Configurazione della reputazione del dominio mittente per l'aggiornamento ESA in corso Apr 2024

Sommario

Introduzione

In questo documento viene descritta la configurazione della reputazione del dominio mittente (SDR) per Email Security Appliance (ESA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Concetti relativi al SEC
- Configurazione ESA

- Conoscenze generali delle funzioni/caratteristiche dei SEG, tra cui: Criteri di flusso della posta, filtri messaggi, filtri contenuti, reputazione del dominio globale.

Componenti usati

Le informazioni di questo documento si basano su AsyncOS per ESA 14.2 e versioni successive.

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.

Panoramica

1. L'SDR è stato sviluppato come servizio aggiuntivo per migliorare il rilevamento di spam phishing.

2. SDR acquisisce più valori di intestazione e li carica nei Talos Threat Intelligence Server dove le vaste risorse Talos determinano un verdetto per ogni messaggio su scala graduata.

3. I valori di intestazione inclusi nella decisione sono:

- Busta - Da
- Da
- Rispondi a
- Verifica DMAR, DKIM e SPF (se configurata).
- Il valore (username) dell'indirizzo e-mail viene inviato facoltativamente dalle intestazioni Da, Busta - Da e Risposta - A
- IP mittente
- Nome visualizzato nelle intestazioni Da e Risposta.

5. SDR Scan viene eseguito su tutti i messaggi in ingresso.

6. L'analisi SDR viene eseguita subito dopo l'accettazione di un messaggio da parte del protocollo SMTP (Simple Mail Transfer Protocol).

7. L'azione SDR può essere eseguita nella fase iniziale di Mail Flow Policy, così come le opzioni Filtro messaggi o Filtro contenuti.

8. I componenti configurati includono:

- Abilita Domain Reputation Service
- Elenchi di eccezioni di dominio (facoltativo)
    - Elenco eccezioni dominio (globale)
    - Elenco di eccezioni del dominio che utilizza il filtro messaggi/contenuti specifico.
    - Azione globale con ripristino del dominio tramite i criteri di flusso della posta.
    - Azione globale con reputazione del dominio che esegue azioni a livello di conversazione SMTP.
- Filtro messaggi o Filtro contenuti

Configurazione

Abilita WebUI servizio reputazione dominio

SDR può essere abilitato sia dall'interfaccia WebUI sia dall'interfaccia CLI.

Interfaccia Web:

1. Passare a Servizi di sicurezza della posta > Reputazione dominio > Abilita.

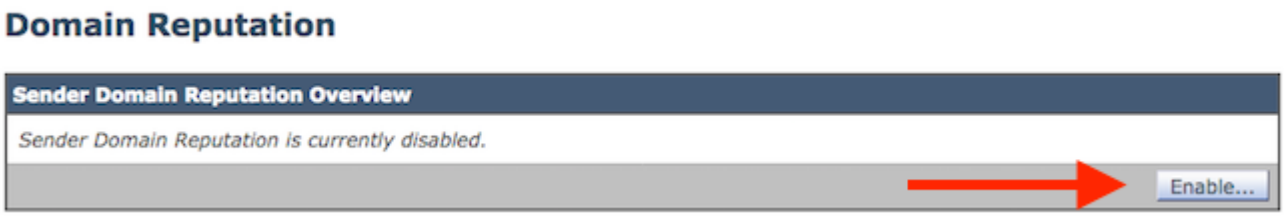
2. Fare clic sulla casella accanto a Abilita filtro reputazione dominio mittente.

3. Scegliere questa casella Includi attributi aggiuntivi: (facoltativo) se si desidera includere il valore dell'intestazione facoltativa nei dati selezionati per una maggiore efficacia. Fare clic su ? per imparare.

