Configurer l'appliance de sécurisation de la messagerie pour autoriser les campagnes d'hameçonnage simulées

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Informations générales](#)

[Motif](#)

[Solution](#)

- [AsyncOS 13.x et versions antérieures](#)

Introduction

Ce document décrit comment configurer l'appliance de sécurité de la messagerie (ESA) pour permettre aux campagnes simulées de plate-forme d'hameçonnage de réussir.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Création de filtres de messages et de contenu sur l'appliance de sécurité de la messagerie Cisco (ESA).
- Configuration de la table d'accès aux hôtes (HAT).
- Compréhension du réseau de messagerie entrant Cisco ESA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les plates-formes d'hameçonnage simulées permettent aux administrateurs d'exécuter des campagnes d'hameçonnage pour tester la sécurité.

Motif

Lorsque Cisco ESA n'est pas configuré pour faire confiance aux hôtes de la plate-forme d'hameçonnage simulée, l'analyse de sécurité et les contrôles de stratégie peuvent arrêter les messages de campagne. Ce comportement peut entraîner l'échec de la campagne ou réduire l'efficacité de la simulation.

Solution

⚠ Mise en garde : Dans cet exemple de configuration, la stratégie de flux de messages TRUSTED est sélectionnée pour permettre à Cisco ESA de passer par des campagnes d'hameçonnage simulées plus importantes sans limitation. L'exécution de campagnes d'hameçonnage en continu à fort volume peut affecter les performances du traitement des e-mails.

Afin de s'assurer que Cisco ESA n'arrête pas les messages de campagne, configurez un groupe d'expéditeurs dédié et contournez l'analyse pour les hôtes de la plate-forme.

1. Accédez à GUI > Mail Policies > HAT Overview.

2. Créez un nouveau groupe d'expéditeurs et liez-le à la stratégie de flux de messagerie TRUSTED. Vous pouvez également créer une nouvelle stratégie avec des options similaires sous GUI > Mail Policies > Mail Flow Policies.

3. Ajoutez les hôtes émetteurs ou les adresses IP de la plate-forme d’hameçonnage simulée à ce groupe d’expéditeurs. Si la plate-forme d’hameçonnage simulée utilise une plage d’adresses IP étendue, ajoutez des noms d’hôtes partiels ou des plages IP, le cas échéant.

4. Classez le groupe d'expéditeurs précédant votre groupe d'expéditeurs BLOCKLIST pour vous assurer qu'il est mis en correspondance de manière statique plutôt que SBRS.

5. Accédez à GUI > Mail Policies > Mail Flow Policies > TRUSTED, ou à la nouvelle stratégie de flux de messages.

6. Désactivez toutes les fonctionnalités de sécurité pour cette stratégie approuvée, comme indiqué dans la capture d'écran.

Security Features	
Spam Detection:	○ Use Default (On) ○ On ◉ Off
AMP Detection	○ Use Default (On) ○ On ◉ Off
Virus Protection:	○ Use Default (On) ○ On ◉ Off
Sender Domain Reputation Verification:	○ Use Default (On) ○ On ◉ Off
Virus Outbreak Filters:	○ Use Default (On) ○ On ◉ Off
Advanced Phishing Protection:	○ Use Default (On) ○ On ◉ Off
Graymail Detection:	○ Use Default (On) ○ On ◉ Off
Content Filters:	○ Use Default (On) ○ On ◉ Off
Message Filters:	○ Use Default (On) ○ On ◉ Off

6. Envoyez les modifications et validez la configuration.

AsyncOS 13.x et versions antérieures

⚠ Mise en garde : Dans cet exemple de configuration, la stratégie de flux de messages TRUSTED est sélectionnée pour permettre à Cisco ESA de passer par des campagnes d'hameçonnage simulées plus importantes sans limitation. L'exécution de campagnes d'hameçonnage en continu à fort volume peut affecter les performances du traitement des e-mails.

Pour s'assurer que les messages de la campagne d'hameçonnage ne sont pas bloqués par un composant de sécurité de Cisco ESA, la configuration doit être mise en place.

1. Accédez à GUI > Mail Policies > HAT Overview.

2. Créez un nouveau groupe d'expéditeurs et liez-le à la stratégie de flux de messagerie TRUSTED.

3. Ajoutez le ou les hôtes émetteurs ou les adresses IP de la plate-forme d’hameçonnage simulée à ce groupe d’expéditeurs. Si la plate-forme d’hameçonnage simulée comporte une large plage d’adresses IP, vous pouvez ajouter des noms d’hôtes partiels ou des plages d’adresses IP, le cas échéant.

4. Classez le groupe d'expéditeurs précédant le groupe d'expéditeurs BLOCKLIST pour vous assurer qu'il correspond de manière statique plutôt qu'en BS.

5. Soumettre et valider ces modifications,

6. Accédez à l'interface de ligne de commande (CLI).

7. Exécutez des filtres.

8. Créez un nouveau filtre de messages. Copiez la syntaxe, modifiez-la pour l'environnement et ajoutez le filtre.

```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```

9. Classez le filtre de message dans la liste pour vous assurer qu'il n'est pas ignoré par un autre filtre de message qui inclut l'action skip-filters.

10. Appuyez sur Entrée pour revenir à l’invite de commandes principale d’AsyncOS.

11. Exécutez commit pour enregistrer les modifications.

12. N'appuyez pas sur Ctrl+C. Il efface les modifications.

13. Accédez à GUI > Mail Policies > Incoming Content Filters.

14. Créez un nouveau filtre de contenu entrant.

15. Définissez la condition sur Autre en-tête.

16. Configurez le filtre pour rechercher l'en-tête personnalisé x-sp et la valeur unique configurée dans le filtre de message.

17. Définissez l'action sur Ignorer les filtres de contenu restants (action finale).

18. Attribuez la valeur 1 au filtre de contenu pour vous assurer que les autres filtres n’agissent pas contre le message d’hameçonnage simulé.

19. Accédez à GUI > Mail Policies > Incoming Mail Policies.

20. Affectez le filtre de contenu à la stratégie requise.

21. Soumettre et valider les modifications.

22. Lancez la campagne de simulation de plate-forme d’hameçonnage.

23. Surveillez les journaux de messages ou le suivi des messages pour vérifier la correspondance entre le flux de messages et la règle de stratégie.

24. Résultat escompté : Cisco ESA accepte les messages de campagne, établit une correspondance avec le groupe d'expéditeurs et les filtres configurés, et ignore les actions d'analyse configurées pour la stratégie approuvée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.