Configure Sender Domain Reputation para ESA REFRESH en curso Abril de 2024

Contenido

Introducción

Este documento describe la configuración de Reputación de dominio de remitente (SDR) para el dispositivo de seguridad Email Security Appliance (ESA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conceptos ESA
- configuración ESA

- Conocimiento general de las funciones/características de SEG, entre las que se incluyen: Políticas de flujo de correo, filtros de mensajes, filtros de contenido, reputación de dominio global.

Componentes Utilizados

La información de este documento se basa en AsyncOS para ESA 14.2 y versiones posteriores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

1. SDR se ha desarrollado como un servicio adicional para mejorar la detección de spam y phishing.

2. SDR captura múltiples valores de encabezado y los carga en Talos Threat Intelligence Servers donde los vastos recursos de Talos determinan un veredicto para cada mensaje en una escala gradual.

3. Los valores de cabecera incluidos en la decisión son:

- De sobre
- Desde
- Responder a
- Verificación de DMAR, DKIM y SPF (si está configurada).
- El valor (nombre de usuario) de la dirección de correo electrónico se envía opcionalmente desde los encabezados De, De sobre y Responder a
- IP del remitente
- Mostrar nombre en los encabezados De y Responder a.

5. El análisis de SDR se realiza en todos los mensajes entrantes.

6. El análisis de SDR tiene lugar justo después de que el Protocolo simple de transferencia de correo (SMTP) acepte un mensaje.

7. La acción de SDR se puede realizar en la fase inicial de la política de flujo de correo, así como

en las opciones de filtro de mensajes o filtro de contenido.

8. Los componentes configurados incluyen:

- Habilitar servicio de reputación de dominio
- Listas de excepciones de dominio (opcional)
    - Lista de excepciones de dominio (global)
    - Lista de excepciones de dominio que utiliza filtros de contenido/mensajes específicos.
    - Acción global con reparación de dominio mediante políticas de flujo de correo.
    - Acción global con Reputación de dominio que realiza acciones en el nivel de conversación SMTP.
- Filtro de mensajes o filtro de contenido

Configurar

Habilitar WebUI del servicio de Reputación de dominio

SDR se puede habilitar desde la interfaz de usuario Web o desde las interfaces CLI.

InterfazWeb:

1. Vaya a Servicios de seguridad de correo > Reputación de dominio > Activar.

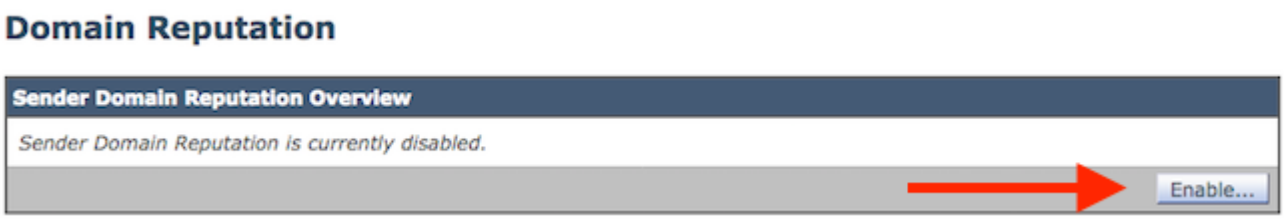
2. Haga clic en la casilla junto a Habilitar filtro de reputación de dominio de remitente.

3. Active esta casilla Incluir Atributos Adicionales: (Opcional) si desea incluir el valor de cabecera opcional en los datos marcados para mejorar la eficacia. Haga clic en ? para aprender.