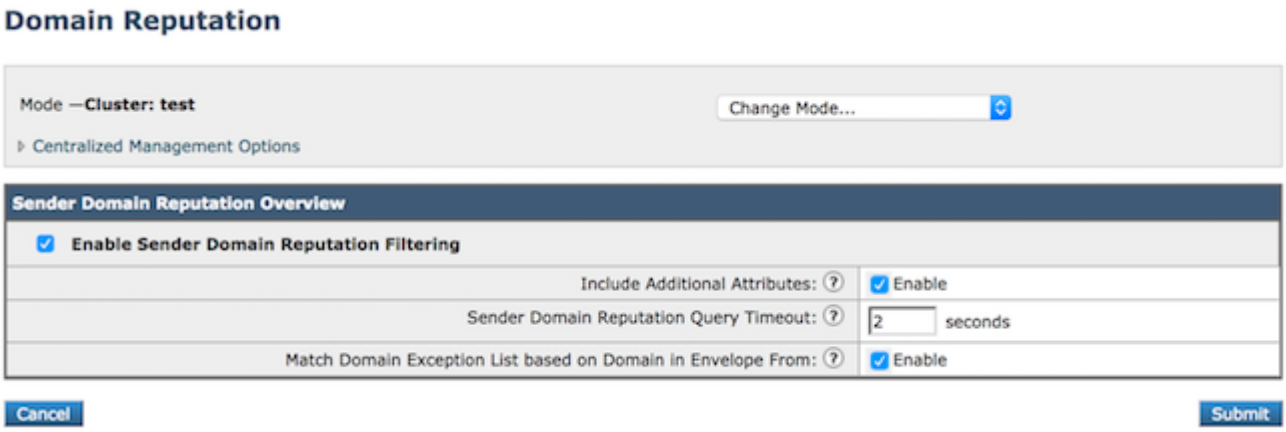
4. Scegliere questa casella Timeout query reputazione dominio mittente. Fare clic su ? per imparare.

5. Scegliere Corrispondenza elenco eccezioni dominio in base al dominio nella busta Da - Abilitato.

6. Fare clic su Sottometti > Conferma come mostrato nell'immagine.



Servizio mittente (reputazione dominio)



Servizi di sicurezza > Reputazione del dominio

Elenco eccezioni dominio

1. L'elenco delle eccezioni del dominio può ignorare l'analisi della reputazione del dominio del mittente per rilevare il flusso di posta in ingresso.

2. L'elenco delle eccezioni del dominio può essere applicato in posizioni diverse per influire sul flusso di posta.

3. L'applicazione Globale può essere applicata a tutti i messaggi scansionati.

4. L'applicazione più dettagliata dei filtri contenuti/messaggi può influire solo sui filtri configurati.

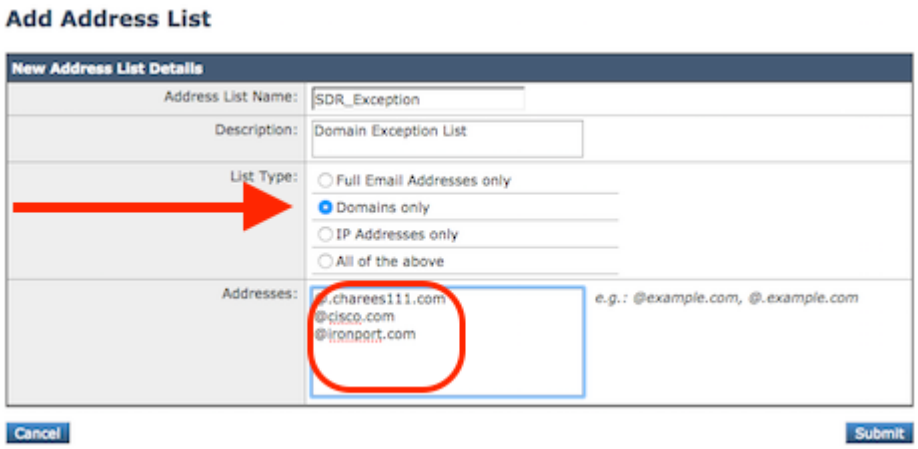
5. L'elenco delle eccezioni dei domini offre due opzioni per fornire un'opzione semplice e una più sicura.

