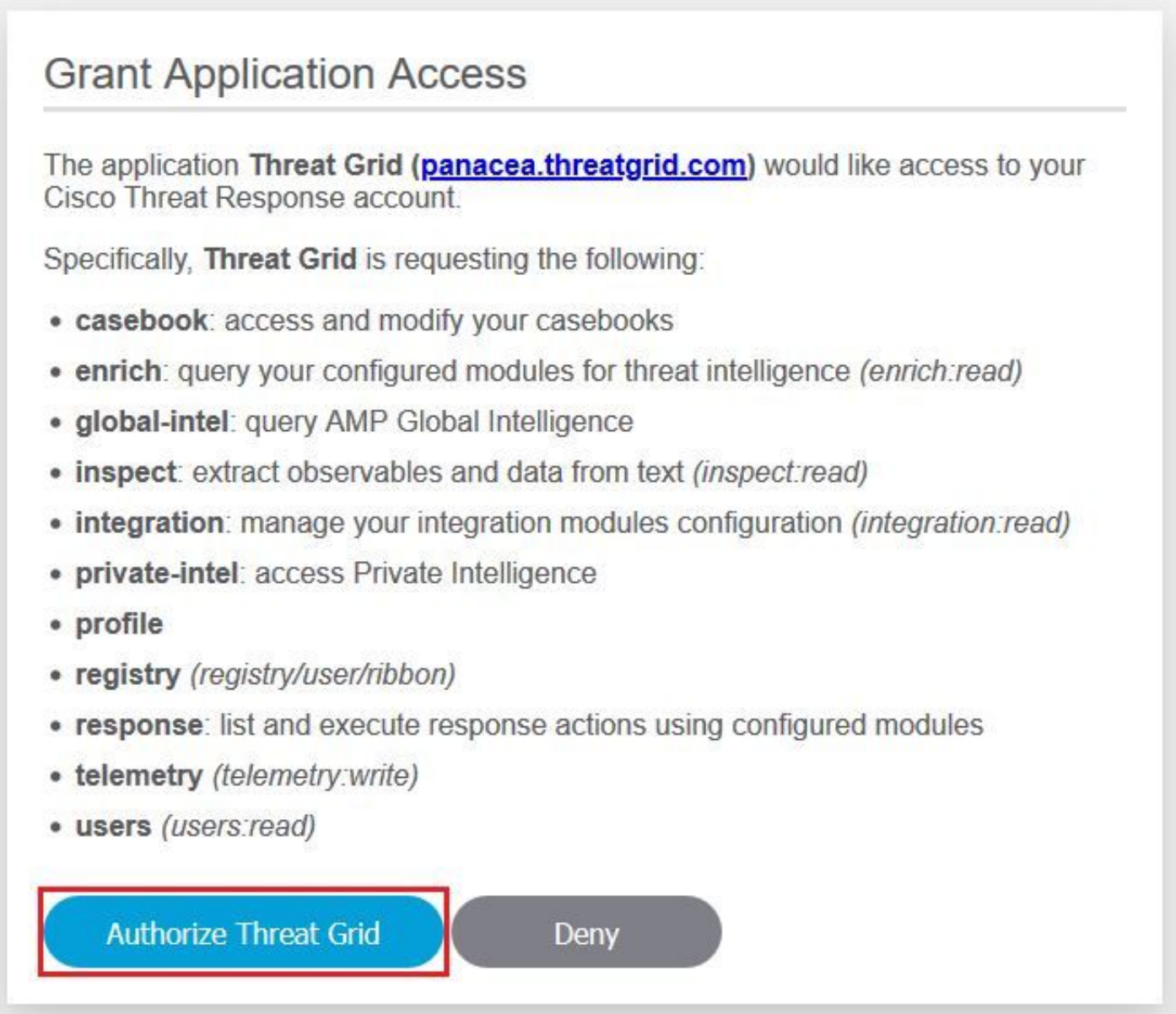
الخطوة 2. انتقل إلى قسم **حساب**، كما هو موضح في الصورة.



