Création d'une stratégie de Whitelist sur Cisco ESA pour des tests de formation de phishing

Contenu

Introduction

Ce document décrit comment créer une stratégie de Whitelist sur l'appliance de sécurité du courrier électronique de Cisco (ESA) ou opacifier l'exemple de sécurité du courrier électronique (CES) pour permettre des tests/campagnes de formation de phishing.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Naviguant et configurant des règles sur Cisco ESA/CES sur le WebUI.
- La création du message filtre sur Cisco ESA/CES sur l'interface de ligne de commande (CLI).
- La connaissance de la ressource utilisée pour la campagne/test de phishing.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les administrateurs exécutant des tests ou des campagnes de formation de phishing auront des emails générés avec les informations qui seront appariées contre les règles en cours de Talos sur les positionnements de règle de filtrage d'anti-Spam et/ou d'épidémie. Dans un tel événement, les emails de campagne de phishing n'atteindront pas des utilisateurs finaux et actioned par Cisco ESA/CES lui-même entraînant de ce fait le test à une interruption. Les administrateurs devraient s'assurer que l'ESA/CES autorise par ces emails à effectuer leur campagne/test.

Configurer

Avertissement : On ne permet pas la position de Cisco sur les constructeurs whitelisting de simulation et de formation de phishing globalement. Nous informons des administrateurs travailler avec le service de simulateur de phishing *(par exemple : PhishMe)* pour obtenir leur IPS les ajoutent alors localement au Whitelist. Cisco doit protéger nos clients ESA/CES contre IPS s'ils changent jamais des mains ou deviennent réellement une menace.

Attention : Les administrateurs devraient seulement maintenir ces IPS dans un Whitelist tout en testant, laisser l'IPS externe sur un Whitelist pour un test de courrier de longue période peut apporter non sollicité ou les emails malveillants aux utilisateurs finaux ces IPS deviennent compromis.

Sur l'appliance de sécurité du courrier électronique de Cisco (ESA), créez un nouveau groupe d'expéditeur pour votre simulation de phishing et assignez-le à la stratégie de flux de courrier $TRUSTED. Ceci permettra tous les emails de simulation de phishing à livrer aux utilisateurs. Les membres de ce nouveau groupe d'expéditeur ne sont pas sujets à la limitation de débit, et le contenu de ces expéditeurs n'est pas balayé par l'engine d'anti-Spam d'IronPort Cisco, mais est toujours balayé par le logiciel antivirus.

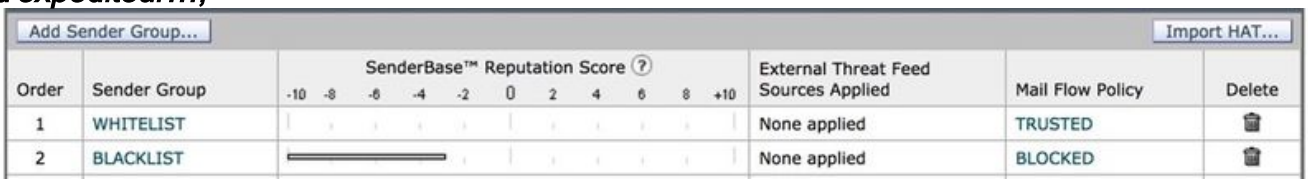
Remarque: Par défaut, la stratégie de flux de courrier $TRUSTED a l'antivirus activé mais l'anti-Spam arrêté.

