اكتشاف انتحال البريد الإلكتروني ومنعه

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

حول هذا المستند

ما هو انتحال البريد الإلكتروني؟

كيف يعمل دفاع انتحال البريد الإلكتروني

الطبقة 1: التحقق من صحة المجال المرسل

الطبقة 2: التحقق من الرأس باستخدام DMARK

الطبقة 3: منع مرسلي البريد العشوائي من إساءة استخدام البريد الإلكتروني المنتحلة

الطبقة 4: تحديد المرسلين الضارين عبر مجال البريد الإلكتروني

الطبقة 5: تقليل الإيجابيات الخاطئة باستخدام نتائج التحقق من DKIM أو SPF

الطبقة 6: الكشف عن الرسائل التي يحتمل أن تكون تحمل اسم مرسل مزور

الطبقة 7: البريد الإلكتروني الانتحالي الذي تم التعرف عليه بشكل إيجابي

الطبقة 8: الحماية من عناوين URL الخادعة

الطبقة 9: المكافحة الدفاعية من تهديد البريد الإلكتروني من Cisco (ETD)

إذا كنت لا تستطيع أن تفعل أكثر من منع الانتحال

المقدمة

يوضح هذا المستند كيفية اكتشاف انتحال البريد الإلكتروني ومنعه عند إستخدام بريد Cisco الإلكتروني الآمن.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية.

- بريد Cisco الإلكتروني الآمن

المكونات المستخدمة

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.

حول هذا المستند

هذا المستند مخصص لعملاء Cisco، وشركاء قنوات Cisco، ومهندسي Cisco الذين يقومون بنشر بريد إلكتروني آمن من Cisco. يغطي هذا المستند:

- ما هو انتحال البريد الإلكتروني؟
- سير عمل دفاع انتحال البريد الإلكتروني
- ما الذي يمكنك القيام به أكثر مع منع الانتحال؟

ما هو انتحال البريد الإلكتروني

انتحال البريد الإلكتروني هو تزييف رأس البريد الإلكتروني حيث يبدو أن الرسالة نشأت من شخص ما أو في مكان ما غير المصدر الحقيقي. يتم إستخدام انتحال رسائل البريد الإلكتروني في حملات التصيد الاحتيالي والرسائل غير المرغوب فيها لأنه من المحتمل أن يقوم الأشخاص بفتح بريد إلكتروني عندما يعتقدون أن مصدرا شرعيا وجديرا بالثقة قد أرسله. لمزيد من المعلومات حول الانتحال، يرجى الرجوع إلى [ما هو انتحال البريد الإلكتروني وكيفية اكتشافه](#).

يقع انتحال رسائل البريد الإلكتروني في هذه الفئات:

هدف رئيسي	الوصف	الفئة
الموظفون	انتحال مجال مشابه في المظروف من كمجال للمستلم.	انتحال المجال المباشر
الموظفون	يظهر الرأس "من" مرسل شرعي باسم تنفيذي لمؤسسة. وتعرف هذه الخوادم أيضا باسم "تسوية البريد الإلكتروني للشركات" (BEC).	عرض الاسم الخداع
العملاء / الشركاء	يظهر الرأس "من" مرسل شرعي باسم العلامة التجارية لمؤسسة معروفة.	انتحال اسم العلامة التجارية
الموظفون / الشركاء	بريد إلكتروني بعنوان URL يحاول سرقة بيانات حساسة أو تسجيل الدخول إلى المعلومات من الضحية. يعد البريد الإلكتروني المزيف من أحد البنوك الذي يطلب منك النقر فوق إرتباط والتحقق من تفاصيل حسابك مثال على هجوم قائم على عنوان URL للتصيد الاحتيالي.	هجوم Phish المستند إلى عنوان URL
الموظفون / الشركاء	يظهر المظروف من أو من قيمة الرأس عنوان مرسل مماثل يقوم بانتحال عنوان حقيقي لتجاوز Sender Policy Framework (SPF)، و DomainKeys Defined Mail (DKIM)، وعمليات فحص مصادقة الرسائل المستندة إلى المجال وإعداد التقارير والمطابقة (DMARK).	هجوم على مجال قريب أو متشابه

الجميع	احصل على وصول غير مصرح به إلى حساب بريد إلكتروني حقيقي يخص شخصا ما، ثم ترسل رسائل بريد إلكتروني إلى ضحايا آخرين كمالك شرعي لحساب البريد الإلكتروني.	الاستيلاء على الحساب / الحساب الذي تم إختراقه

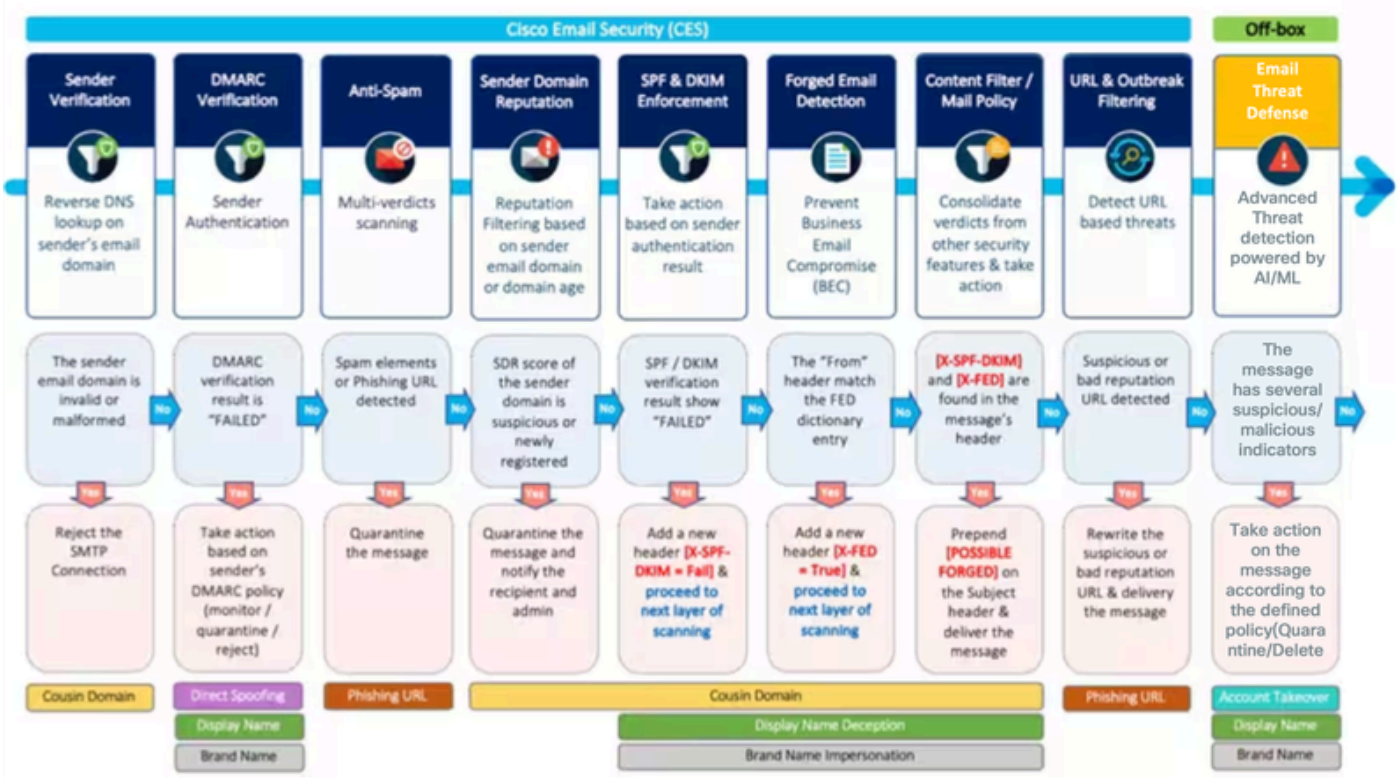
تتعلق الفئة الأولى بتعديات على اسم مجال المالك في المظروف من القيمة الموجودة في رأس البريد الإلكتروني على الإنترنت. يمكن للبريد الإلكتروني الآمن من Cisco إصلاح هذه الهجوم باستخدام التحقق من صحة خادم اسم مجال المرسل (DNS) للسماح فقط للمرسلين الشرعيين. ومن الممكن تحقيق نفس النتيجة على مستوى العالم باستخدام التحقق من SPF، و DKIM، و DMARK معيار.

