Creazione di una policy di lista bianca su un Cisco ESA per i test di formazione sul phishing

Sommario

Introduzione

Questo documento descrive come creare una policy Whitelist sull'istanza Cisco Email Security Appliance (ESA) o Cloud Email Security (CES) per consentire test/campagne di formazione sul phishing.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Navigazione e configurazione delle regole su Cisco ESA/CES su WebUI.
- Creazione di filtri messaggi su Cisco ESA/CES sull'interfaccia della riga di comando (CLI).
- Conoscenza della risorsa utilizzata per la campagna/il test di phishing.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Gli amministratori che eseguono test o campagne di formazione sul phishing riceveranno e-mail generate con informazioni che verranno confrontate con le regole Talos correnti sui set di regole Antispam ed Epidemie. In tal caso, i messaggi di posta elettronica della campagna di phishing non raggiungeranno gli utenti finali e saranno gestiti dall'ESA/CES Cisco stessa, causando l'interruzione del test. Gli amministratori dovrebbero garantire che l'ESA/CES consenta, attraverso queste e-mail, di effettuare la loro campagna/test.

Configurazione

Avviso: La posizione di Cisco sui fornitori globali di simulazioni di phishing e istruzione non è consentita. Si consiglia agli amministratori di utilizzare il servizio di simulatore di phishing *(ad esempio: PhishMe)* per ottenere i loro IP, quindi aggiungerli localmente alla Whitelist. Cisco deve proteggere i nostri clienti ESA/CES da questi IP se dovessero passare di mano o diventare una minaccia.

Attenzione: Gli amministratori devono solo mantenere questi IP in una Whitelist durante il test, lasciando gli IP esterni su una Whitelist per un periodo di tempo prolungato dopo il test può portare e-mail indesiderate o dannose agli utenti finali se questi IP vengono compromessi.

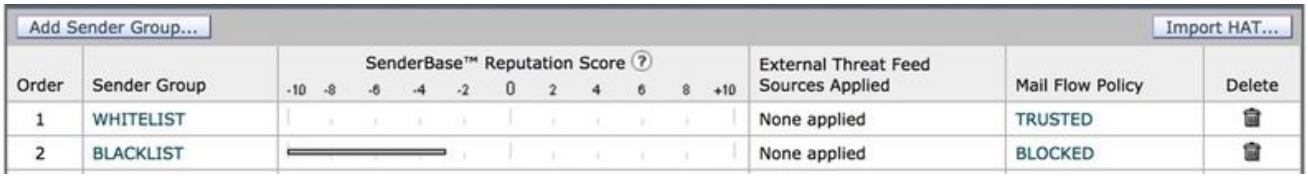
Su Cisco Email Security Appliance (ESA), creare un nuovo gruppo di mittenti per la simulazione di phishing e assegnarlo al criterio del flusso di posta $TRUSTED. In questo modo, tutti i messaggi di simulazione di phishing verranno recapitati agli utenti finali. I membri di questo nuovo gruppo di mittenti non sono soggetti a limitazioni di velocità e il contenuto di tali mittenti non viene analizzato da Cisco IronPort Anti-Spam Engine, ma viene comunque analizzato da software antivirus.

Nota: Per impostazione predefinita, nel criterio del flusso di posta $TRUSTED è abilitato l'antivirus ma l'antivirus è disattivato.