6. In questo documento vengono descritte le opzioni per ignorare correttamente l'SDR per un messaggio che utilizza l'elenco delle eccezioni del dominio.

7. Spiegazione dei requisiti dell'elenco delle eccezioni dei domini

Creazione di un elenco indirizzi

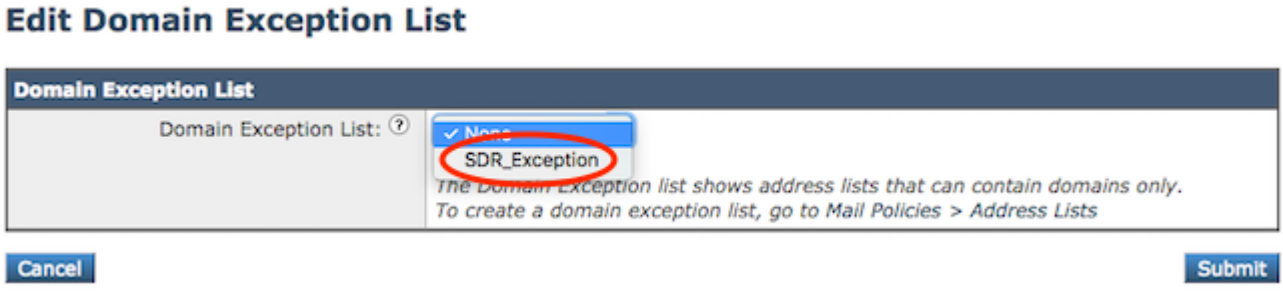
1. Selezionare Mail Policies > Address List > Add Address List > Name > Description > List Type: (Policy di posta > Elenco indirizzi > Aggiungi elenco indirizzi > Nome > Descrizione > Tipo elenco). Solo domini.
2. Aggiungere ogni nome di dominio utilizzando la virgola come separatore.
3. Fare clic su Submit (Invia) e su Commit delle modifiche, come mostrato nell'immagine.



Elenco indirizzi da applicare all'elenco eccezioni del dominio

Applica l'elenco indirizzi all'elenco eccezioni del dominio globale SDR

1. Passare a Servizi di sicurezza > Reputazione dominio > Elenco eccezioni dominio > Modifica impostazioni > Elenco eccezioni dominio (selezionare l'elenco).
2. Fare clic su Submit (Invia) e su Commit delle modifiche, come mostrato nell'immagine.



Selezionare un elenco di indirizzi dall'elenco a discesa

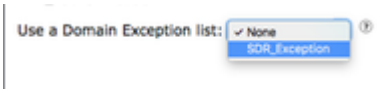
Applicazione dell'elenco indirizzi ai filtri contenuti/messaggi

Filtri contenuti in arrivo:

1. Passare a Condizione > Reputazione URL > Opzione feed minacce.

2. Reputazione dominio condizione.

3. Fare clic qui:



L'elenco delle eccezioni di dominio consente per azione di criterio.

Filtri messaggi

L'applicazione Elenco eccezioni dominio all'interno dei filtri messaggi viene inclusa come opzione in una condizione.

Nota: Questi esempi includono domain_exception_list come parte dell'intera condizione.

---

1. sdr-reputation (['awful', 'poor', 'contaminato', 'weak', 'known', 'neutral', 'good'], domain_exception_list)
2. sdr-age ("giorni", <, 5, domain_exception_list)
3. sdr-unscannable (elenco_eccezioni_dominio)

Una spiegazione più esauriente ed esempi dell'applicazione del filtro Message sono reperibili nelle Guide per l'utente ESA sotto i titoli:

- Regola di reputazione del dominio per ETF
- Filtro dei messaggi in base alla reputazione del dominio del mittente che utilizza il filtro messaggi

Creazione di un filtro contenuti per intervenire sul verdetto dell'SDR

1. SDR è abilitato solo per il flusso della posta in arrivo.
2. Nome della condizione SDR: Reputazione del dominio.
3. È possibile creare più condizioni per combinare risultati diversi.
4. La condizione relativa alla reputazione del dominio contiene due diversi controlli contenenti più opzioni per ciascuno di essi:

- Reputazione dominio mittente
    - Verdetto reputazione dominio mittente
    - Età dominio mittente
    - Reputazione dominio mittente non analizzabile
- Feed di minacce esterne
    - Consente di utilizzare gli elenchi di contenuti scaricati dei feed di minacce per eseguire la scansione in base alle stesse intestazioni di dominio raccolte per SDR.