ومع ذلك، تنتهك الفئات الأخرى جزء المجال من عنوان البريد الإلكتروني الخاص بالمرسل بشكل جزئي فقط. وبالتالي، ليس من السهل ردعه عندما تستخدم سجلات DNS النصية أو التحقق من المرسل فقط. من الأفضل، نظريا، دمج بعض مميزات البريد الإلكتروني الآمن من Cisco لمكافحة هذه التهديدات من Cisco والدفاع عن تهديد البريد الإلكتروني الآمن (ETD) من Cisco وتكوين المتقدمة. كما تعرف، يمكن أن تختلف إدارة البريد الإلكتروني الآمن من Cisco بسبب المميزات من مؤسسة إلى مؤسسة، ويمكن أن يؤدي التطبيق غير الصحيح إلى حدوث نسبة عالية من الإيجابيات الخاطئة. ولذلك، من الضروري فهم إحتياجات المنظمة في مجال الأعمال وتصميم المالمح.

سير عمل دفاع انتحال البريد الإلكتروني

يتم عرض مميزات الأمان التي تتعامل مع أفضل الممارسات لمراقبة هجمات الانتحال وتحذيرها وتنفيذها في الرسم التخطيطي (الصورة 1). يتم توفير تفاصيل لكل ميزة في هذا المستند. أفضل الممارسات هي منهج دفاعي معمق للكشف عن انتحال رسائل البريد الإلكتروني. يمكن للمهاجمين تغيير أساليبهم مقابل مؤسسة عبر الوقت، لذا يجب على المسؤول مراقبة أي تغييرات والتحقق من التحذيرات وعمليات الإنفاذ المناسبة.

الصورة 1. تدفقات الدفاع الخاصة بمخالفة البريد الإلكتروني الآمن من Cisco

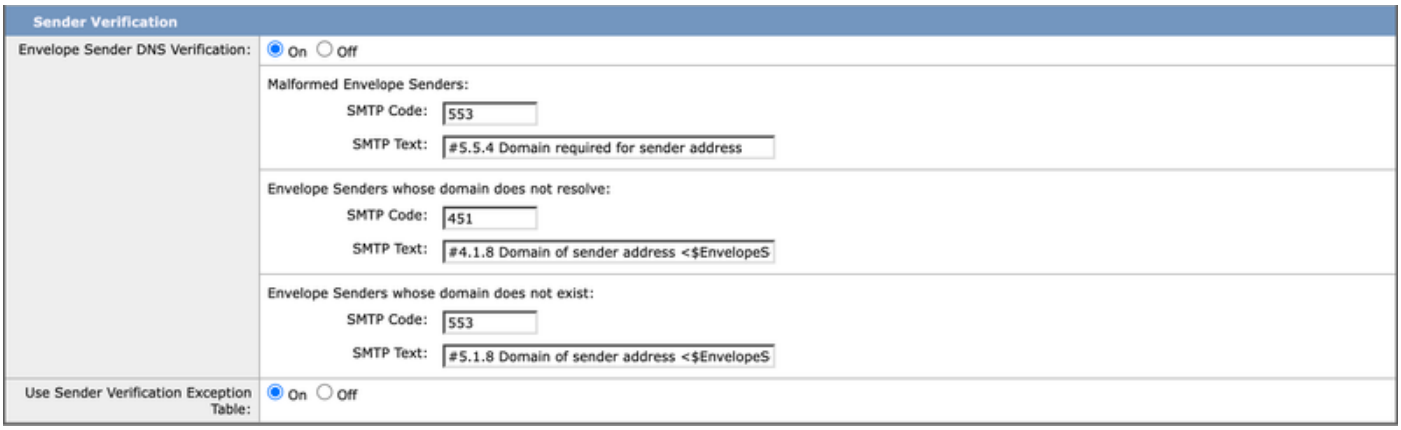


الطبقة 1: التحقق من صحة مجال المرسل

يعتبر "التحقق من المرسل" طريقة أكثر مباشرة لمنع رسائل البريد الإلكتروني المرسلة من مجال بريد إلكتروني زائف، مثل انتحال مجال ابن عم (على سبيل المثال، c1sc0.com وهو ملصق ل cisco.com). يقوم بريد Cisco الإلكتروني الآمن بإجراء استعلام سجل MX للمجال الخاص بعنوان البريد الإلكتروني للمرسل وإجراء بحث عن سجل على سجل MX أثناء محادثة SMTP. إذا قام استعلام DNS بإرجاع NXDOMAIN، فيمكن معاملة المجال على أنه غير موجود. ومن الأساليب الشائعة التي يستخدمها المعتدون لتزوير معلومات مرسل المغلف بحيث يتم قبول البريد الإلكتروني المرسل من مرسل لم يتم التحقق منه ومعالجته بشكل أكبر. يمكن أن يرفض بريد Cisco الإلكتروني الآمن جميع الرسائل الواردة التي تفشل في التحقق من التحقق من الصحة الذي يستخدم هذه الميزة ما لم تتم إضافة مجال المرسل أو عنوان IP مسبقا في جدول الاستثناءات.

أفضل ممارسة: قم بتكوين بريد Cisco الإلكتروني الآمن لرفض محادثة SMTP إذا كان مجال البريد الإلكتروني لحقل مرسل المظروف غير صالح. السماح فقط للمرسلين الشرعيين من خلال تكوين نهج تدفق البريد والتحقق من المرسل وجدول الاستثناء (إختياري). لمزيد من المعلومات، تفضل بزيارة حماية المصلحة باستخدام "التحقق من المرسل".

الصورة 2. قسم التحقق من المرسل في نهج تدفق البريد الافتراضي



الطبقة 2: التحقق من الرأس باستخدام DMARK

تعد عملية التحقق من DMARK ميزة أكثر فعالية لمكافحة الانتحال المباشر للمجال، كما تتضمن أيضا هجمات اسم العرض وانتحال العلامة التجارية. يربط DMARK المعلومات المصادق عليها مع SPF أو DKIM (إرسال مصدر المجال أو التوقيع) مع ما يتم تقديمه إلى المستلم النهائي في الرأس "من" ويتحقق من أن معرفات SPF و DKIM متوافقة مع معرف الرأس "من".

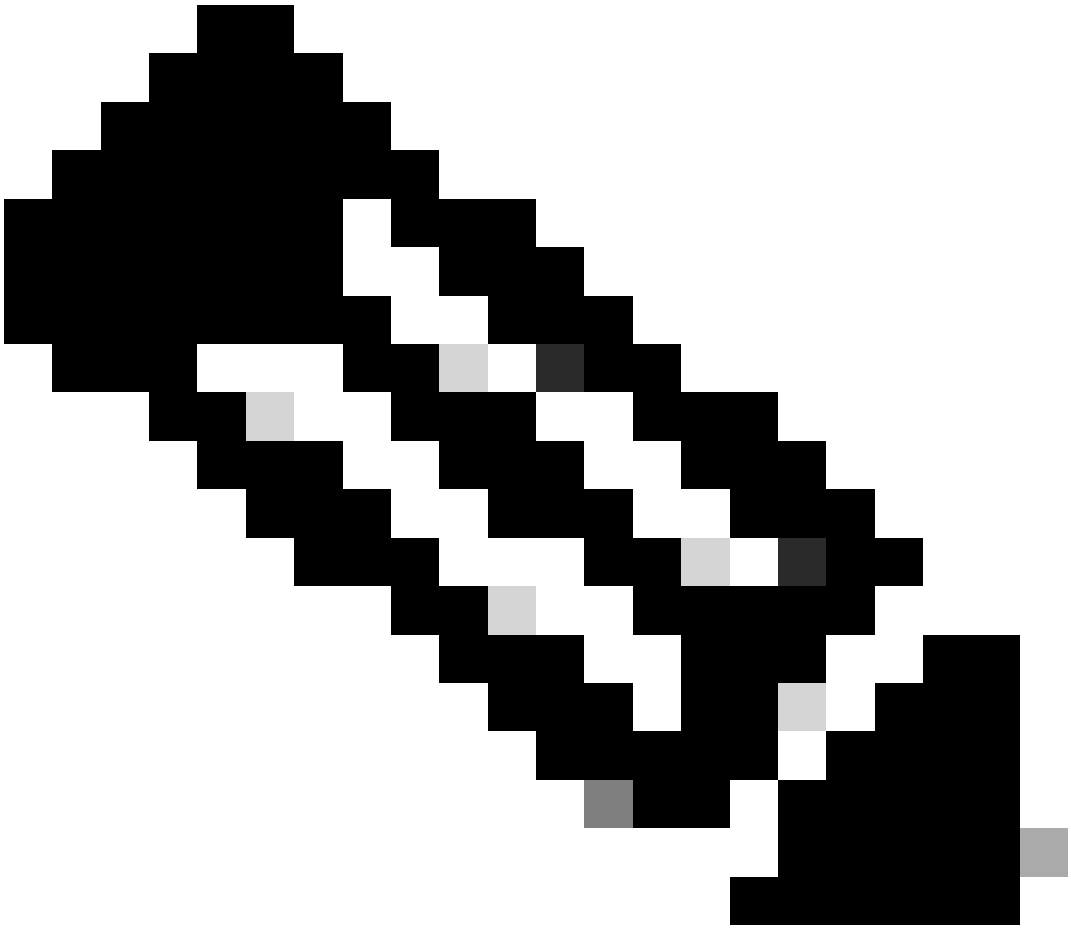
لتمرير التحقق من DMARK، يجب أن يمر البريد الإلكتروني الوارد بواحدة على الأقل من آليات المصادقة هذه. وبالإضافة إلى ذلك، يسمح البريد الإلكتروني الآمن من Cisco أيضا للمسؤول بتحديد ملف تعريف التحقق من DMARK لتجاوز سياسات DMARK لمالك المجال وإرسال تقارير التجميع (RUA) والفشل/الطب الشرعي (RUF) إلى مالكي المجال. ويساعد ذلك في تعزيز عمليات نشر المصادقة الخاصة بهم في المقابل.