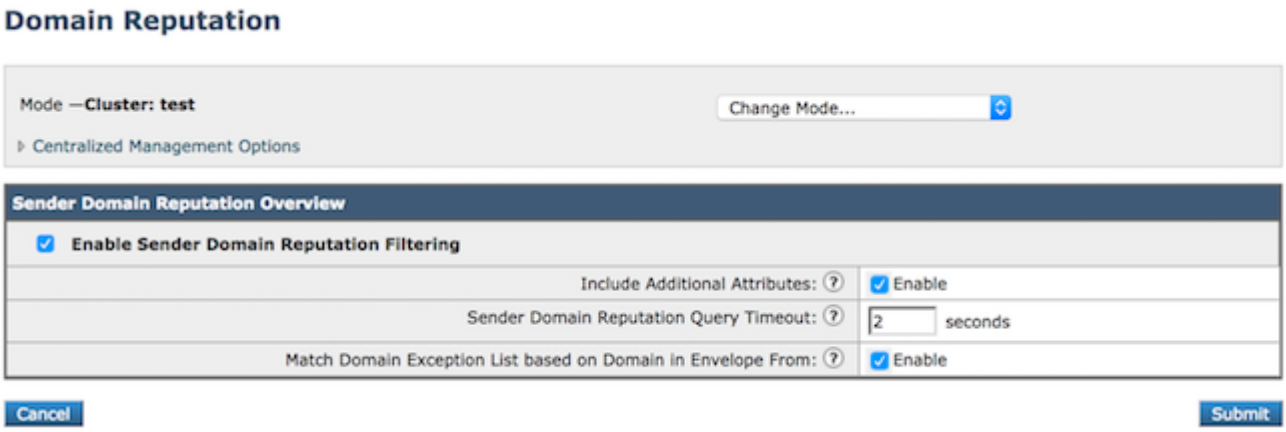
4. Active esta casilla Tiempo de Espera de Consulta de Reputación de Dominio de Remitente. Haga clic en ? para aprender.

5. Seleccione Coincidir con Lista de Excepciones de Dominio según Dominio en De Sobre - Activado.

6. Haga clic en Submit > Commit como se muestra en la imagen.



Servicio de remitente (reputación de dominio)



Servicios de seguridad > Reputación de dominio

Lista de excepciones de dominio

1. La Lista de excepciones de dominio puede omitir el Análisis de Reputación de Dominio de Remitente para el flujo de correo entrante.

2. La lista de excepciones de dominio se puede aplicar en diferentes ubicaciones para afectar al flujo de correo.

3. La aplicación Global se puede aplicar a todos los correos escaneados.

4. La aplicación más detallada dentro de los filtros de contenido/mensaje puede afectar solamente a un filtro configurado.

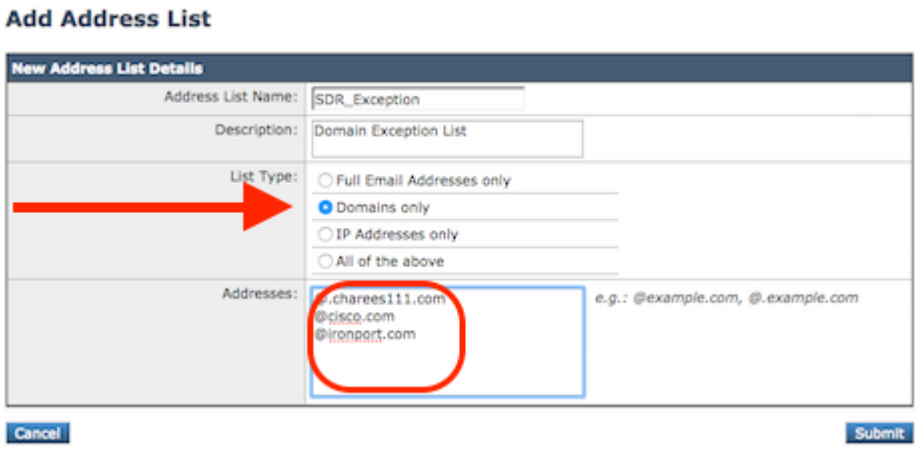
5. La Lista de excepciones de dominio proporciona 2 opciones para proporcionar una opción tanto sencilla como más segura.

6. En este documento se describen las opciones para omitir correctamente SDR en un mensaje que utiliza la Lista de excepciones de dominio.