✎ Nota: Queste opzioni all'interno della condizione Domain Reputation possono cambiare visivamente in base alle diverse opzioni per ogni selezione.

---

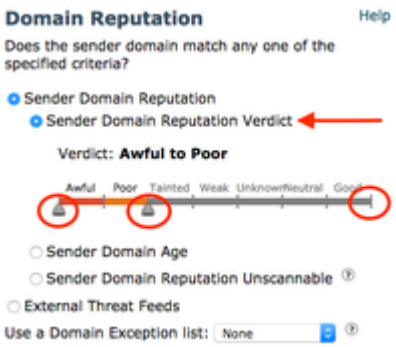
5. L'opzione finale nella condizione della reputazione del dominio è l'elenco delle eccezioni del dominio.

6. La funzione Elenco eccezioni dominio associata a un elenco indirizzi aggiunge un maggiore controllo all'applicazione dell'azione, applicando l'elenco al livello più dettagliato dei criteri di posta per l'elaborazione dei messaggi.

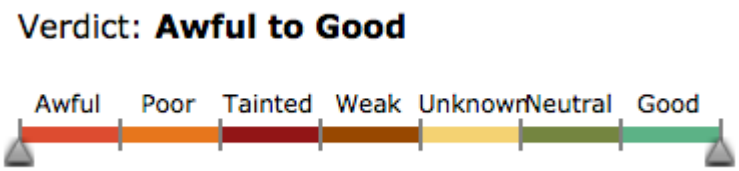
7. Selezionare Mail Policy > Incoming Content Filters > Add Filter > Add Condition > Domain Reputation (Policy di posta > Filtri contenuti in arrivo > Aggiungi filtro > Aggiungi condizione > Reputazione dominio).

8. Condizione 1: Verdetto reputazione dominio mittente.

- Terribile, Povero, Contaminato, Debole, Sconosciuto, Neutro, Buono
- Contiene marcatori triangolari scorrevoli per scegliere l'intervallo da abbinare.
- Awful e Poor sono i valori consigliati per l'azione da eseguire.
- I messaggi che corrispondono a Awful e Poor possono avere una categoria aggiuntiva, ad esempio Spam o Malicious visualizzabile in Message Tracking.



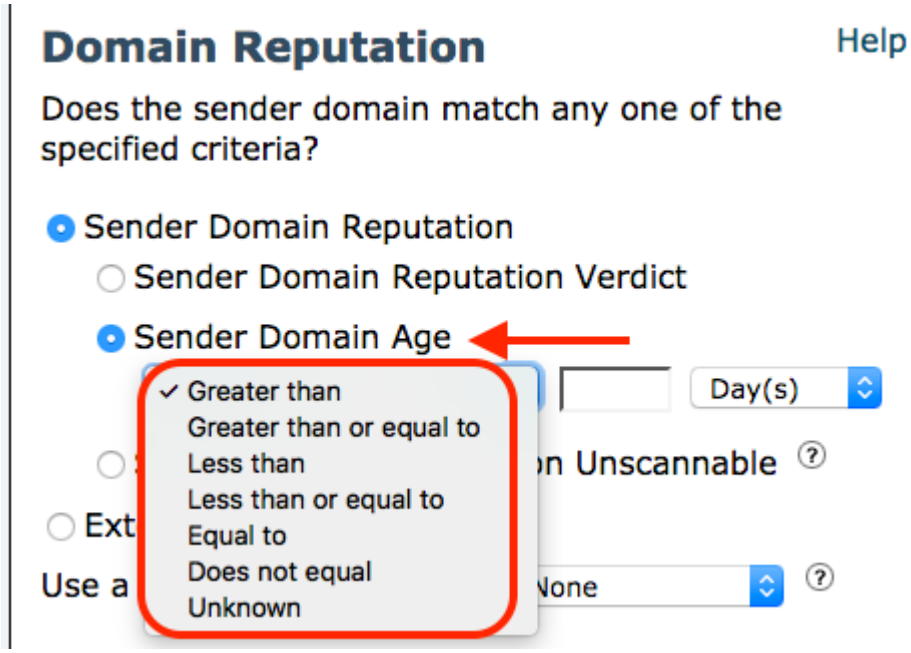
Barra scorrevole intervallo regolabile verdetto SDR.