أفضل ممارسة: تحرير ملف تعريف DMARK الافتراضي الذي يستخدم إجراءات نهج DMARK التي ينصحها المرسل. بالإضافة إلى ذلك، يجب تحرير الإعدادات العمومية للتحقق من DMARK لتمكين إنشاء التقرير الصحيح. بمجرد تكوين ملف التعريف بشكل صحيح، يجب تمكين خدمة التحقق من DMARK في النهج الافتراضي لسياسات تدفق البريد.

الصورة 3. ملف تعريف التحقق من DMARK

Create DMARC Verification Profile

Profile Name:	DEFAULT
Message Action when the Policy in DMARC Record is Reject:	○ No Action ○ Quarantine to: ACCOUNT_TAKEOVER (centralized) ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC unauthenticated mai
Message Action when the Policy in DMARC Record is Quarantine:	○ No Action ◉ Quarantine to: Policy (centralized)
Message Action for Temporary Failure:	◉ Accept ○ Reject SMTP Code: 451 SMTP Response: #4.7.1 Unable to perform DMARC v
Message Action for Permanent Failure:	○ Accept ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC verification failed.



ملاحظة: يجب تنفيذ DMARK عن طريق إرسال مالك المجال بالاقتران مع أداة مراقبة المجال، مثل Cisco Domain Protection. عند تنفيذه بشكل مناسب، يساعد تنفيذ DMARK في Cisco Secure Email على الحماية من رسائل البريد الإلكتروني للتصيد الاحتيالي التي يتم إرسالها إلى الموظفين من مرسلين أو مجالات غير مصرح بها. للحصول على مزيد من المعلومات حول Cisco Domain Protection، يرجى زيارة هذا الارتباط: نظرة سريعة على حماية مجال البريد الإلكتروني الآمن من Cisco.

الطبقة 3: منع مرسلي البريد العشوائي من إرسال رسائل البريد الإلكتروني المنتحلة

يمكن أن تكون هجمات الانتحال شكلا شائعا آخر من حملات البريد العشوائي. لذلك، يعد تمكين الحماية من البريد العشوائي أمرا أساسيا لتحديد رسائل البريد الإلكتروني الاحتيالية التي تحتوي على عناصر البريد الإلكتروني العشوائي/التصيد الاحتيالي بشكل فعال ومنعها بشكل إيجابي. توفر خدمة مكافحة البريد العشوائي، مقترنة بإجراءات أفضل الممارسات الأخرى الموصوفة بشكل شامل في هذا المستند، أفضل النتائج دون فقد رسائل البريد الإلكتروني الشرعية.

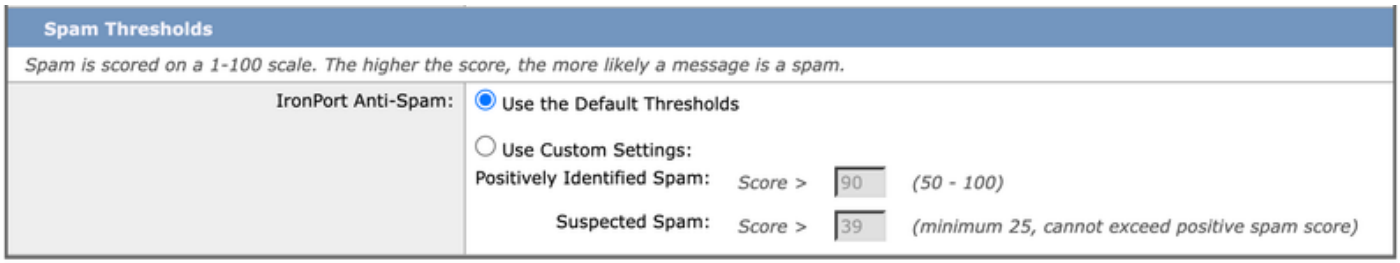
أفضل الممارسات: تمكين المسح الضوئي لمكافحة البريد العشوائي في نهج البريد الافتراضي وتعيين إجراء العزل لتحديد إعدادات البريد العشوائي بشكل إيجابي. قم بزيادة الحد الأدنى لحجم المسح الضوئي لرسائل البريد العشوائي إلى 2 م على الأقل بشكل عام.

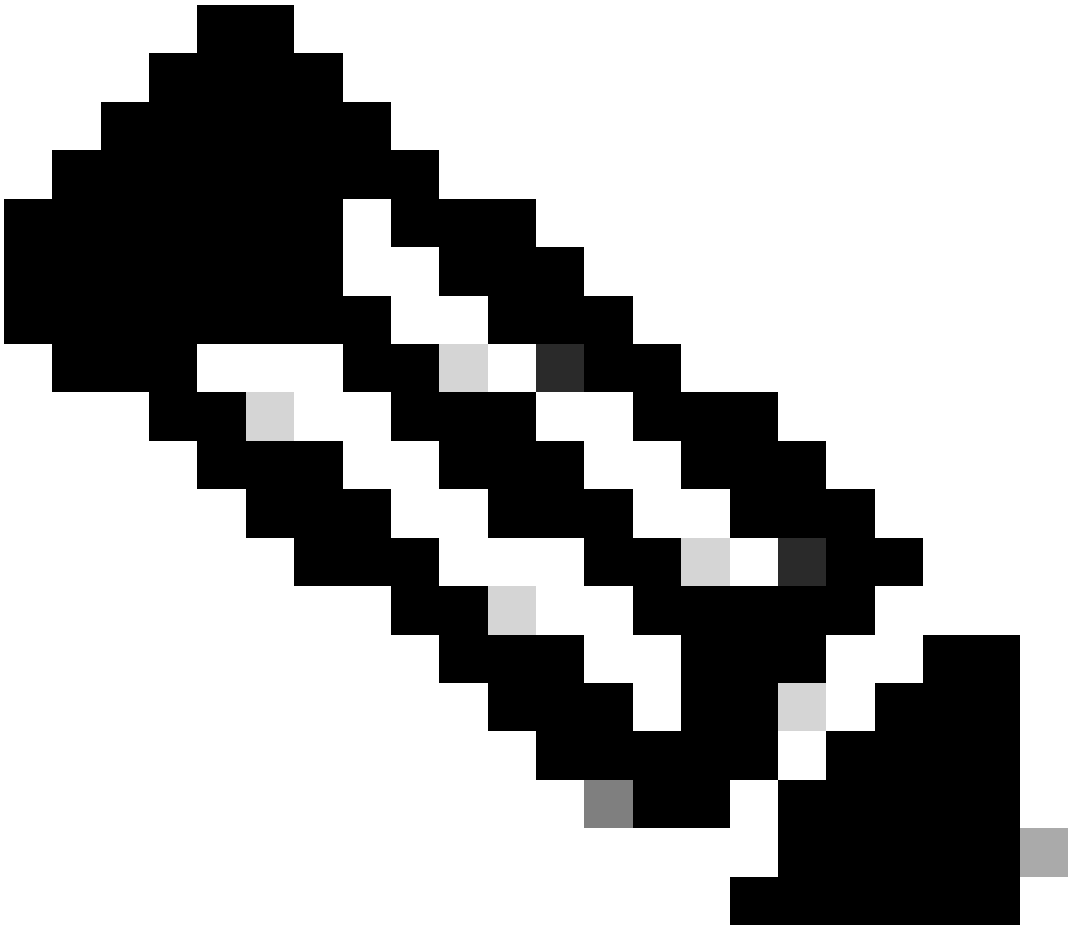
الصورة 4. إعداد مكافحة البريد العشوائي في نهج البريد الافتراضي

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	◉ Use IronPort Anti-Spam service ○ Disabled
Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine *Note: If local and external quarantines are defined, mail will be sent to local quarantine.*
Add Text to Subject:	Prepend [SPAM]
▷ Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	○ No ◉ Yes
Apply This Action to Message:	Deliver Send to Alternate Host (optional):
Add Text to Subject:	Prepend [SUSPECTED SPAM]
▷ Advanced	Optional settings for custom header and message delivery.

