Verificar cambio de Reputación de dominio de remitente en actualización de AsyncOS 14.2.0

Contenido

Introducción

En este documento se describen los cambios de para Sender Domain Reputation (SDR) en la plataforma Secure Email para las instalaciones, el entorno virtual (ESA) y el entorno de nube (CES).

P. ¿Cuáles son los cambios realizados en SDR AsyncOS 14.2.0?

Advertencia: Las configuraciones de SDR de la acción Rechazar para veredictos viciados y/o débiles se cambian automáticamente al actualizar a la versión 14.2. La configuración cambia la configuración de ESA SDR para que se rechace en el nivel de amenaza neutra.

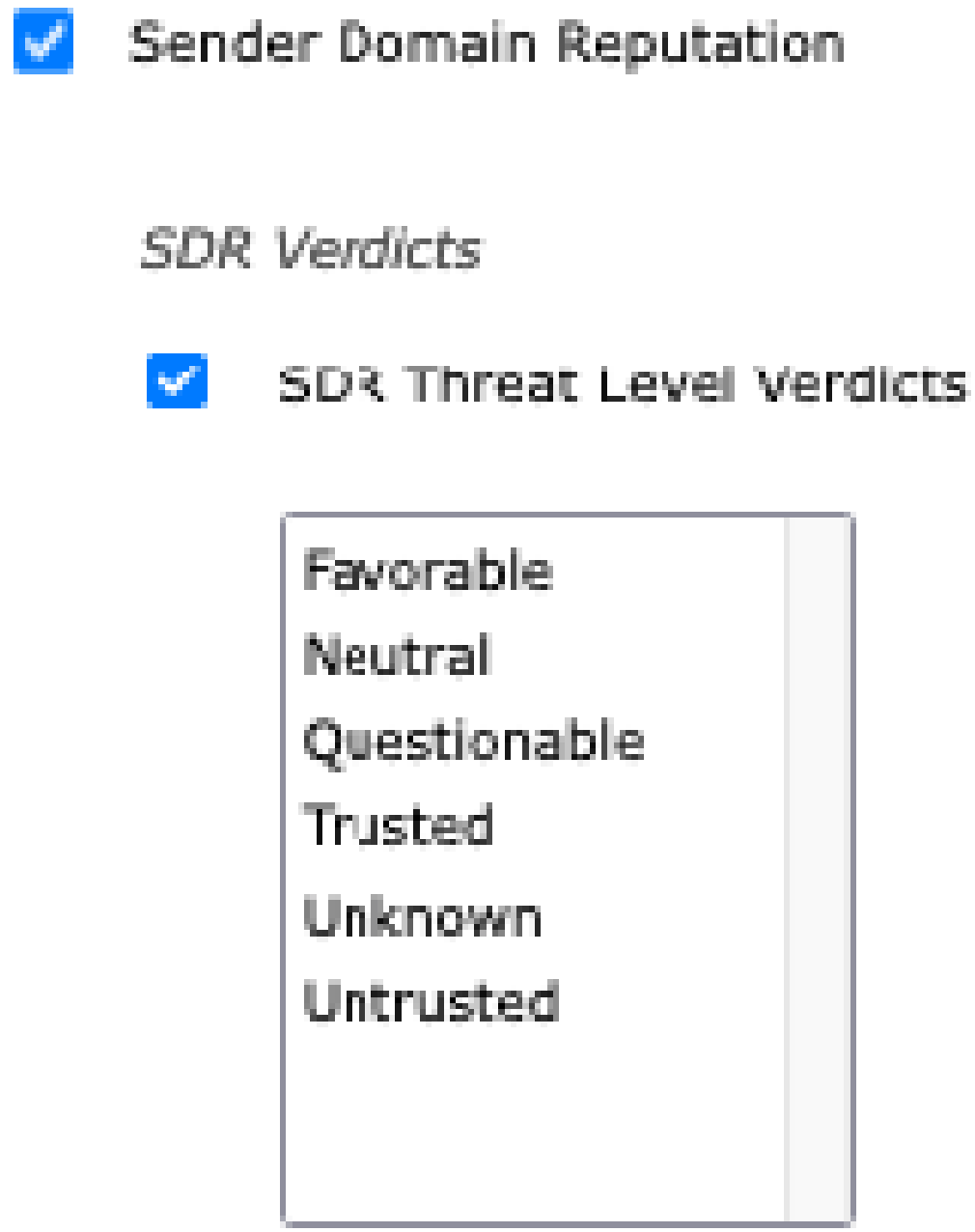
1) Los veredictos heredados de SDR cambian de veredictos ahora denominados Niveles de amenaza, como se muestra en la imagen:

Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

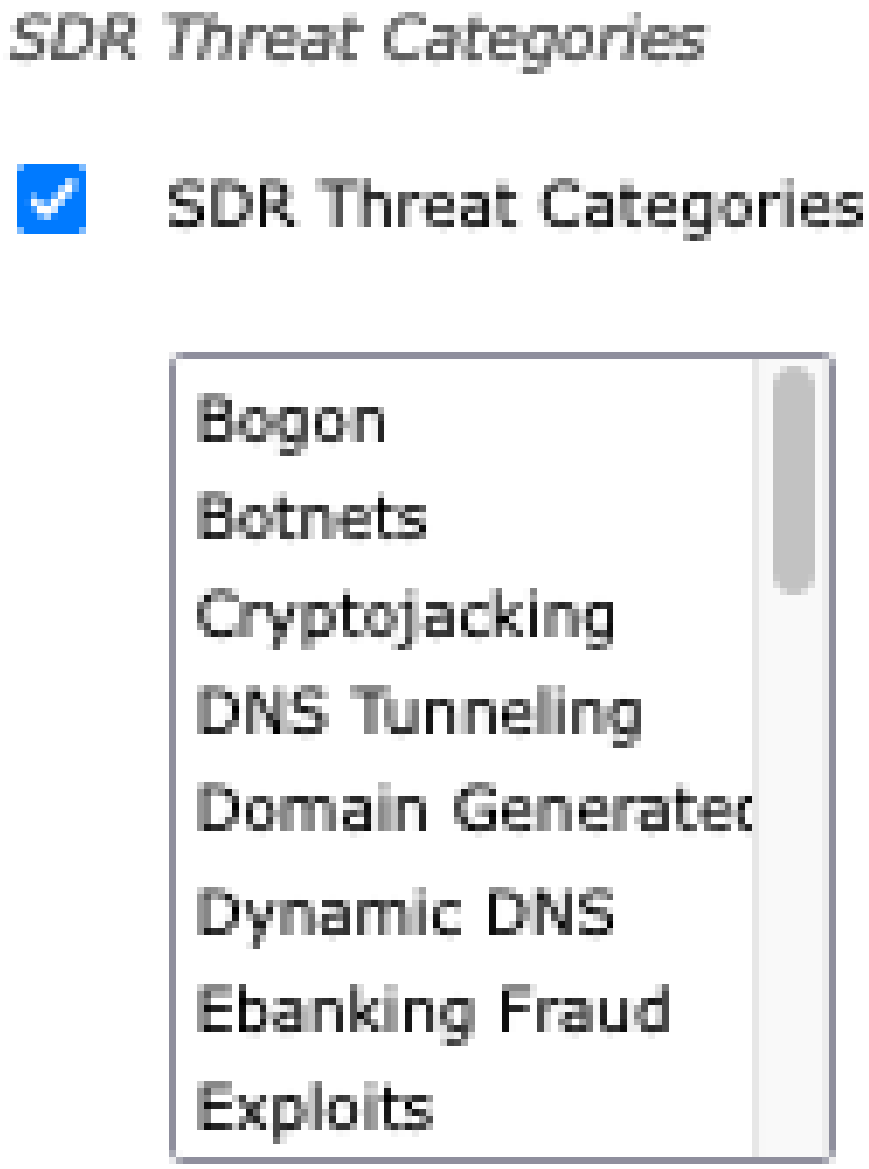
Nota: Se trata de un cambio en el comportamiento de análisis de SDR con un mecanismo de decisión de veredicto diferente. No debe esperar que el veredicto coincida con la

solución anterior para cada conjunto de información del remitente.

2) 'Rastreo de mensajes' por la condición avanzada de SDR se reemplaza con la lista mostrada:



3) La categoría de amenaza de fraude bancario de SDR se cambia a fraude bancario electrónico, como se muestra en la imagen:



Nota: Todas las categorías no fiables no aparecen en la lista; sin embargo, las categorías de SDR como, por ejemplo, 'spam', 'malicioso', etc., se marcan como No fiable o Cuestionable.

4) mail_logs contiene una línea de registro adicional para los veredictos de SDR. Se escribe después de From logline si la reputación de los remitentes no se rechaza. Aparece una segunda línea de SDR en los registros de correo.