Visualizzazione completa della barra di scorrimento del verdetto SDR.

9. Condizione 2: Età dominio mittente.

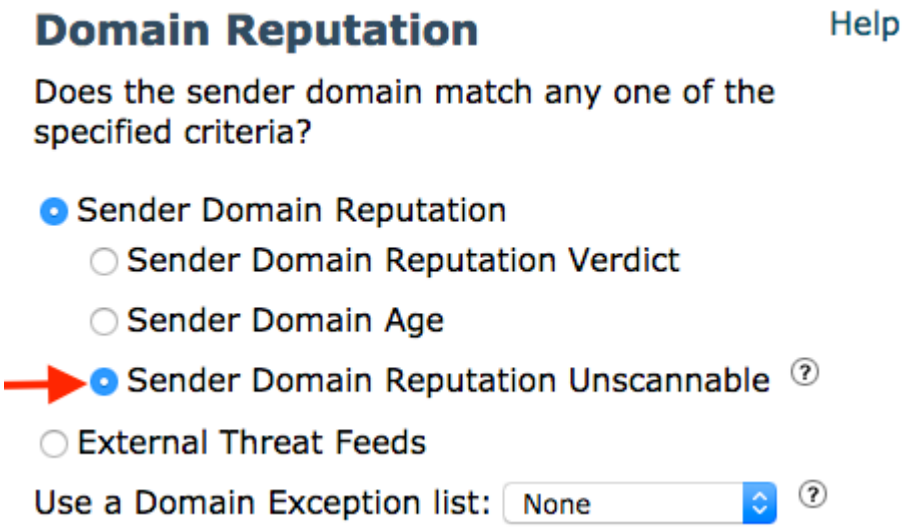
- L'età del Dominio può essere associata a rischi maggiori o a un'affidabilità consolidata.
- La possibilità di un dominio con meno di 10 giorni di età può essere più rischiosa.



Età dominio mittente. Valori bassi suggeriscono maggiori rischi.