يمكن ضبط حد البريد العشوائي للبريد العشوائي الإيجابي والمشتبه فيه لزيادة الحساسية أو تقليلها (الصورة 5)، ومع ذلك، تثني Cisco المؤول عن القيام بذلك والا تستخدم إلا الحدود الافتراضية كخط أساس إلا إذا أبلغت Cisco خلاف ذلك.

الصورة 5. إعداد حدود مكافحة البريد العشوائي في نهج البريد الافتراضي





ملاحظة: يوفر البريد الإلكتروني الآمن من Cisco محرك مسح متعدد ذكي (IMS) يوفر مجموعات مختلفة من محرك مكافحة البريد العشوائي لزيادة معدلات التقاط البريد العشوائي (أكثر معدلات الصيد عدوانية).

الطبقة 4: تحديد المرسلين الضارين عبر مجال البريد الإلكتروني

Cisco Talos Sender Domain Reputation (SDR) هي خدمة سحابية توفر حكما على السمعة لرسائل البريد الإلكتروني استنادا إلى المجالات الموجودة في مظروف البريد الإلكتروني والرأس. يتيح تحليل السمعة المستند إلى المجال معدل التقاط بريد عشوائي أعلى من خلال تجاوز السمعة المعروفة لعناوين IP المشتركة أو المضيفين أو موفري البنية

الأساسية. وبدلا من ذلك، فإنه يستمد الأحكام استنادا إلى المميزات المرتبطة بأسماء المجالات المؤهلة بالكامل (FQDN) ومعلومات المرسل الأخرى في المحادثة الخاصة ببروتوكول نقل البريد البسيط (SMTP) ورؤوس الرسائل.

يعد إستحقاق المرسل ميزة أساسية لتحديد سمعة المرسل. يتم إنشاء "نضج المرسل" تلقائيا لتصنيف البريد العشوائي استنادا إلى مصادر متعددة للمعلومات، ويمكن أن يختلف عن عمر المجال المستند إلى Whois. تم تعيين إستحقاق المرسل إلى حد 30 يوما، وبعد هذا الحد، يعتبر المجال ناضجا كمرسل بريد إلكتروني، ولا يتم توفير تفاصيل إضافية.

أفضل الممارسات: قم بإنشاء عامل تصفية محتوى وارد يلتقط مجال المرسل الذي يقع فيه الحكم بسمعة SDR تحت أمر غير موثوق به/مشكوك فيه أو يكون إستحقاق المرسل أقل من 5 أيام أو يساوي. الإجراء الموصى به هو إجراء عزل للرسالة وإعلام مسؤول أمان البريد الإلكتروني والمستلم الأصلي. لمزيد من المعلومات حول كيفية تكوين SDR، الرجاء عرض فيديو Cisco في [تحديث أمان البريد الإلكتروني من Cisco (الإصدار 12.0): سمعة مجال المرسل (SDR)]

الصورة 6. عامل تصفية المحتوى لسمعة SDR وعمر المجال مع إجراءات "الإعلام" و"العزل".

Conditions

Add Condition... | Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	Domain Reputation	sdr-reputation (['untrusted', 'questionable'], "")	
2	Domain Reputation	sdr-sender-maturity ("days", <=, 5, "")	

Actions

Add Action...

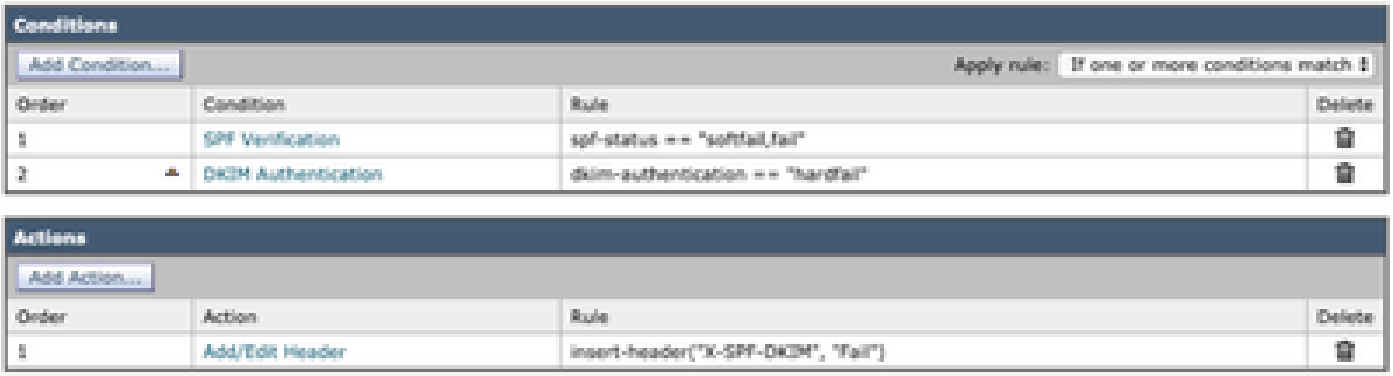
Order	Action	Rule	Delete
1	Notify	notify ("administrator@customer.com, $EnvelopeRecipients", "Malicious-SDR")	
2	Quarantine	quarantine("Policy")	

الطبقة 5: تقليل الإيجابيات الخاطئة باستخدام نتائج التحقق من SPF أو DKIM

من الضروري فرض التحقق من SPF أو DKIM (كل أو كل) لبناء طبقات متعددة من الكشف عن البريد الإلكتروني لمعظم أنواع الهجمات. بدلا من إتخاذ إجراء نهائي (مثل الإسقاط أو الحجر الصحي)، توصي Cisco بإضافة رأس جديد مثل [X-SPF-DKIM] على الرسالة التي تفشل في التحقق من SPF أو DKIM وتعاون النتيجة باستخدام ميزة اكتشاف البريد الإلكتروني المزيف (FED)، والتي يتم تغطيتها لاحقا، لصالح معدل التقاط محسن لرسائل البريد الإلكتروني المنتحلة.

أفضل الممارسات: إنشاء عامل تصفية محتوى يقوم بفحص نتائج التحقق من SPF أو DKIM لكل رسالة واردة تمر من خلال عمليات الفحص السابقة. قم بإضافة رأس X جديد (على سبيل المثال X-SPF-DKIM=Fail) على الرسالة التي تفشل في التحقق من SPF أو DKIM وتصل إلى الطبقة التالية من المسح الضوئي - اكتشاف البريد الإلكتروني المزيف (FED).