7. Explicación de los requisitos de la lista de excepciones de dominio

Crear una lista de direcciones

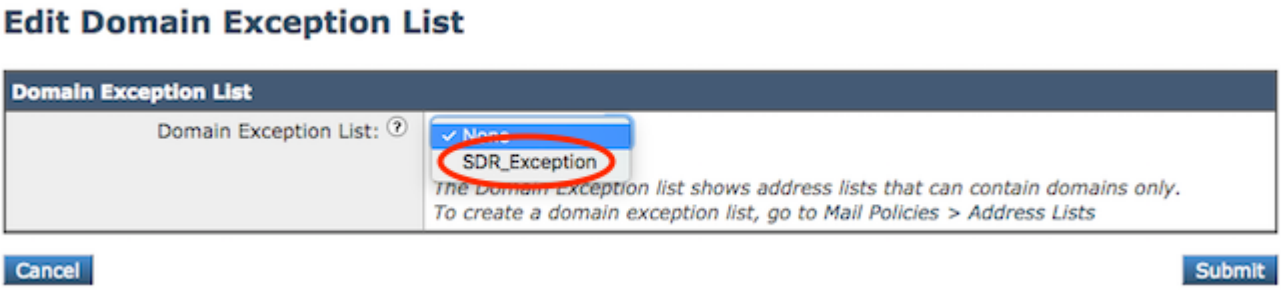
1. Vaya a Políticas de correo > Lista de direcciones > Agregar lista de direcciones > Nombre > Descripción > Tipo de lista: Sólo dominios.
2. Agregue cada nombre de dominio mediante el uso de la separación por comas.
3. Haga clic en Submit y Commit Changes como se muestra en la imagen.



Lista de direcciones que se aplicará a la lista de excepciones de dominio

Aplicar la lista de direcciones a la lista de excepciones de dominio global de SDR

1. Vaya a Servicios de seguridad > Reputación de dominio > Lista de excepciones de dominio > Editar configuración > Lista de excepciones de dominio (seleccione la lista).
2. Haga clic en Submit y Commit Changes como se muestra en la imagen.



Elija una lista de direcciones del menú desplegable

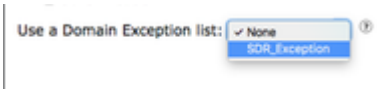
Aplicación de la lista de direcciones a los filtros de contenido/mensajes

Filtros de contenido entrante:

1. Vaya a Condición > Reputación de URL > Opción Fuentes de amenazas.

2. Condición Reputación de dominio.

3. Haga clic aquí:



La lista de excepciones de dominio permite cada acción de directiva.

Filtros de mensajes

La aplicación Lista de excepciones de dominio dentro de los filtros de mensajes se incluiría como una opción dentro de una condición.

Nota: Estos ejemplos incluyen domain_exception_list como parte de toda la condición.

---

1. reputación de sdr (['horrible', 'pobre', 'contaminado', 'débil', 'desconocido', 'neutral', 'bueno'], domain_exception_list)
2. sdr-age ("days", <, 5, domain_exception_list)
3. sdr-unscannable (domain_exception_list)

Puede encontrar una explicación más completa y ejemplos de la aplicación del filtro de mensajes con las Guías de usuario ESA bajo los encabezados:

- Regla de reputación de dominio para ETF
- Filtrado de mensajes basado en Reputación de dominio de remitente que utiliza el filtro de mensajes

Crear un filtro de contenido para tomar medidas sobre el veredicto de SDR

1. SDR solo está activado para el flujo de correo entrante.
2. El nombre de la condición SDR: Reputación de dominio.
3. Se pueden crear varias condiciones para combinar resultados diferentes.
4. La condición de reputación de dominio contiene dos comprobaciones diferentes que contienen varias opciones para cada una:

- Reputación de dominio de remitente
    - Veredicto de Reputación de dominio de remitente
    - Antigüedad del dominio del remitente
    - Reputación de dominio de remitente no escaneable
- Fuentes sobre amenazas externas
    - Permite la utilización de las listas de contenido descargado de fuentes de amenazas para analizar los mismos encabezados de dominio recopilados para SDR.

✎ Nota: Estas opciones de la Condición de reputación de dominio pueden cambiar visualmente en función de las diferentes opciones de cada selección.