10. Condizione 3: Impossibile analizzare la reputazione del dominio mittente.

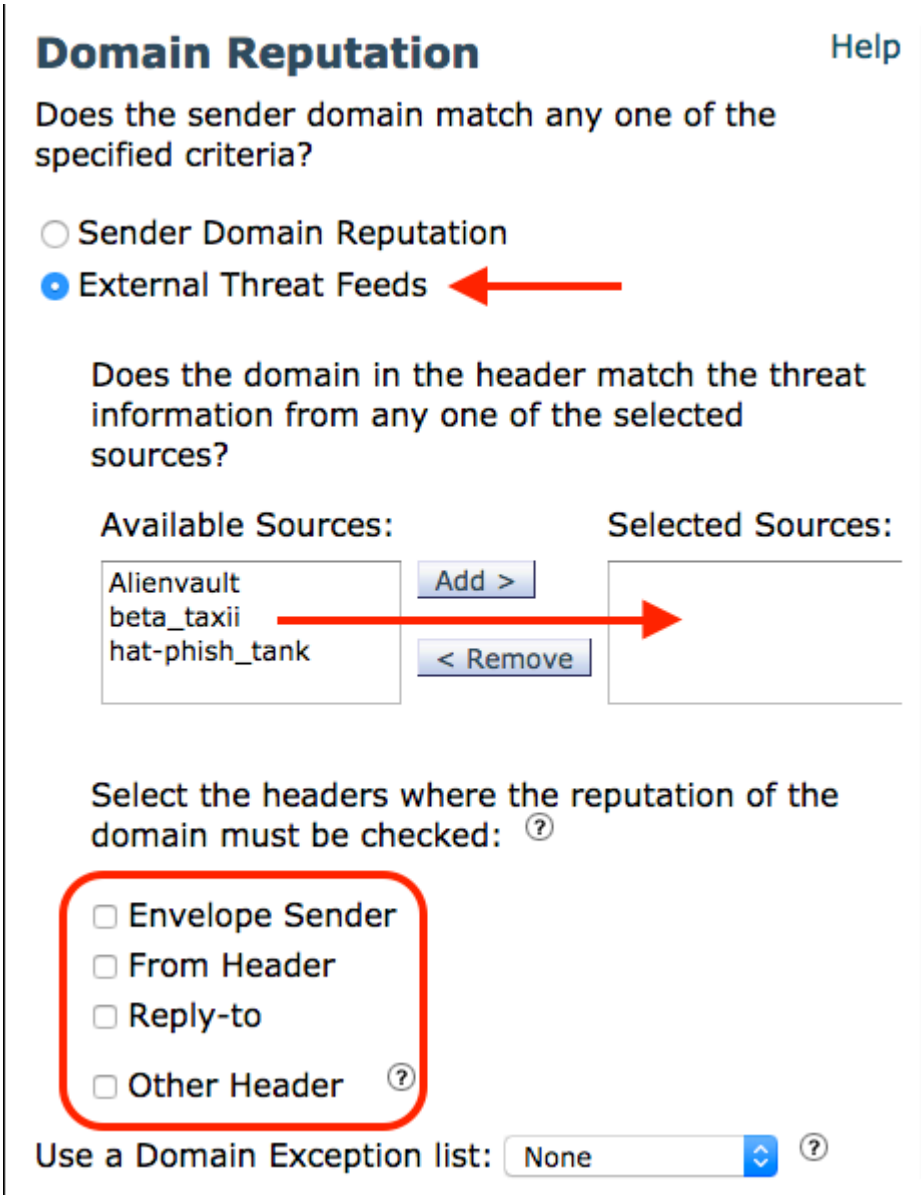
- Consentire agli amministratori di intervenire se non è possibile ottenere un verdetto.



SDR non scansionabile

11. Condizione 4: Feed minaccia esterna

- Le intestazioni incluse in SDR Scanning possono anche essere scansionate con il contenuto STIX/TAXII scaricato in modo personalizzato.
- I feed delle minacce esterne sono illustrati in dettaglio qui. Feed delle minacce esterne.

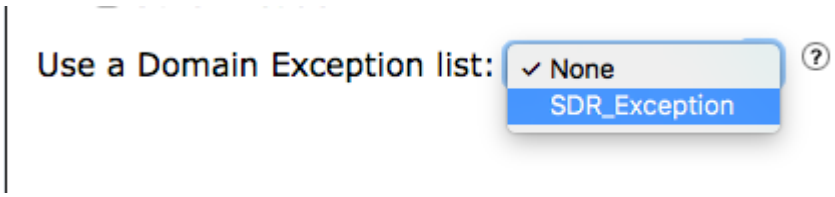


I feed delle minacce esterne possono essere utilizzati per analizzare le stesse intestazioni utilizzate per l'SDR.

- Guide per l'utente di Email Security Appliance

12. Condizione 5: Utilizzare l'elenco eccezioni del dominio.

- L'utilizzo dell'elenco eccezioni di dominio all'interno del filtro contenuto aggiunge un maggiore controllo rispetto all'elenco globale.



L'elenco delle eccezioni di dominio consente per azione di criterio.