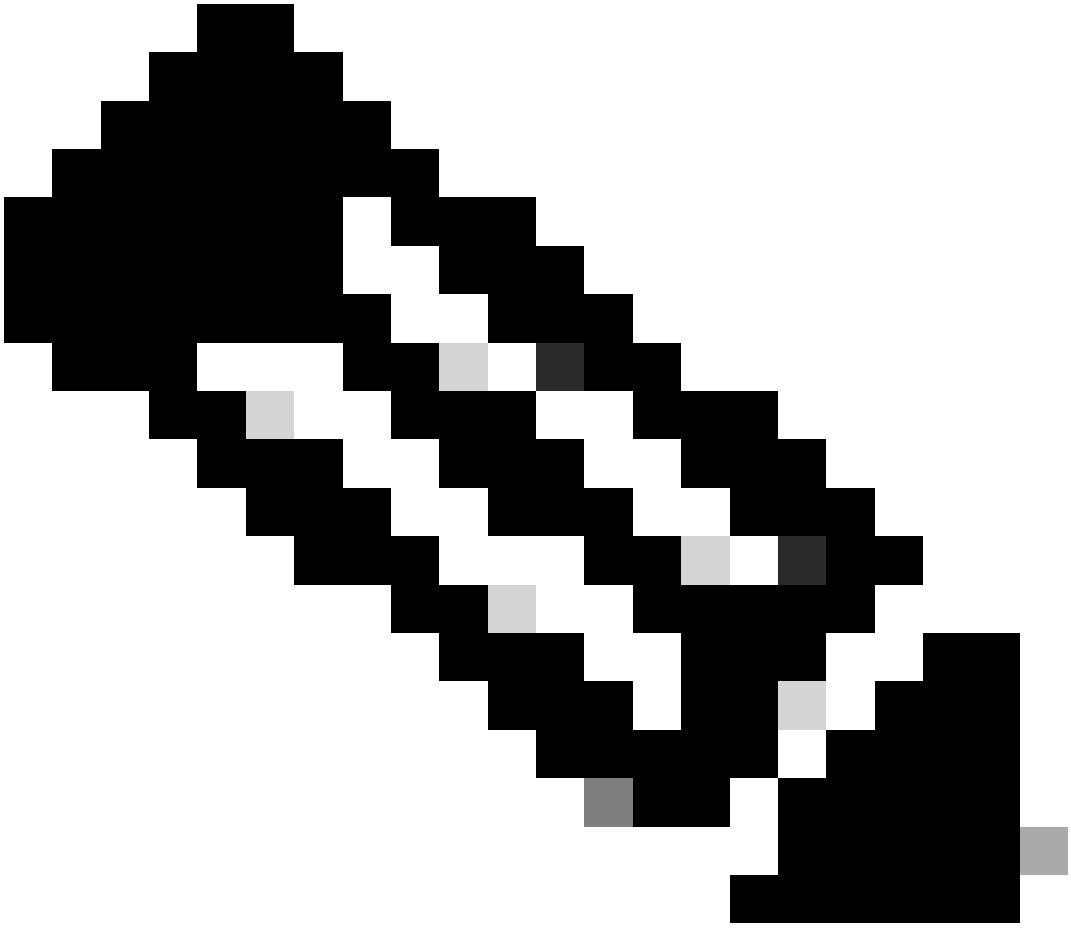
الصورة 7. عامل تصفية المحتوى الذي يفحص الرسائل بنتائج SPF أو DKIM الفاشلة



الطبقة 6: الكشف عن الرسائل التي يحتمل أن تكون تحمل اسم مرسل مزور

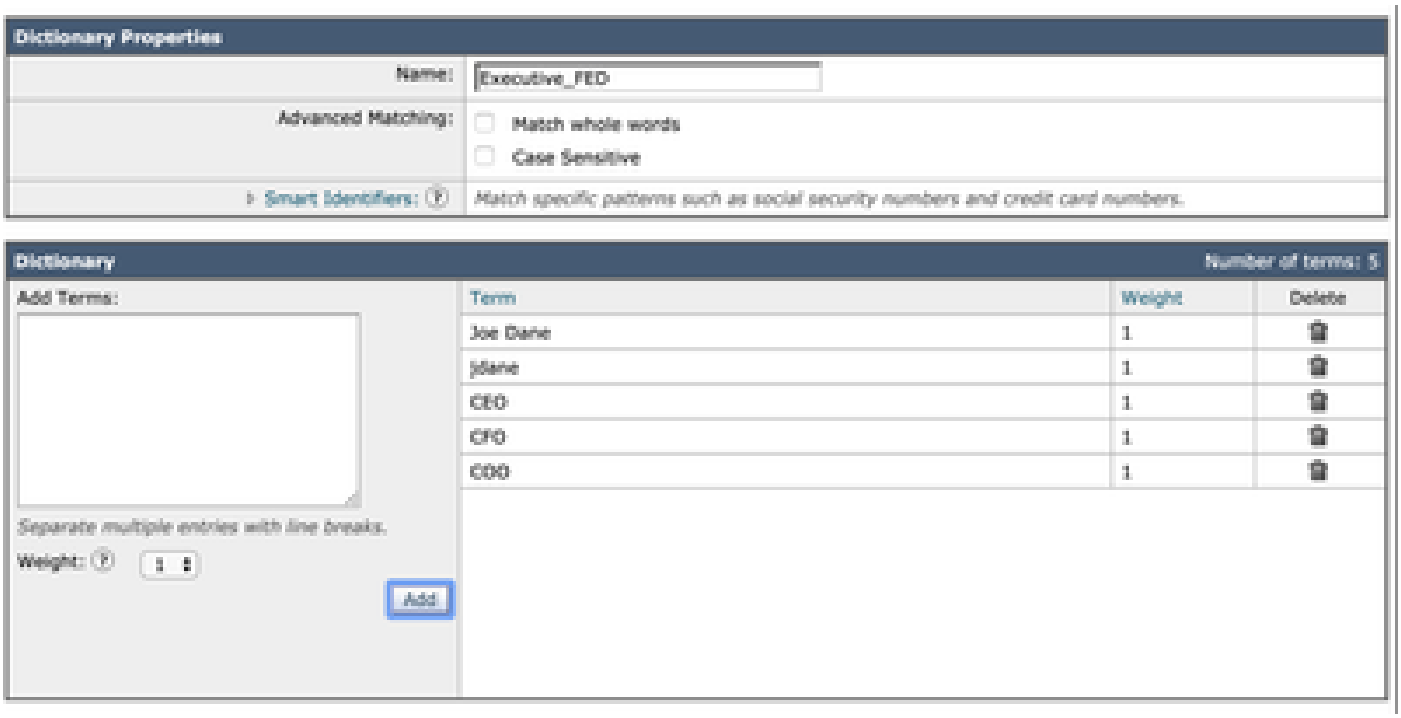
كما أن تكميل عمليات التحقق من SPF و DKIM و DMARK بالإضافة إلى الكشف المزور عن البريد الإلكتروني (FED) يعد خط دفاع آخر حاسم ضد انتحال البريد الإلكتروني. ويعد بنك الاحتياطي الفيدرالي مثالياً لعالج هجمات الانتحال التي تسيء إستخدام القيمة "من" في نص الرسالة. بافتراض أنك تعرف بالفعل الأسماء التنفيذية داخل المؤسسة، يمكنك إنشاء قاموس لهذه الأسماء ثم الإشارة إلى ذلك القاموس بحالة FED في مرشحات المحتوى. علاوة على ذلك، يمكنك إنشاء قاموس من مجالات قريبة أو متماثلة استناداً إلى مجالك باستخدام DNSTWIST (DNSTWIT) للمطابقة مع انتحال مجال متشابه.

أفضل الممارسات: حدد المستخدمين في مؤسستك الذين من المحتمل أن تكون رسائلهم مزورة. إنشاء قاموس مخصص يمثل المسؤولين التنفيذيين. لكل اسم تنفيذي، يجب أن يتضمن القاموس اسم المستخدم وجميع أسماء المستخدمين الممكنة كمصطلحات (الصورة 8). عند اكتمال القاموس، أستخدم اكتشاف البريد الإلكتروني المزيف في مرشح المحتوى لمطابقة قيمة "من" من الرسائل الواردة مع إدخالات القاموس هذه.