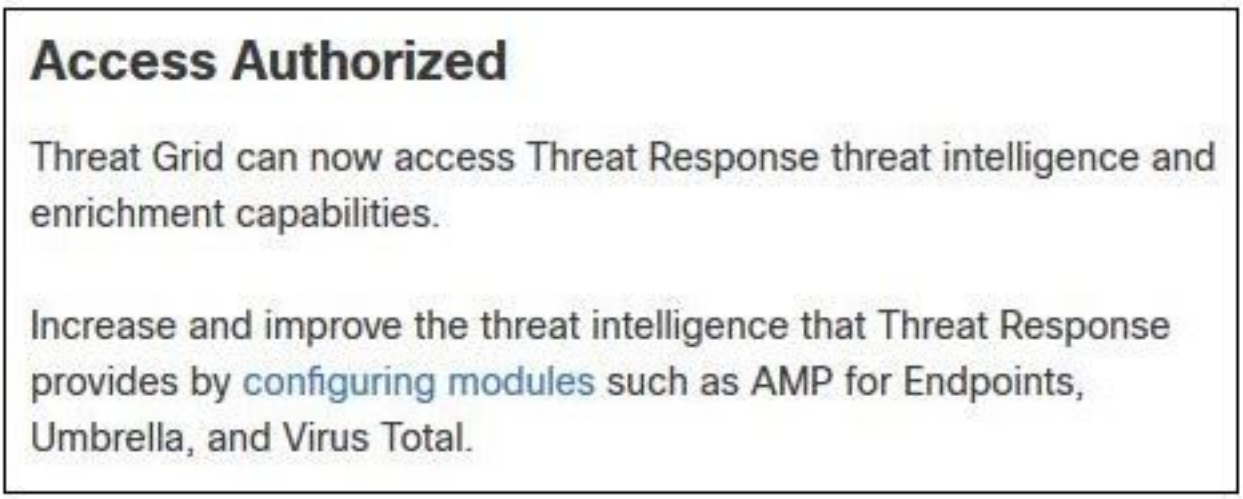
الخطوة 3. انتقل إلى قسم **الاتصالات** وحدد **خيار توصيل الاستجابة للتهديدات** كما هو موضح في الصورة.

سبتمبر 4. حدد خيار **التخويل** للسماح لشبكة التهديد بالوصول إلى إستجابة تهديدات Cisco، كما هو موضح في الصورة.

الخطوة 5. حدد خيار **تخويل شبكة تهديدات** لمنح الوصول إلى التطبيق، كما هو موضح في الصورة.



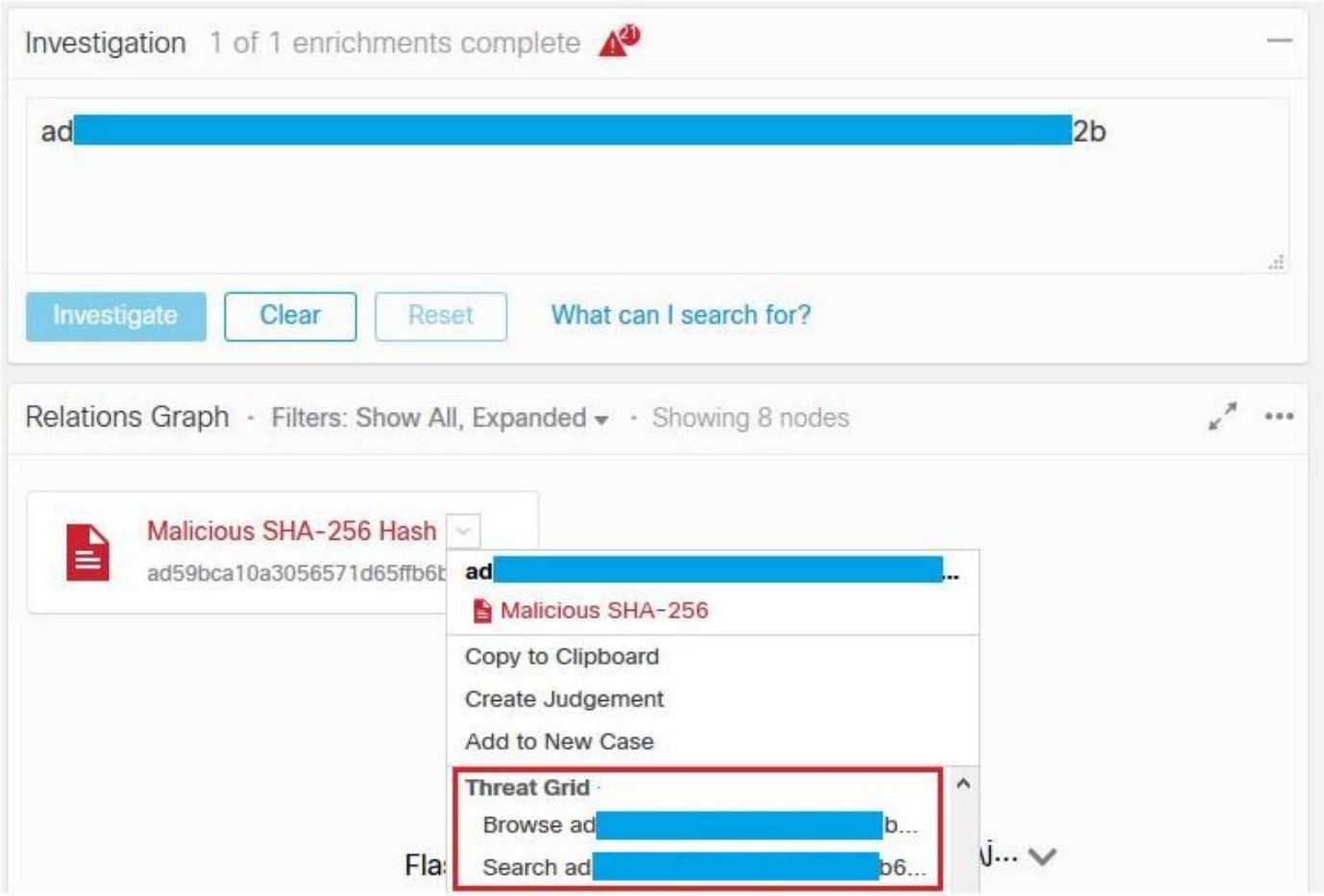
الخطوة 6. يجب أن الرسالة المصرح بها للوصول تتحقق من أن شبكة التهديدات لديها إمكانية الوصول إلى معلومات إستخباراتية وقدرات إثراء تتعلق بتهديد الرد على التهديد، كما هو موضح في الصورة.