13. L'azione combinata con queste condizioni può variare da minima a estrema e dipende dai risultati desiderati dall'amministratore.

14. Sono elencate alcune delle azioni più popolari:

- Quarantena/Copia in quarantena
- Drop
- Aggiungere una dichiarazione di non responsabilità o un avviso all'oggetto o al corpo del messaggio.
- Creare una voce di log per generare una parola, una frase o un valore specifico nei log di verifica messaggi.

Configurazione dell'SDR tramite i filtri messaggi

1. Le Guide per l'utente ESA rappresentano una fonte eccellente per la sintassi, le definizioni e gli esempi del filtro messaggi.
2. Oltre alle informazioni fornite qui, cercare nella Guida per l'utente ulteriori contenuti per i filtri messaggi.

- Filtro dei messaggi in base alla reputazione del dominio del mittente con filtro messaggi

3. Al filtro messaggi SDR sono associate le seguenti condizioni:

- se sdr-reputation (['awful', 'poor'] >>> tutti i valori per questa proprietà includono: Terribile, Povero, Contaminato, Debole, Sconosciuto, Neutro, Buono
- if sdr-reputation (['awful', 'poor'], "<domain_exception_list>") >> È incluso l'utilizzo di un elenco di eccezioni di dominio
- if sdr-age (<'unit'>, <'operator'> <'actual value'>) >> Consultare il Manuale dell'utente per la definizione di "operatore".
    - if (sdr-age ("known", "")) >>> unit = known. I valori rimanenti sono sostituiti con ""
    - esempio: if (sdr-age ("mesi", <, 1, ""). >>> unità = giorni, mesi, anni. Operatore = < (minore di). Valore effettivo = 1
- se sdr-unscannable (<'domain_exception_list'>) >> Come viene visualizzato, se il messaggio risulta unscannable. In questo esempio viene inclusa anche la condizione dell'elenco eccezioni del dominio.
- if (sdr-unscannable ("") >>> In questo esempio non viene incluso l'elenco delle eccezioni. Il valore viene sostituito con ("")

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Una volta abilitato il servizio SDR, i log di posta e il Message Tracking iniziano a mostrare l'SDR: voci di log.

1. mail_logs contiene il punteggio dei dati SDR raccolti.

2. Il punteggio viene determinato nelle prime fasi del flusso di posta, prima di determinare la politica di posta.

3. Le azioni eseguite sul verdetto si verificano al momento delle operazioni filtro messaggi e filtro contenuti.

<#root>

xxx.com>

mail_logs sample including SDR verdict

```
Tue Dec 3 15:22:44 2019 Info: New SMTP ICID 5539460 interface Data 1 (10.10.10.170) address 55.1.x.y re
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 ACCEPT SG Production_INBOUND match xxx1.xxx.com SBRS 2.5 cou
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SHA
Tue Dec 3 15:22:44 2019 Info: Start MID 3291517 ICID 5539460
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 From: <customer@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 RID 0 To: <owner@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 IncomingRelay(PROD_TO_BETA): Header Received found, IP 172.20
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Message-ID '<mail>'
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Subject "You\\'ve Been Nominated for inclusion with Who\\'s W
```

Tue Dec 3 15:22:44 2019 Info: MID 3291517 SDR: Domains for which SDR is requested: reverse DNS host: Not

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Consolidated Sender Reputation: Awful, Threat Category: N

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Tracker Header : 5Zrl76622ZDGPsS6cByUUXq7LTXXS3/wonoZb5cG

```
Tue Dec 3 15:22:46 2019 Info: MID 3291517 ready 10011 bytes from <owner@xxx.com>
Tue Dec 3 15:22:46 2019 Info: MID 3291517 Custom Log Entry: MF_URL_Category_all HIT
Tue Dec 3 15:22:46 2019 Info: MID 3291517 matched all recipients for per-recipient policy DEFAULT in th
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim verdict using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim AV verdict using Sophos CLEAN
Tue Dec 3 15:22:47 2019 Info: MID 3291517 antivirus negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 AMP file reputation verdict : SKIPPED (no attachment in messa
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: GRAYMAIL negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 Custom Log Entry: SDR_Verdict_matched_Awful_Poor
```

```
Tue Dec 3 15:22:47 2019 Info: Start MID 3291519 ICID 0
```