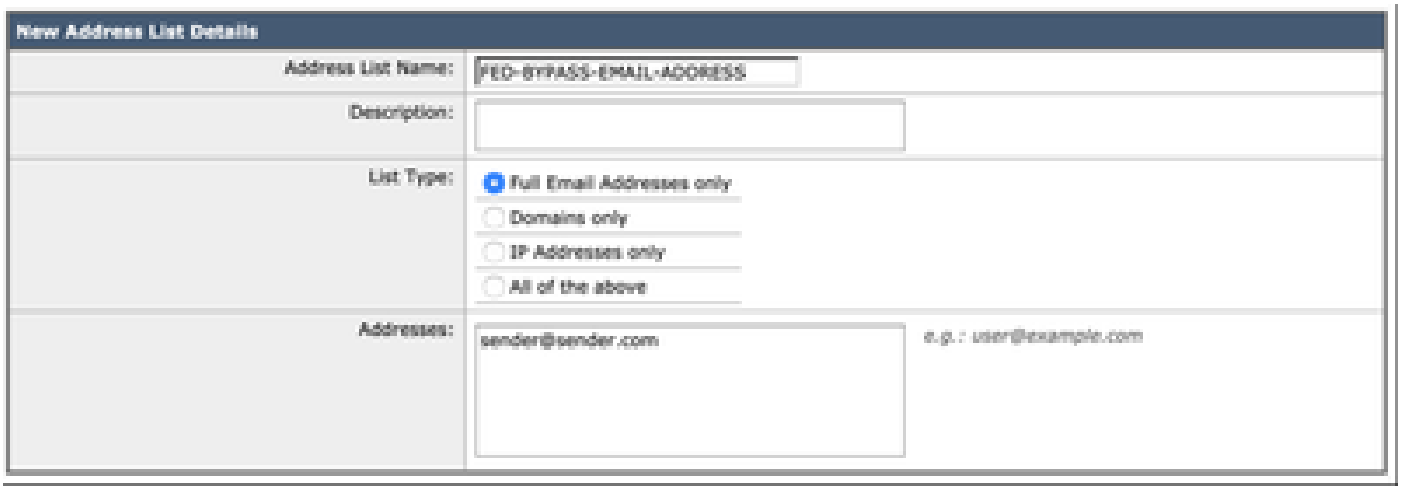
ملاحظة: نظرا لأن معظم المجالات ليست تعابير مسجلة، يحمي التحقق من مرسل DNS منها. إذا أخترت إستخدام إدخالات القاموس، انتبه فقط إلى المجالات المسجلة، وتأكد من عدم تجاوز 500 إلى 600 مدخل لكل قاموس.

الصورة 8. الدليل المخصص لاكتشاف البريد الإلكتروني المزيف



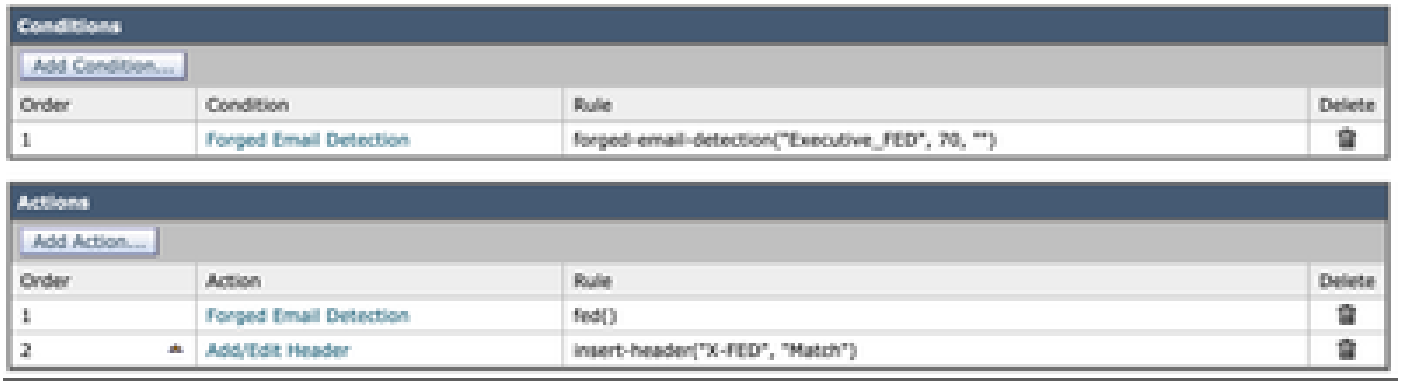
من الاختياري إضافة حالة إستثناء لمجال بريدك الإلكتروني في المغلف إرسال لتجاوز فحص FED. بدلا من ذلك، يمكن إنشاء قائمة عناوين مخصصة لتجاوز فحص FED إلى قائمة عناوين البريد الإلكتروني التي يتم عرضها في FromHeader (الصورة 9).

الصورة 9. إنشاء قائمة عناوين لتجاوز فحص FED



تطبيق الإجراء الخاص "الكشف المزور عن البريد الإلكتروني" لشطب القيمة "من" ومراجعة عنوان البريد الإلكتروني الفعلي لمرسل المظروف في علبة وارد الرسائل. ثم، بدلا من تطبيق عملية نهائية، قم بإضافة رأس X جديد (على سبيل المثال، X-FED=MATCH) على الرسالة التي تطابق الحالة واستمر في تسليم الرسالة إلى الطبقة التالية من التفتيش (صورة 10).

الصورة 10. إعداد عامل تصفية المحتوى الموصى به ل FED

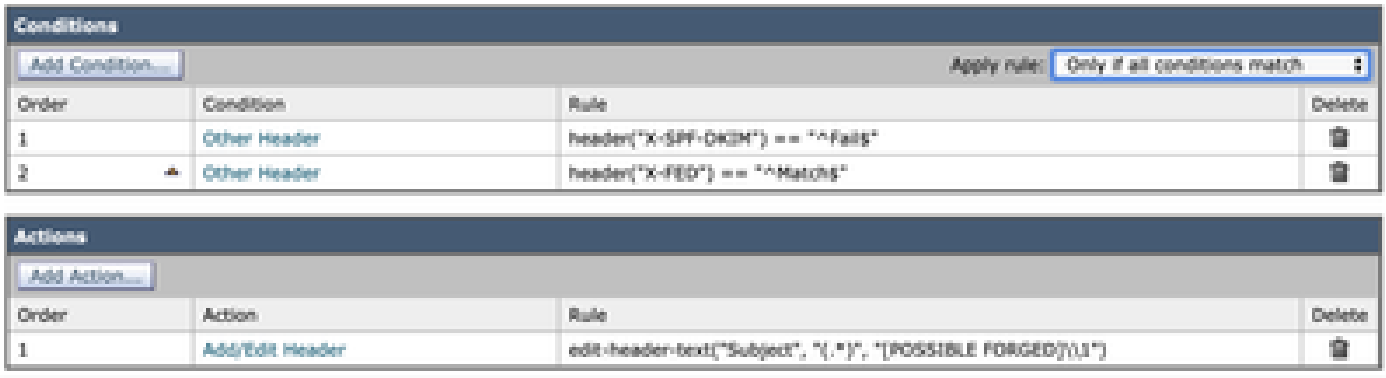


المستوى 7: البريد الإلكتروني الانتحال الذي تم التعرف عليه بشكل إيجابي

يعتبر تحديد حملة انتحال حقيقية أكثر فعالية من خلال الإشارة إلى أحكام أخرى من مختلف السمات الأمنية في خط الإنتاج، مثل معلومات الرأس السيني التي تنتجها وكالة إنفاذ القوانين التابعة للسلطة الشعبية الصينية/إدارة كيم وإنفاذ القانون. على سبيل المثال، يمكن للمسؤولين إنشاء عامل تصفية محتوى لتعريف الرسائل التي تمت إضافتها باستخدام كل من الرؤوس X الجديدة نتيجة فشل التحقق من SPF / DKIM (X-SPF-DKIM=Fail) وأي من الرؤوس يطابق إدخالات قاموس FED (X-FED=Match).

يمكن أن يكون الإجراء الموصى به إما الحجر الصحي على الرسالة وإبلاغ المستلم، أو متابعة تسليم الرسالة الأصلية مع تعليق كلمات [يمكن تزويرها] مسبقا على سطر الموضوع كتحذير للمستلم، كما هو موضح (الصورة 11).

