إنشاء سياسة WhiteList على Cisco ESA لاختبارات تعليم التصيد الاحتيالي

المحتويات

المقدمة

يوضح هذا المستند كيفية إنشاء سياسة قائمة على البيانات البيضاء على جهاز أمان البريد الإلكتروني (ESA) من Cisco أو مثيل أمان البريد الإلكتروني للسحابة (CES) للسماح باختبارات/حملات تعليم التصيد الاحتيالي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- التنقل في القواعد وتكوينها على Cisco ESA/CES على WebUI.
- يتم إنشاء عوامل تصفية الرسائل على Cisco ESA/CES على واجهة سطر الأوامر (CLI).
- معرفة المورد المستخدم لحملة/إختبار التصيد الاحتيالي.

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

معلومات أساسية

سيكون لدى المسؤولين الذين يقومون بتنفيذ إختبارات أو حملات تعليم التصيد الاحتيالي رسائل بريد إلكتروني تم إنشاؤها تتضمن معلومات سيتم مطابقتها مع قواعد Talos الحالية الخاصة بمجموعات قواعد مكافحة البريد العشوائي و/أو عامل تصفية التفشي. وفي مثل هذا الحدث، لن تصل رسائل البريد الإلكتروني الخاصة بحملات التصيد الاحتيالي إلى المستخدمين النهائيين، كما سيتم التأثير عليها من قبل Cisco ESA/CES نفسها مما يؤدي إلى توقف الاختبار. وسيتعين على المسؤولين التأكد من أن الإيسا/مركز الأنظمة الإلكترونية يسمح من خلال رسائل البريد الإلكتروني هذه بتنفيذ حملتهم/إختبارهم.

التكوين

تحذير: موقف Cisco من بائعي محاكاة التصيد الاحتيالي والتعليم بشكل عام غير مسموح به. وننصح المسؤولين بالعمل مع خدمة محاكاة التصيد الاحتيالي *(على سبيل المثال: PhishMe)* للحصول على عناوين IP الخاصة بهم ثم إضافتها محليا إلى Whitelist. يجب على Cisco حماية عملاء ESA/CES التابعين لنا من عناوين IP هذه في حالة تغيير أيديهم أو تحولهم بالفعل إلى تهديد.

تحذير: يجب على المسؤولين الحفاظ على عناوين IP هذه في جهاز أبيض فقط أثناء الاختبار، وقد يؤدي ترك عناوين IP الخارجية على جهاز أبيض لفترة طويلة من الوقت بعد الاختبار إلى جلب رسائل بريد إلكتروني غير مرغوب فيها أو ضارة للمستخدمين النهائيين في حال تم أختراق عناوين IP هذه.

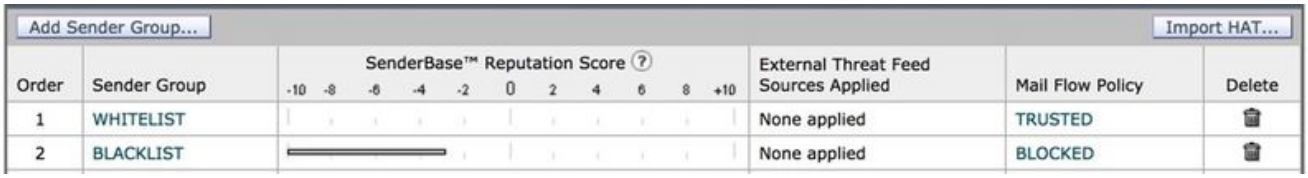
في جهاز أمان البريد الإلكتروني (ESA) من Cisco، قم بإنشاء مجموعة مرسل جديدة لمحاكاة التصيد الاحتيالي لديك وتعيينها إلى نهج تدفق البريد الموثوق به الذي يبلغ دولارا أمريكيا. سيتيح ذلك تسليم كافة رسائل البريد الإلكتروني لمحاكاة التصيد الاحتيالي إلى المستخدمين النهائيين. لا يخضع أعضاء مجموعة المرسلين الجديدة هذه لتحديد المعدل، ولا يتم فحص المحتوى من هؤلاء المرسلين بواسطة محرك Cisco IronPort Anti-Spam Engine، ولكن لا يزال يتم فحصه بواسطة برنامج مكافحة الفيروسات.

ملاحظة: بشكل افتراضي، تم تمكين "مكافحة الفيروسات" لنهج تدفق البريد الموثوق به الذي يبلغ $TRUSTED ولكن تم إيقاف تشغيل "مكافحة البريد العشوائي".