---

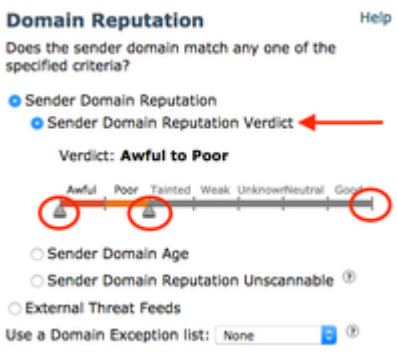
5. La última opción de la Condición de Reputación de Dominio es la Lista de Excepciones de Dominio.

6. La función Lista de excepciones de dominio asociada a una lista de direcciones añade más control a la aplicación de la acción al aplicar la lista al nivel más detallado de la política de correo del procesamiento de mensajes.

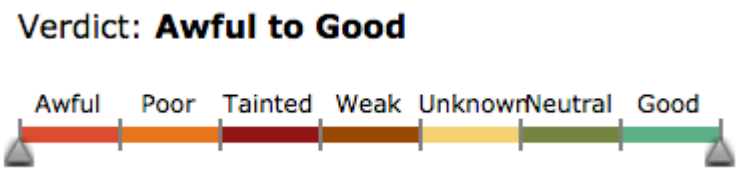
7. Vaya a Mail Policy > Incoming Content Filters > Add Filter > Add Condition > Domain Reputation.

8. Condición 1: Veredicto de Reputación de dominio de remitente.

- Horrible, pobre, manchado, débil, desconocido, neutral, bueno
- Contiene marcadores triangulares deslizantes para elegir el rango que desea igualar.
- Los valores Awful y Poor son los valores recomendados para tomar medidas.
- Los mensajes que coinciden con Malo y Malo pueden tener una Categoría adicional, valor como Spam o Malintencionado visible dentro de Rastreo de mensajes.



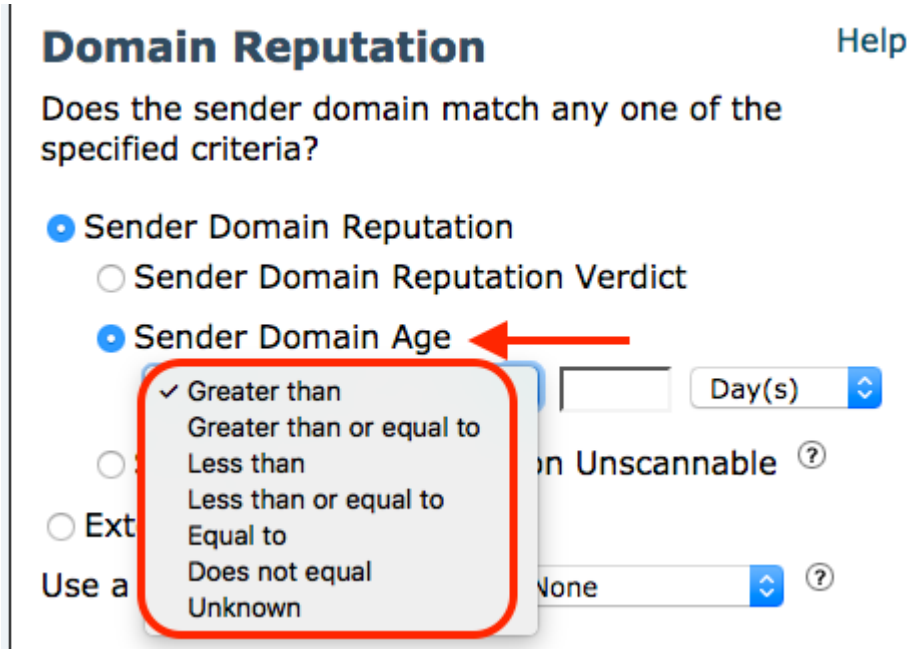
Barra deslizante de alcance ajustable de SDR Verdict.



Vista completa de la barra deslizante de veredicto de SDR.