الصورة 11. دمج كل الرؤوس س في قاعدة واحدة (نهائية)

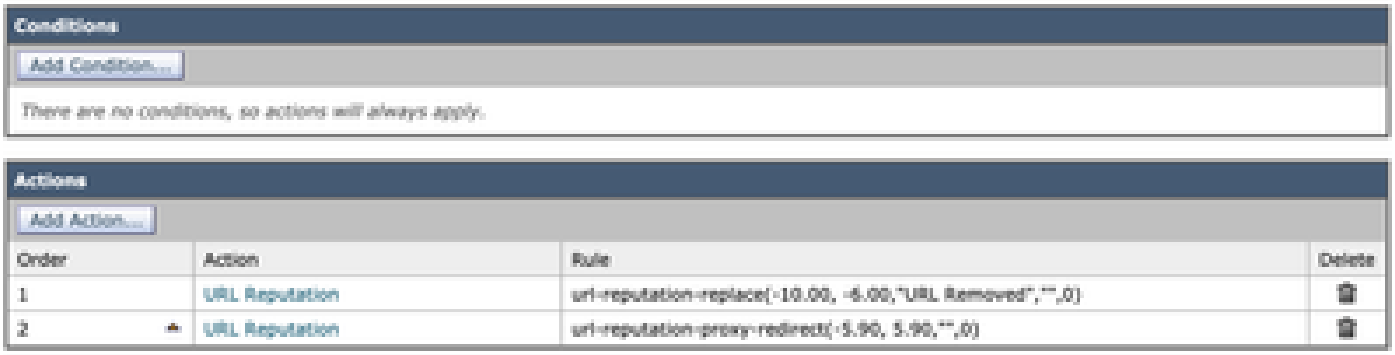


الطبقة 8: الحماية من عناوين URL الخادعة

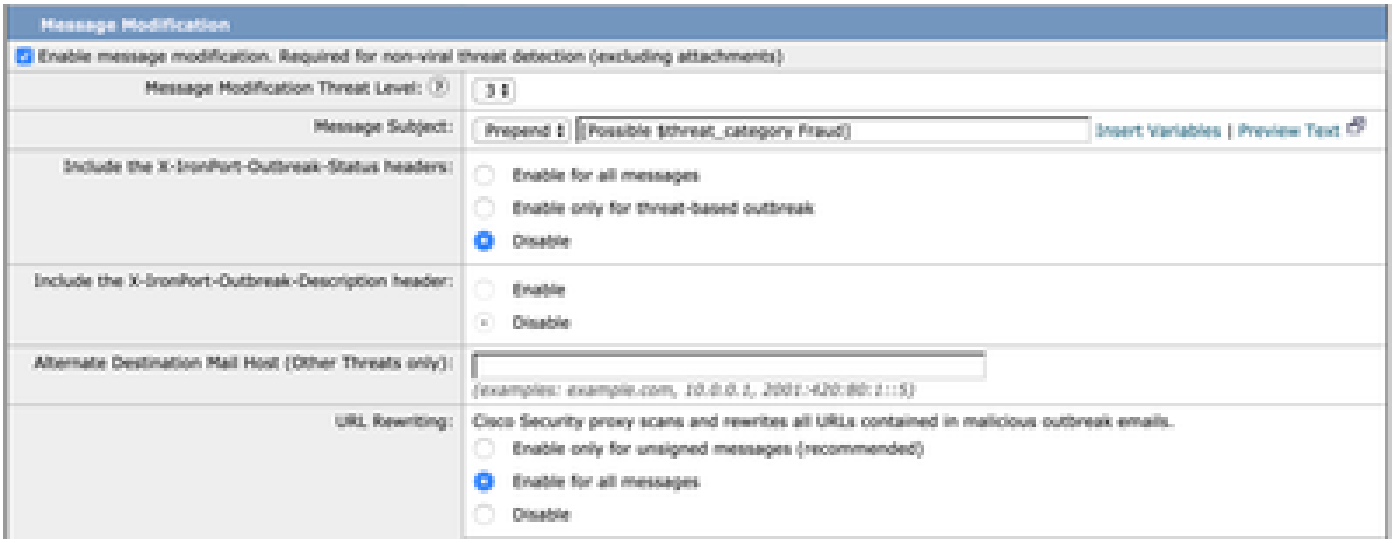
يتم تضمين الحماية من إرتباطات التصيد الاحتيالي في عنوان URL وتصفية التفشي في بريد Cisco الإلكتروني الآمن. تجمع التهديدات المرموزة بين رسائل الانتحال والتصيد الاحتيالي لتبدو أكثر شرعية للهدف. إن تمكين "تصفية" التفشي هو أمر حيوي للمساعدة على اكتشاف مثل هذه التهديدات وتحليلها ووقفها في الوقت الفعلي. تجدر الإشارة إلى أنه يتم تقييم سمعة عنوان URL داخل محرك مكافحة البريد العشوائي، ويمكن إستخدامه كجزء من قرار اكتشاف البريد العشوائي. إذا لم يوقف محرك Anti-Spam الرسالة التي تحتوي على عنوان URL كبريد عشوائي، يتم تقييمها بواسطة URL وتصفية التفشي في الجزء الأخير من تدفق الأمان.

التوصية: قم بإنشاء قاعدة عامل تصفية محتوى تقوم بحظر عنوان URL ذي درجة سمعة سيئة أو بتعديل عنوان URL مع تسجيل سمعة محايد إلى وكيل أمان Cisco (الصورة 12). قم بتمكين "عوامل تصفية تفشي التهديدات" عن طريق تمكين تعديل الرسالة. تتيح إعادة كتابة عنوان URL إمكانية تحليل عناوين URL المريبة بواسطة وكيل أمان Cisco (الصورة 13). لمزيد من المعلومات، قم بزيارة: [تكوين تصفية URL لعبارة البريد الإلكتروني الآمن وبوابة السحابة]

الصورة 12. عامل تصفية المحتوى لسمات URL



الصورة 13. تمكين إعادة كتابة URL في تصفية التفشي



الطبقة 9: إمكانية اكتشاف انتحال الزيادة باستخدام برنامج الدفاع الآمن عن تهديد البريد الإلكتروني من Cisco (ETD)

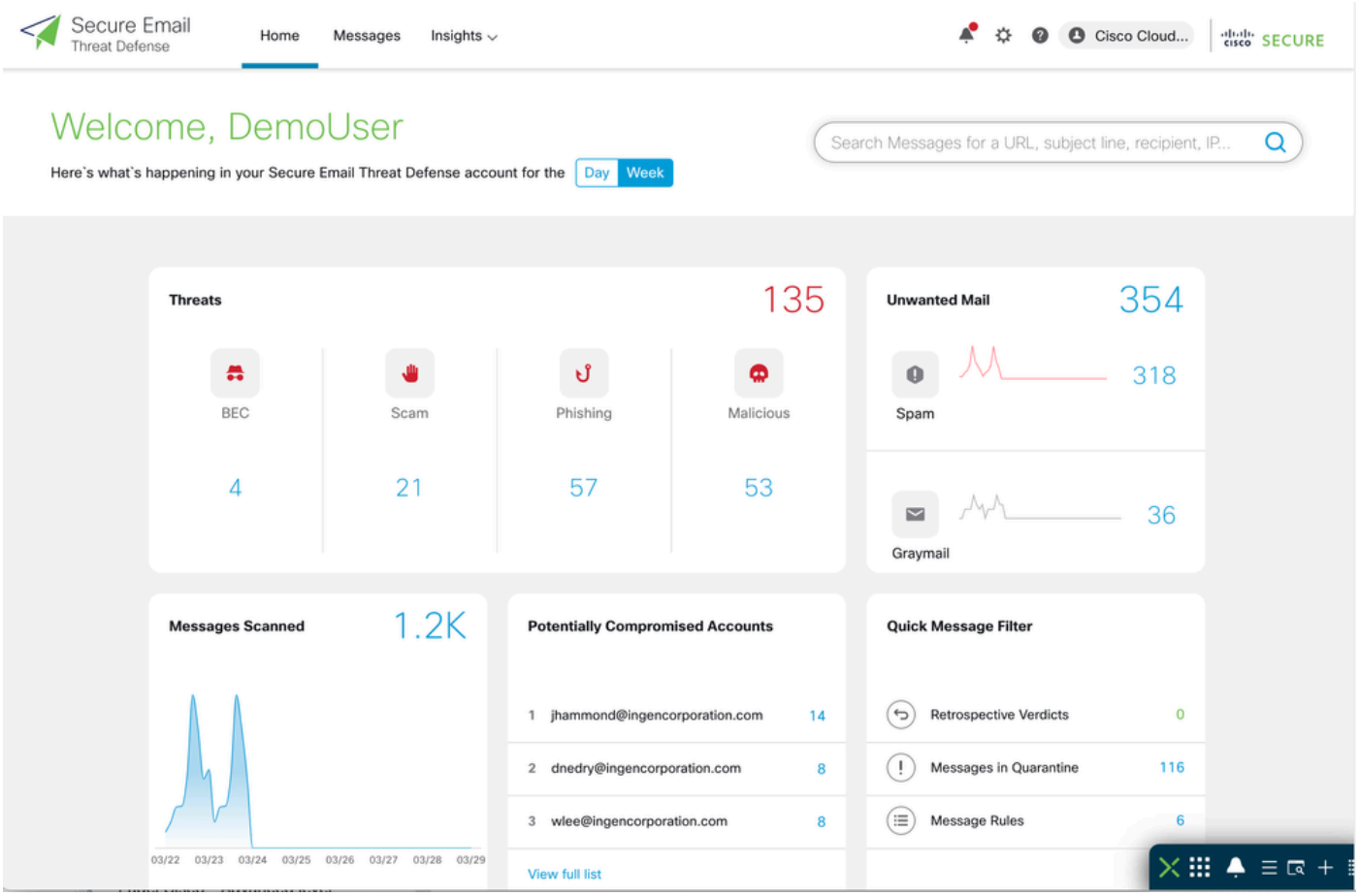
توفر Cisco ميزة الدفاع عن تهديد البريد الإلكتروني، وهي حل أصلي من السحابة يستفيد من ذكاء التهديد الفائق من Cisco Talos. يحتوي على بنية تدعم واجهة برمجة التطبيقات (API) لتوفير أوقات إستجابة أسرع وإمكانية رؤية كاملة للبريد الإلكتروني، بما في ذلك رسائل البريد الإلكتروني الداخلية وعرض محادثة للحصول على معلومات سياقية أفضل وأدوات لمعالجة التهديدات المتربصة في علب بريد Microsoft 365 تلقائياً أو يدوياً. تفضل بزيارة [وقفة بيانات الدفاع عن تهديد البريد الإلكتروني الآمن من Cisco] للحصول على مزيد من التفاصيل.