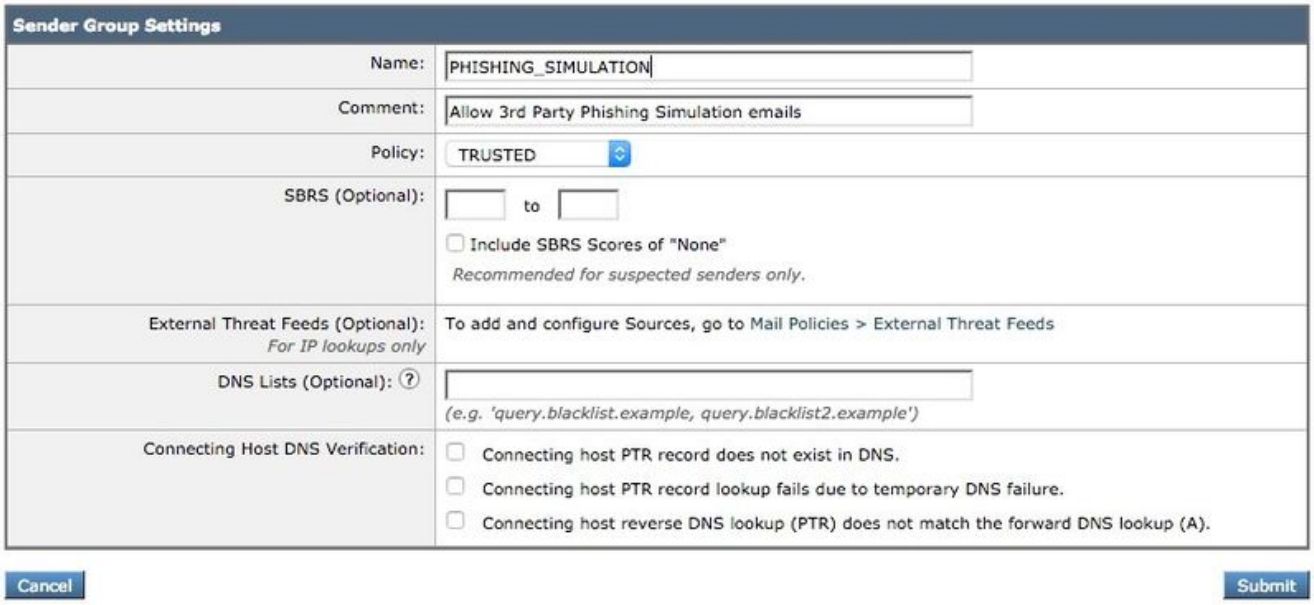
إنشاء مجموعة المرسلين

1. انقر فوق علامة التبويب ***سياسات البريد***.
2. تحت قسم ***جدول وصول المضيف***، حدد ***نظرة عامة على HAT***

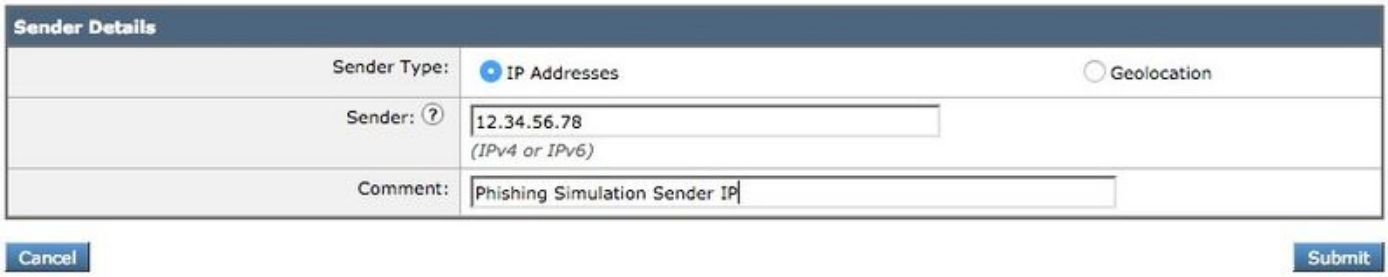
3. على اليمين، تأكد من تحديد وحدة إصغاء ***InboundMail*** حاليا،
4. من عمود ***مجموعة المرسلين*** أدناه، انقر فوق ***إضافة مجموعة مرسل...***،



5. قم بتعبئة حقلي ***الاسم*** و***التعليق***. تحت القائمة المنسدلة ***النهج***، حدد '$TRUSTED' ثم انقر فوق ***إرسال*** و***إضافة المرسلين*** >>.



6. أدخل IP أو اسم المضيف الذي تريده أن يكون أبيض اللون في الحقل الأول. سيزودك شريك محاكاة الخداع بمعلومات IP الخاصة بالمرسل.



عند الانتهاء من إضافة الإدخالات، انقر فوق الزر ***إرسال***. تذكر النقر فوق الزر ***تنفيذ التغييرات*** لحفظ التغييرات.

إنشاء عامل تصفية الرسائل

بعد إنشاء "مجموعة المرسلين" للسماح بتجاوز Anti-Spam و Anti-Virus، يلزم "عامل تصفية الرسائل" لتخطي محركات الأمان الأخرى التي قد تطابق حملة/إختبار التصيد الاحتيالي.

1. الاتصال ب CLI الخاص ب ESA.
2. قم بتشغيل ***عوامل تصفية*** الأوامر.
3. قم بتشغيل الأمر ***جديد*** لإنشاء عامل تصفية رسائل جديد.
4. انسخ مثال عامل التصفية التالي ولصقه، مع إجراء تحريرات على أسماء مجموعة المرسلين الفعلية إذا لزم الأمر:

```
:skip_amp_graymail_vof_for_phishing_campaigns
```

```
("if(sendergroup == "PHISHING_SIMULATION
                                                    }
                                          ;()skip-ampcheck
                                 ;()skip-marketingcheck
                                    ;()skip-socialcheck
                                      ;()skip-bulkcheck
                                       ;()skip-vofcheck
                                                    {
```

5. ارجع إلى موجه أوامر واجهة سطر الأوامر (CLI) الرئيسية واضغط مفتاح الإدخال.
6. قم بتشغيل ***الالتزام*** لحفظ التكوين.

التحقق من الصحة

أستخدم مورد جهة خارجية لإرسال حملة/إختبار مخادعة والتحقق من النتائج الموجودة على سجلات تعقب الرسائل للتأكد من تخطي كافة المحركات وتسليم البريد الإلكتروني.

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).