Création du groupe d'expéditeur

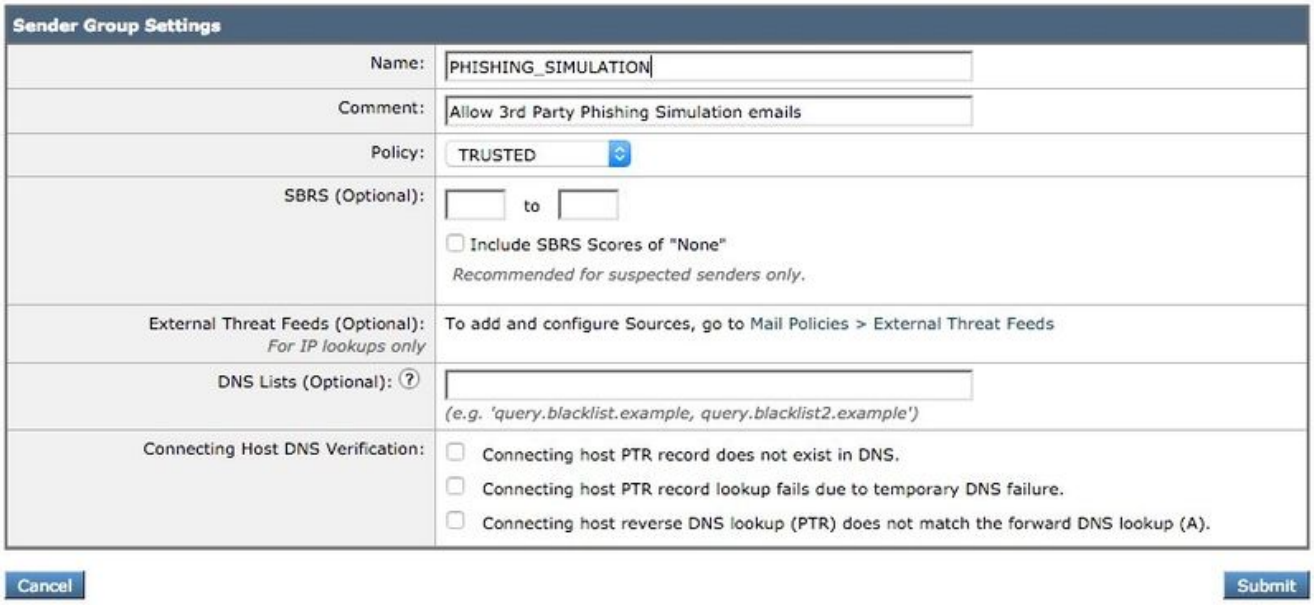
1. Cliquez sur l'onglet de ***stratégies de messagerie***.
2. Sous la section de ***Tableau d'accès au hôte***, ***vue d'ensemble*** choisie de ***CHAPEAU***

3. Du côté droit, assurez-vous que votre auditeur d'***InboundMail*** est actuellement sélectionné,
4. De la colonne de ***groupe d'expéditeur*** ci-dessous, cliquez sur Add le ***groupe***

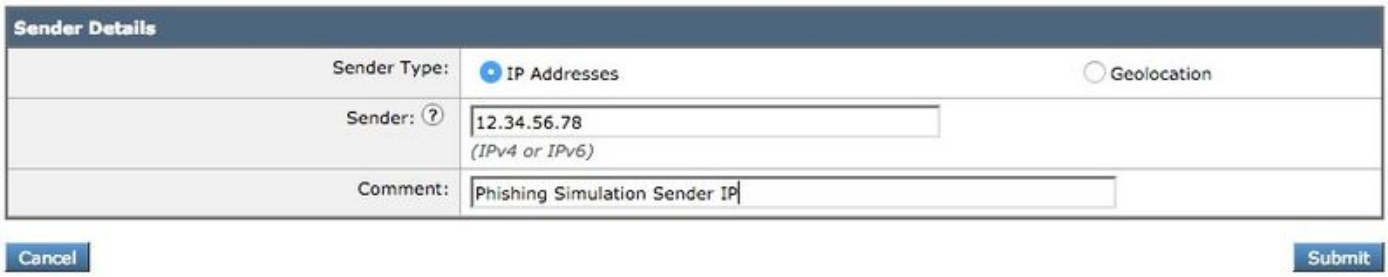
d'expéditeur…,



5. Complétez les champs de ***nom*** et de ***commentaire***. Dans le cadre de la ***stratégie*** déroulante, « **$TRUSTED** » choisis et alors cliquent sur Submit ***et ajoutent des expéditeurs >>.***



6. Entrez dans l'IP ou l'adresse Internet que vous voulez à Whitelist dans le premier domaine. Votre partenaire de simulation de phishing te fournira les informations IP d'expéditeur.



Quand vous finissez d'ajouter des entrées, cliquez sur le bouton de ***soumission***. Souvenez-vous pour cliquer sur les ***modifications de validation*** se boutonnent pour sauvegarder vos modifications.

Création du filtre de message

Après création du groupe d'expéditeur pour permettre le contournement de l'anti-Spam et de l'antivirus, un filtre de message est exigé pour ignorer les autres engines de Sécurité qui peuvent apparier la campagne/test de phishing.

1. Connectez au CLI de l'ESA.
2. Exécutez les ***filtres de*** commande.
3. Exécutez la commande ***nouvelle*** pour créer un nouveau filtre de message.

4. Copiez et collez l'exemple suivant de filtre, faisant édite pour vos noms de groupe réels d'expéditeur si nécessaire :

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

5. Revenez à la demande principale CLI et appuyez sur entrent.
6. Exécutez la *validation* pour sauvegarder la configuration.

Vérifiez

Employez la tiers ressource pour envoyer une campagne/test de phishing et vérifier les résultats sur le message dépistant des logs pour assurer toutes les engines ont été ignorés et l'email a été fourni.