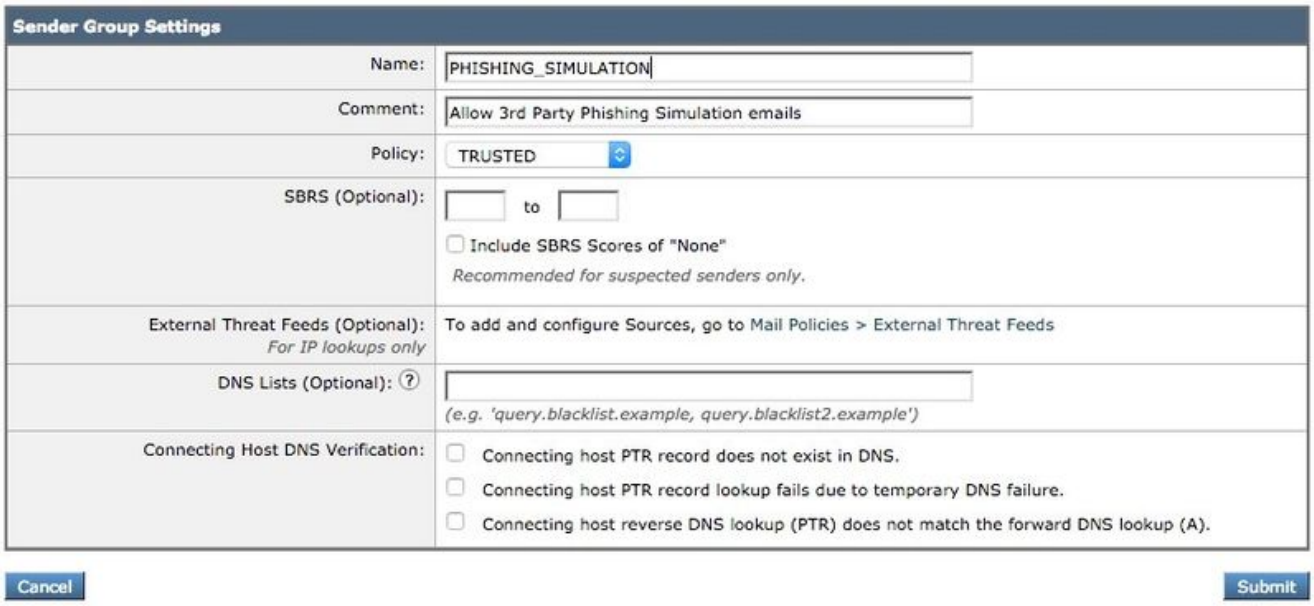
Creazione del gruppo di mittenti

1. Fare clic sulla scheda *Criteri di posta*.
2. Nella sezione *Tabella di accesso host*, selezionare *Panoramica HAT*

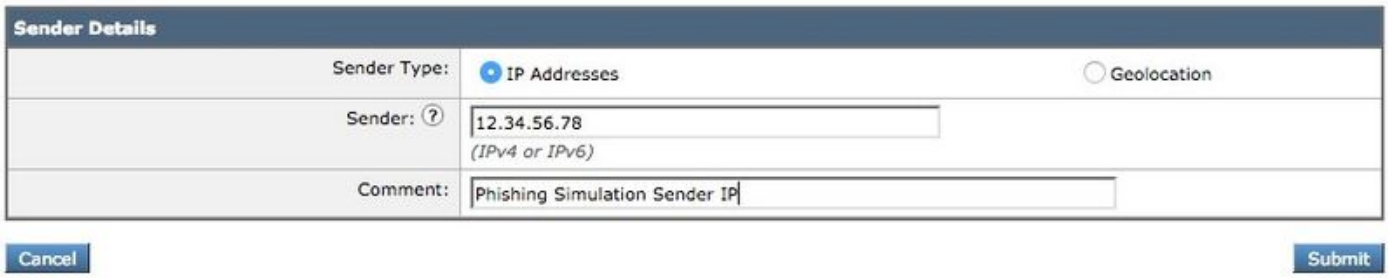
3. A destra, assicurarsi che il listener *InboundMail* sia selezionato.
4. Dalla colonna *Gruppo mittenti* seguente, fare clic su *Aggiungi gruppo mittenti...,*



5. Compilare i campi ***Name*** e ***Comment***. Nell'elenco a discesa ***Criterio***, selezionare '**$TRUSTED**' e fare clic su ***Submit and Add Senders >>***.



6. Immettere l'indirizzo IP o il nome host che si desidera inserire nella lista bianca nel primo campo. Il partner per la simulazione di phishing fornirà le informazioni sull'indirizzo IP del mittente.



Dopo aver aggiunto le voci, fare clic sul pulsante ***Invia***. Ricordarsi di fare clic sul pulsante ***Commit modifiche*** per salvare le modifiche.

Creazione del filtro messaggi

Dopo aver creato il gruppo di mittenti per consentire il bypass di antispam e antivirus, è necessario un filtro messaggi per ignorare gli altri motori di sicurezza che potrebbero corrispondere alla campagna/test di phishing.

1. Connettersi alla CLI dell'ESA.
2. Eseguire i ***filtri*** dei comandi.
3. Eseguire il comando ***new*** per creare un nuovo filtro messaggi.
4. Copiare e incollare il seguente esempio di filtro, apportando le modifiche necessarie per i

nomi effettivi del gruppo di mittenti:

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

5. Tornare al prompt della CLI principale e premere Invio.
6. Eseguire il comando ***commit*** per salvare la configurazione.

Verifica

Utilizzare la risorsa di terze parti per inviare una campagna/test di phishing e verificare i risultati nei log di verifica dei messaggi per assicurarsi che tutti i motori siano stati ignorati e che l'e-mail sia stata recapitata.