يعمل "الدفاع الآمن عن تهديد البريد الإلكتروني من Cisco" على مكافحة التصيد الاحتيالي باستخدام إمكانات مصادقة المرسل وكشف BEC. ويجمع هذا النظام بين التعلم الآلي

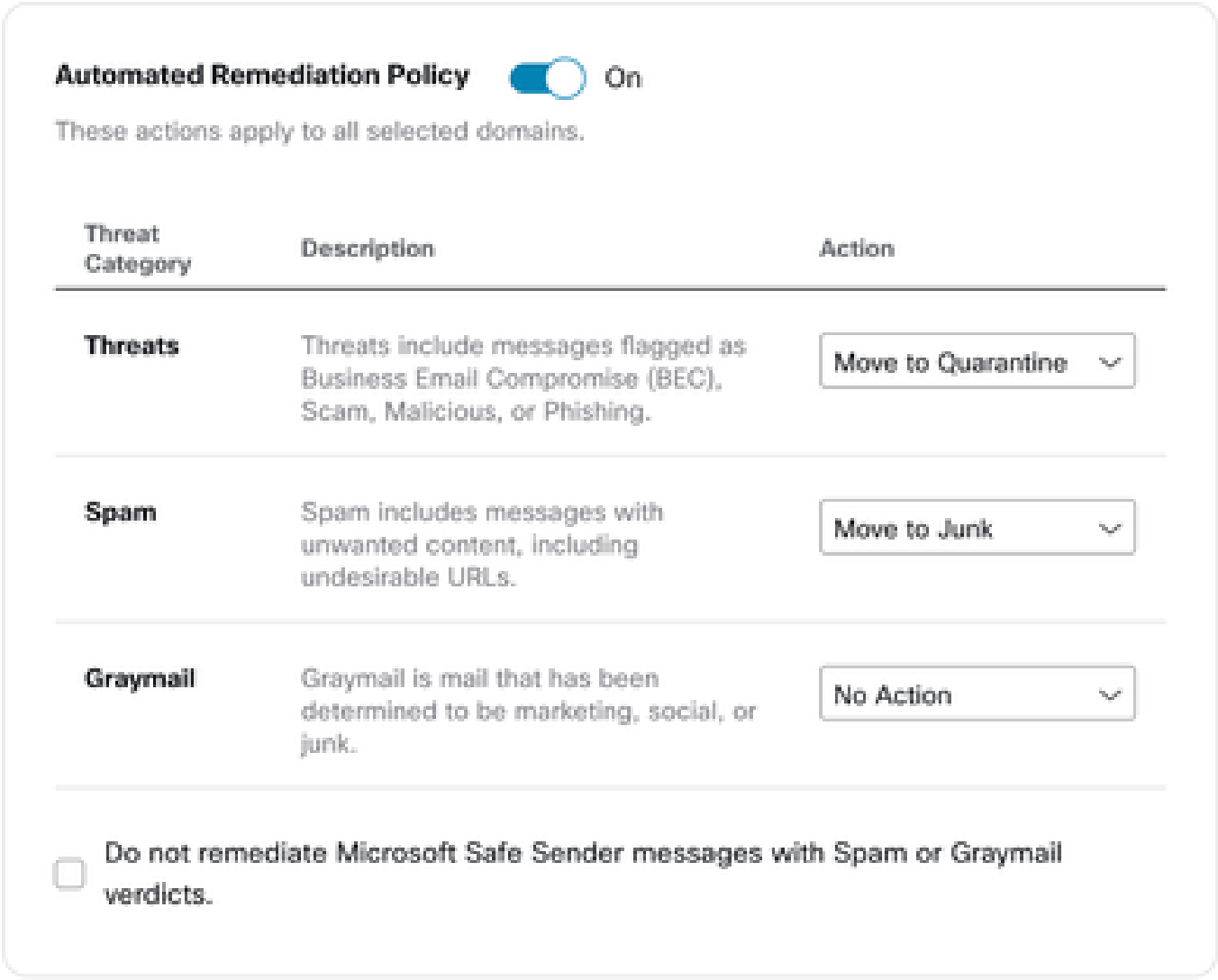
ومحركات الذكاء الاصطناعي التي تجمع بين نمذجة الهوية المحلية والعلاقة مع تحليلات للسلوك في الوقت الحقيقي للحماية من التهديدات القائمة على خداع الهوية. إنها تنمذج لسلوك البريد الإلكتروني الموثوق به داخل المؤسسات وبين الأفراد. يوفر برنامج الدفاع ضد تهديدات البريد الإلكتروني، من بين ميزات رئيسية أخرى، هذه الفوائد:

- قم بكشف التهديدات المعروفة والناشئة والمستهدفة مع قدرات اكتشاف التهديدات المتقدمة.
- حدد التقنيات الضارة واكسب السياق للمخاطر التجارية المحددة.
- البحث السريع عن التهديدات الخطيرة ومعالجتها في الوقت الفعلي.
- إستخدم ميزة تتبع التهديدات القابلة للبحث لتصنيف التهديدات ومعرفة أي أجزاء من مؤسستك هي الأكثر عرضة للهجوم.

شكل 14. يوفر برنامج الدفاع الآمن ضد تهديدات البريد الإلكتروني من Cisco معلومات حول كيفية إستهداف مؤسستك.



الصورة 15. يحدد إعداد نهج الدفاع عن تهديد البريد الإلكتروني من Cisco تلقائيا ما إذا كانت الرسالة تطابق فئة التهديد المحددة



ماذا يمكنك أن تفعل أكثر مع منع الانتحال

يمكن إصلاح العديد من الانتحال مع بعض الاحتياطات البسيطة التي تشمل، ولكن لا تقتصر على، ما يلي:

- الحد المسموح به للمجالات المدرجة في جدول الوصول إلى المضيف (HAT) لعدد قليل جدا من شركاء الأعمال الأساسيين.
- تتبع الأعضاء في مجموعة المرسلين SPOOF_ALLOW وتحديثهم باستمرار إذا قمت بإنشاء واحد واستخدام التعليمات الواردة في إرتباط أفضل الممارسات.
- قم بتمكين الكشف عن بريد الجريب ووضعه في العزل العشوائي أيضا.

ولكن الأمر الأكثر أهمية على الإطلاق هو تمكين الصندوق الشعبي الخاص، والصندوق الشعبي للتعامل مع الكوارث، ومبادرة إدارة الكوارث، وتنفيذ هذه الخطط على النحو اللائق. ومع ذلك، فإن الإرشادات المتعلقة بنشر سجلات SPF و DKIM و DMARK تتجاوز نطاق هذا المستند. لذلك، ارجع إلى هذا التقرير: [أفضل ممارسات مصادقة البريد الإلكتروني: أفضل الطرق لنشر SPF و DKIM و DMARK](#).

تعرف على التحدي المتمثل في معالجة هجمات البريد الإلكتروني مثل حملات الانتحال التي تمت مناقشتها هنا. إذا كانت لديك أسئلة حول تنفيذ أفضل الممارسات هذه، فاتصل

بالدعم الفني من Cisco وافتح حالة. بدلا من ذلك، اتصل بفريق حساب Cisco للحصول على حل وإرشادات التصميم. للحصول على مزيد من المعلومات حول بريد Cisco الإلكتروني الآمن، ارجع إلى موقع بريد Cisco الإلكتروني الآمن على الويب.

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).