4. Semplici comandi grep per controllare la frequenza o l'esistenza di verdetti specifici.

- >> grep "Reputazione mittente: Brutti" log_di_posta
- >> grep "Reputazione mittente: Scarso" mail_logs

5. Inoltre, i dettagli del log di posta possono essere ottenuti usando il comando findevent della CLI insieme al valore MID.

```
xxx.com> grep "SDR: Domain Reputation.*Poor" mail_logs
Tue Dec 3 11:07:01 2019 Info: MID 3265844 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
Tue Dec 3 12:57:28 2019 Info: MID 3277401 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
```

```
xxx.com> grep "SDR: Domain Reputation.*Awful" mail_logs
Tue Dec 3 10:24:08 2019 Info: MID 3261075 SDR: Consolidated Sender Reputation: Awful, Threat Category: N
Tue Dec 3 15:18:27 2019 Info: MID 3291182 SDR: Consolidated Sender Reputation: Awful, Threat Category: N
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

1. Nessun SDR: log presenti in mail_logs o Message Tracking.

- I registri SDR possono essere sempre presenti per i messaggi che passano attraverso un criterio di flusso di posta ACCEPT.
- Accertarsi che il Servizio sia stato attivato come indicato nelle fasi iniziali di questa guida.

2. Timeout SDR:

- Verificare che il server cloud Cisco per SDR sia aperto e disponibile per l'uso.
- v2.sds.cisco.com
- Un test molto generale può essere eseguito usando il telnet dalla CLI.
- Se viene visualizzato il banner, è possibile confermare la raggiungibilità di base.
    - CLI > telnet v2.sds.cisco.com 443 (questo può verificare solo un point in time).
- Controllare i registri di altri servizi per determinare se vi sono potenziali errori di comunicazione con i servizi basati su Internet.
- CLI > visualizza gli avvisi per verificare la presenza di ulteriori segnali di errore di

comunicazione.
- Nelle versioni precedenti alla 13.5, AsyncOS, SDR e URL Filtering utilizzano entrambi il sito v2.sds.cisco.com.
    - Se il comando CLI del filtro URL > websecuritydiagnostics contiene una latenza, è possibile verificare se il percorso di rete contiene una latenza.
- Controllare l'impostazione di timeout della reputazione del dominio mittente e determinare se il valore può essere aumentato di 1-10 secondi. Passare a Servizi di sicurezza > Reputazione dominio > Modifica > Timeout query reputazione dominio mittente:2

L'impostazione predefinita è 2 secondi e l'impostazione massima è 10 secondi.

Aggiornamento importante per versioni AsyncOS successive a 14

Dopo la transizione, il nome host v2.sds.cisco.com può ancora essere disponibile ma non può più essere ottimizzato sia per il filtro URL che per l'SDR.

È necessario consentire questi nomi host e indirizzi IP sul firewall per il traffico della porta TCP 443 in uscita.

Nomi host:

- serviceconfig.talos.cisco.com
- grpc.talos.cisco.com
- email-sender-ip-rep-grpc.talos.cisco.com

Intervalli indirizzi IP:

- 146.112.62.0/24
- 146.112.63.0/24
- 146.112.255.0/24
- 146.112.59.0/24
- 2a04:e4c7:ffff:/48
- 2a04:e4c7:fffe: 1000/48

Si tratta degli endpoint Cisco Talos Intelligence Services utilizzati per ottenere la reputazione IP, la reputazione e la categoria dell'URL e per inviare i dettagli dei log di servizio.

Informazioni correlate

- Guide per l'utente ESA
- Note release ESA
- Guide di riferimento CLI ESA
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).