9. Condición 2: Antigüedad del dominio del remitente.

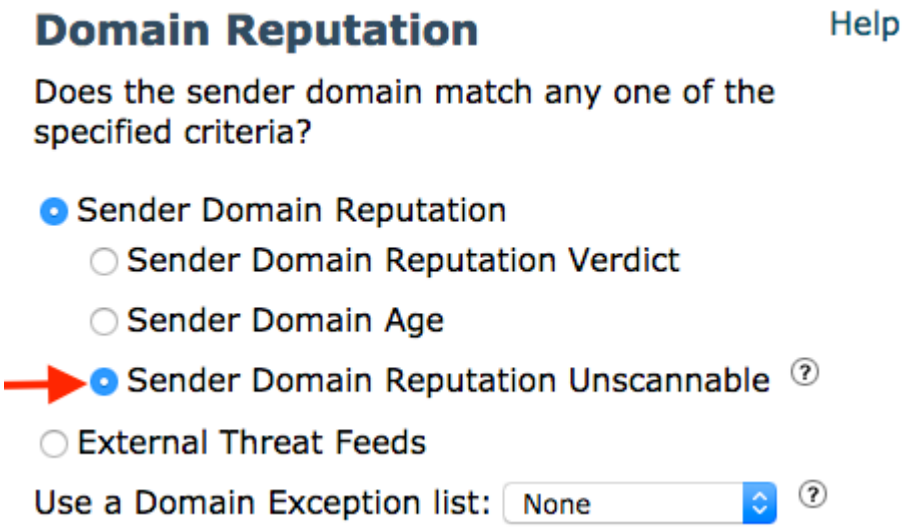
- La antigüedad del dominio puede estar asociada a un mayor riesgo o a una confiabilidad establecida desde hace mucho tiempo.
- La posibilidad de un dominio con una antigüedad inferior a 10 días puede ser más arriesgada.



Antigüedad del dominio del remitente. Los valores más bajos sugieren más riesgo.

10. Condición 3: Reputación de dominio de remitente no escaneable.

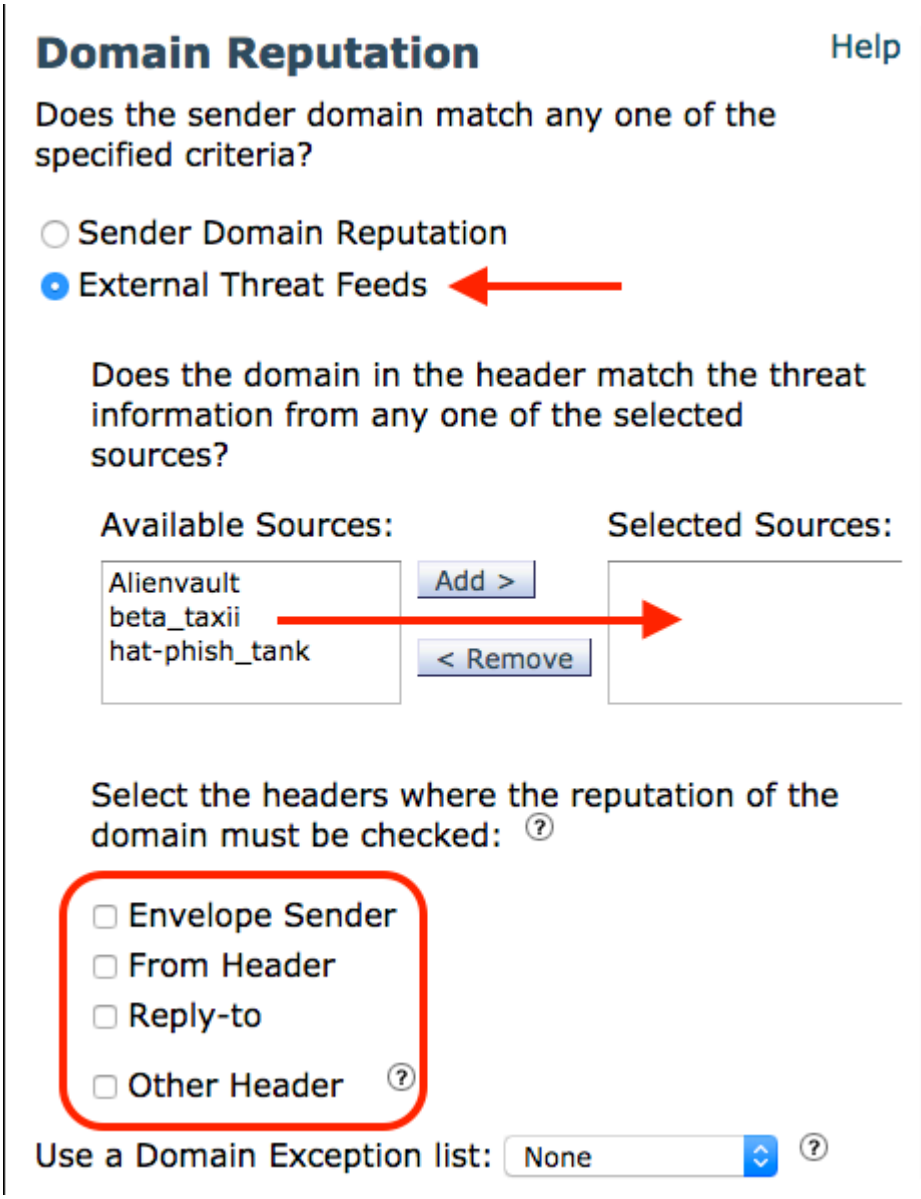
- Proporcione una opción para que los administradores tomen medidas si no se puede obtener un veredicto.