<#root>

```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11

SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: desktop-9pf6f2t, env-from:

Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s)
Info: MID 11 ICID 19884 RID 0 To: test@cisco.com
```

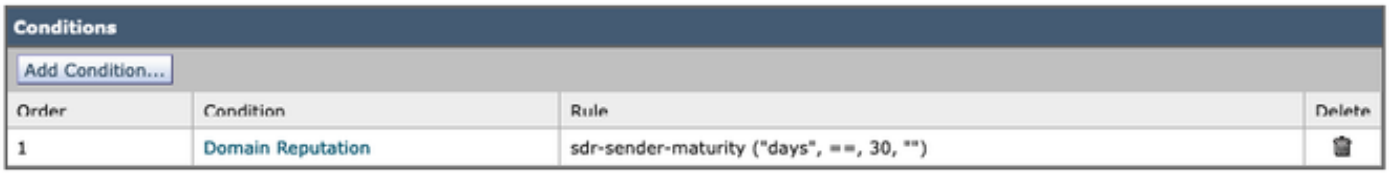
```
Info: MID 11 Message-ID 'op.1m7bljjr8qfre9@desktop-9pf6f2t'
Info: MID 11 Subject "test 1"
Info: MID 11

SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: desktop-9pf6f2t, env-from:

Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s)
Info: MID 11 SDR: Tracker Header : 629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOt
```

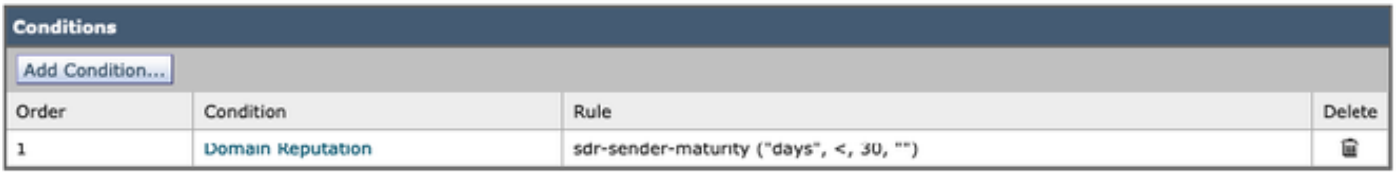
5) SDR configurado para rechazar en la configuración global se produce en la fase de sobre de la conversación SMTP, que es justo después de que se envía el sobre desde el encabezado y no se ha enviado ningún otro dato todavía.

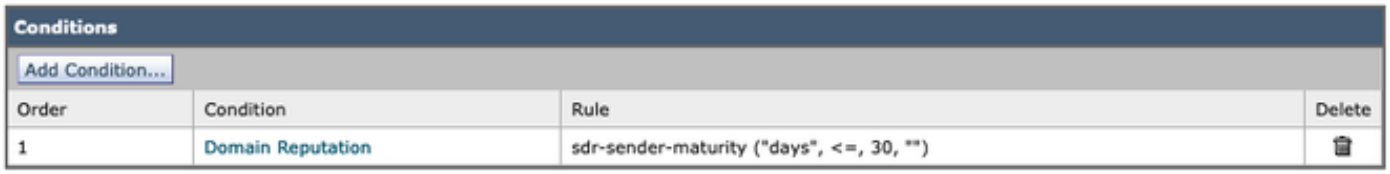
<#root>

```
Info: Start MID 9364 ICID 79
Info: MID 9364 ICID 79 From: <test@incomingtest.contentfilter.com>
Info: MID 9364 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: mail.cisco
Info: MID 9364

SDR: Consolidated Sender Threat Level: Untrusted, Threat Category: N/A, Suspected Domain(s) : lana.cf. S

Info: MID 9364 ICID 79 Receiving Failed: Message rejected by Sender Domain Reputation engine
Info: MID 9364 SDR: Tracker Header : 629d5de5_JxmxzLXzbSob4h6Tqmxj2QFeN6eeb3J8CJ2zj9h8XgF/+e0YQVxd05lnV
Info: MID 9364

Subject ""

Info:

Message aborted MID 9364 Receiving aborted

Info: Message finished MID 9364 aborted
```

6) Debido al comportamiento esperado explicado como se proporciona en 'Cisco bug ID CSCwb32685' y aquí Aviso de campo: FN - 72389 - Cisco Secure Email Gateway: Talos Domain Age Update no debe utilizar las tres condiciones en sus filtros: menor que, igual a, y menor que e igual a, de lo contrario todos los dominios que alcanzan la política o políticas coinciden con las condiciones, como se muestra en la imagen:







Nota: La madurez del remitente está establecida en un límite de 30 días y, más allá de este límite, un dominio se considera maduro como remitente de correo electrónico y no se proporcionan más detalles.

Información Relacionada

Notas de la versión de Cisco Secure Email AsyncOS 14.2.

Notas de la versión de Cisco Secure Email and Web Manager AsyncOS 14.2.

Aviso práctico: FN - 72389 - Cisco Secure Email Gateway: Talos Domain Age Update

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).