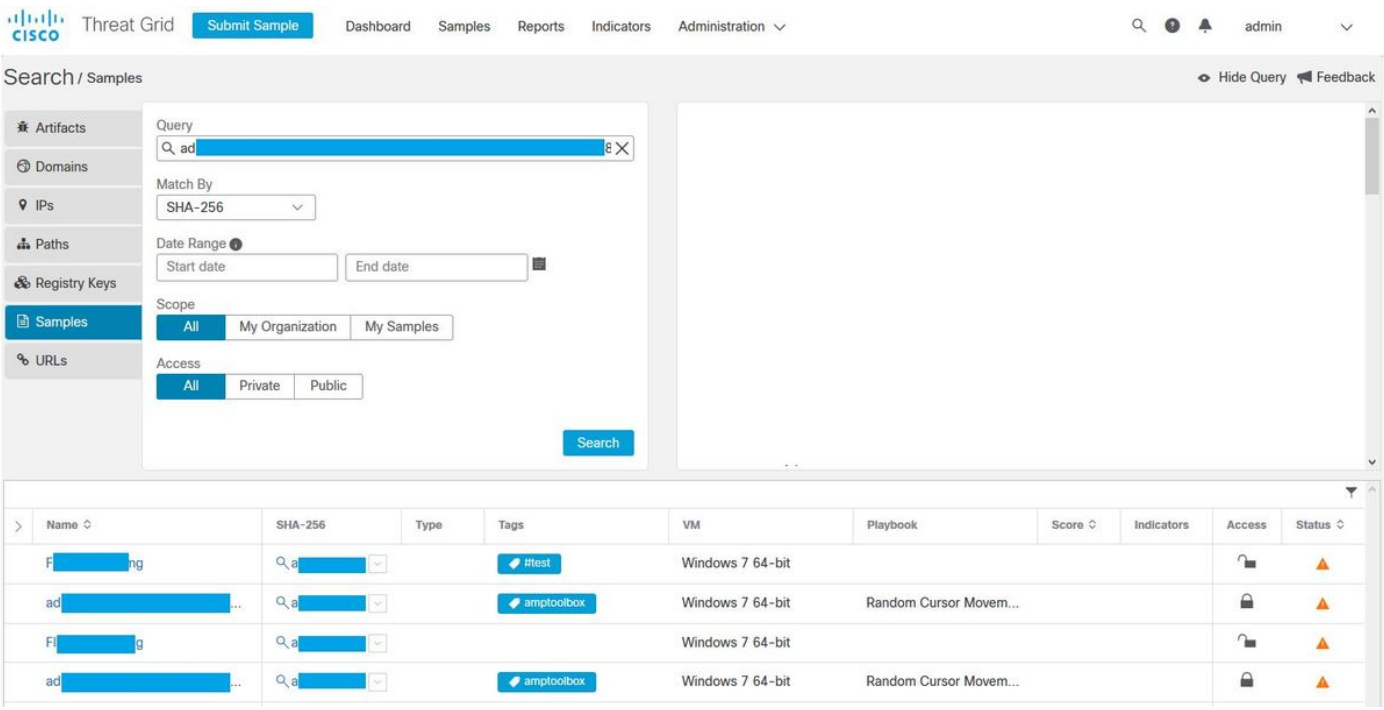
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من تكامل CTR و TG، يمكنك إجراء **تحقيق** على وحدة تحكم CTR، عندما تظهر جميع تفاصيل **التحقيق**، يمكنك رؤية خيار شبكة التهديد، كما هو موضح في الصورة.



يمكنك تحديد خيار إستعراض أو بحث في شبكة التهديد وإعادة توجيهه إلى بوابة شبكة التهديد لجمع معلومات إستخباراتية إضافية حول الملفات / التجزئة / ip / المجالات / عناوين URLs في مخزن معلومات شبكة التهديد، كما هو موضح في الصورة.



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).