التحقق من المجال في عنصر تحكم سحابة الأمان - تحديث CUI

المحتويات

المقدمة

يصف هذه وثيقة كيف الـ جديد مجال تحقق في أمن طبقة تحكم (SCC) بعد الـ cisco هوية تحديث موحدة (CUI).

الخلفية

عند المطالبة بمجال والتحقق من صحته في "التحكم في سحابة أمان Cisco" (SCC)، يطلب من المسؤولين نشر سجل DNS TXT لإثبات ملكية المجال.

المشكلة

هناك تغيير في وضع سجل DNS المطلوب للتحقق بنجاح. تستخدم التعليمات السابقة مجال تحقق فرعي مخصص Cisco المشار إليها في وثائق:

_cisco-sxso-verification.example.com

ومع ذلك، تتطلب عملية التحقق الحالية نشر رمز التحقق من TXT المقدم من Cisco مباشرة تحت المجال الجذر، بدلا من المجال الفرعي المخصص للتحقق.

ما الذي تغير؟

التكوين السابق (لم يعد ينطبق على سير عمل التحقق الحالي):

حقل DNS	القيمة
نوع السجل	تكست
المضيف / الاسم	_cisco-sxso-verification.example.com

القيمة	رمز التحقق المميز من Cisco

تكوين جديد (مطلوب):

حقل DNS	القيمة
نوع السجل	تكست
المضيف / الاسم	@
القيمة	رمز التحقق المميز من Cisco

الحل

خطوات التنفيذ

1. قم بتسجيل الدخول إلى موفر DNS للمجال الخاص بك (GoDaddy، CloudFlare، Route 53، Azure DNS، وما إلى ذلك).
2. انتقل إلى إدارة DNS للمجال.
3. إنشاء سجل TXT جديد.
4. قم بتكوين السجل كما يلي:
   النوع: تكست
   المضيف / الاسم: @
   القيمة: لصق رمز التحقق المميز الذي تم إنشاؤه بواسطة Cisco SCC.
   ttl: القيمة الافتراضية.
5. حفظ سجل DNS والسماح بوقت نشر DNS.
6. ارجع إلى Cisco SCC وانقر فوق التحقق.

التحقق

يمكنك تأكيد نشر سجل TXT بشكل صحيح باستخدام هذا الأمر:

```
dig TXT example.com
```

يجب أن تتضمن الاستجابة رمز التحقق من Cisco المميز.

بمجرد ظهور السجل في DNS، قم بالرجوع إلى SCC وأعد محاولة التحقق من المجال.

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).