SDR no escaneable

11. Condición 4: Fuentes de amenazas externas

- Los encabezados incluidos en el escaneo de SDR también se pueden escanear con contenido STIX/TAXI descargado personalizado.
- Las fuentes de amenazas externas se tratan con más detalle aquí. Fuentes de amenazas externas.

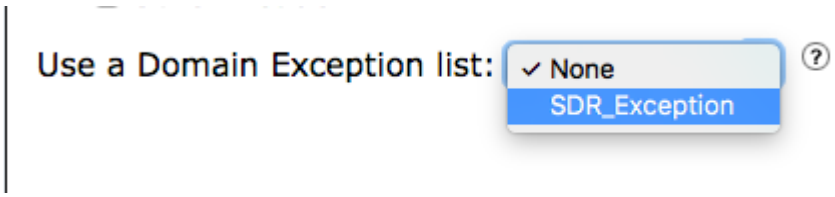


Las fuentes de amenazas externas se pueden utilizar para analizar los mismos encabezados utilizados para SDR.

- Guías de usuario de Email Security Appliance

12. Condición 5: Usar lista de excepciones de dominio.

- El uso de la Lista de excepciones de dominio dentro del Filtro de contenido agrega más control que la Lista global.



La lista de excepciones de dominio permite cada acción de directiva.

13. La acción combinada con estas condiciones puede oscilar entre mínima y extrema y depende de los resultados deseados del administrador.

14. Se enumeran algunas de las acciones más populares:

- Cuarentena/Copiar a cuarentena
- Abandonar
- Agregue una renuncia o advertencia al asunto o al cuerpo del mensaje.
- Cree una entrada de registro para generar una palabra, frase o valor específico para los registros de seguimiento de mensajes.

Configuración de SDR mediante el uso de filtros de mensajes

1. Las Guías de usuario ESA son una fuente excelente para la sintaxis, definiciones y ejemplos del filtro de mensajes.
2. Busque este encabezado en la guía del usuario para obtener contenido adicional para los filtros de mensajes además de la información proporcionada aquí.

- Filtrado de mensajes basado en Reputación de dominio de remitente con filtro de mensajes

3. Estas condiciones están asociadas con el filtro de mensajes SDR:

- if sdr-reputación (['horrible', 'pobre'] **>>>** todos los valores para esto incluyen: Horrible, pobre, manchado, débil, desconocido, neutral, bueno
- if sdr-reputation (['horrible', 'poor'], "<domain_exception_list>") **>>>** Esto incluye el uso de una Lista de excepciones de dominio
- if sdr-age (<‘unit'>, <‘operator'> <‘real value’>) **>>>** Consulte la guía del usuario para obtener la definición de "operator".
    - if (sdr-age ("unknown", "")) **>>>** unit = unknown. Los valores restantes se sustituyen por ""
    - ejemplo: if (sdr-age ("meses", <, 1, "")). **>>>** unit = días, meses, años. Operador = < (menor que). Valor real = 1
- if sdr-unscannable (<'domain_exception_list'>) **>>>** As present, if the message results in unscannable. Este ejemplo también incluye la condición de lista de excepciones de dominio.
- if (sdr-unscannable ("") **>>>** Este ejemplo no incluye la lista de excepciones. El valor se sustituye por ("")

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Una vez que se ha habilitado el servicio SDR, los mail_logs y el rastreo de mensajes comienzan a mostrar el SDR: entradas de registro.

1. mail_logs contiene la puntuación de los datos de SDR recopilados.

2. La puntuación se determina en una fase temprana del flujo de correo, antes de determinar la política de correo.

3. Las acciones realizadas sobre el veredicto se producen en el momento del filtro de mensajes y de las acciones de filtrado de contenido.

<#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. Comandos grep simples para verificar la frecuencia o existencia de veredictos específicos.

- >> grep "Sender Reputation: Awful" mail_logs
- >> grep "Sender Reputation: Deficiente" mail_logs

5. Además, los detalles del registro de correo se pueden obtener con el uso del comando findevent de la CLI junto con el valor 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: I
Tue Dec 3 15:18:27 2019 Info: MID 3291182 SDR: Consolidated Sender Reputation: Awful, Threat Category: I
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

1. Sin SDR: registros presentes en mail_logs o Rastreo de mensajes.

- Los registros de SDR siempre pueden estar presentes para los mensajes que pasan a través de una política de flujo de correo ACCEPT.
- Asegúrese de que el servicio se ha habilitado tal y como se describe en los pasos iniciales de esta guía.

2. Tiempo de espera de SDR agotado:

- Verifique que el servidor en la nube de Cisco para SDR esté abierto y disponible para su uso.
- v2.sds.cisco.com
- Se puede realizar una prueba muy general con el uso de telnet desde la CLI.
- Si aparece el banner, puede confirmar el alcance básico.
    - CLI > telnet v2.sds.cisco.com 443 (esto puede verificar solamente un punto en el

tiempo).

- Compruebe los registros de otros servicios para determinar si hay posibles fallos de comunicación con los servicios basados en Internet.
- CLI > muestra alertas para verificar si hay señales adicionales de fallas de comunicación.
- Antes de la versión 13.5 de AsyncOS, SDR y el filtrado de URL utilizaban v2.sds.cisco.com.
    - Una verificación del comando URL Filtering CLI > websecuritydiagnostics puede proporcionar cierta validación si la trayectoria de red contiene latencia.
- Verifique la Configuración de Tiempo de Espera de Reputación de Dominio de Remitente, y determine si el valor puede aumentarse de 1 a 10 segundos. Vaya a Servicios de seguridad > Reputación de dominio > Editar > Tiempo de espera de consulta de Reputación de dominio de remitente:2

El valor predeterminado es 2 segundos y un valor máximo de 10 segundos.

Actualización importante para versiones de AsyncOS posteriores a 14

Después de la transición, el nombre de host v2.sds.cisco.com todavía puede estar disponible, pero ya no puede optimizarse para el filtrado de URL y SDR.

Debe permitir estos nombres de host y direcciones IP en su firewall para el tráfico de salida del puerto TCP 443.

Nombres de host:

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

Intervalos de direcciones 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::/48

Se trata de terminales de Cisco Talos Intelligence Services utilizados para obtener reputación de IP, reputación de URL y categoría, así como para enviar detalles de registros de servicios.

Información Relacionada

- Guías de usuario ESA
- Notas de la versión ESA
- Guías de referencia de ESA CLI
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).