Verificar alteração da Reputação de Domínio do Remetente na atualização do AsyncOS 14.2.0

Contents

Introduction

Este documento descreve as alterações do SDR (Sender Domain Reputation) na plataforma Secure Email para ambientes locais, virtuais (ESA) e em nuvem (CES).

P. Quais são as alterações feitas no SDR AsyncOS 14.2.0?

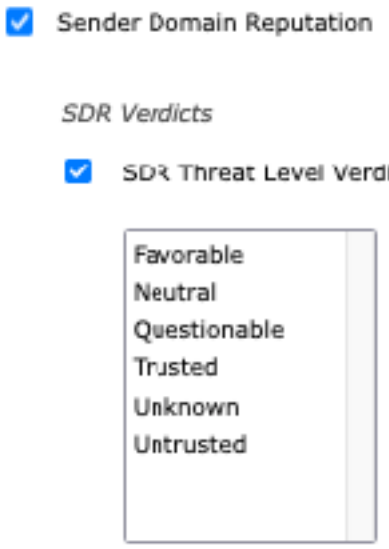
> **aviso: As configurações do SDR da ação Rejeitar para Veredictos Tainted e/ou Weak são alteradas automaticamente na atualização para 14.2. A configuração altera a configuração do SDR do ESA para rejeitar no nível de ameaça neutra.**

1) Os vereditos legados do SDR alteram os vereditos agora chamados **níveis de ameaça**, como mostrado na imagem:

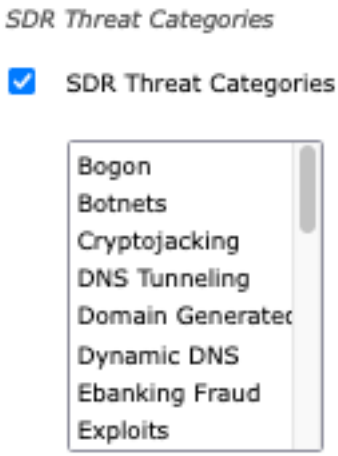
Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **Note**: Essa é uma alteração no comportamento de varredura do SDR com um mecanismo de decisão de veredito diferente. Você não deve esperar que o veredito corresponda à solução antiga para cada conjunto de informações do remetente.

2) "Rastreamento de mensagem" pela condição avançada do SDR é substituído pela lista mostrada:



3) A Categoria de Ameaça de SDR **Fraude Bancária** é alterada para **Fraude Ebanking**, como mostrado na imagem:



Note: **Todos os não confiáveis** não têm uma categoria listada, no entanto, as categorias de SDR como '*spam*,' '*mal-intencionado*,' etc, são sinalizadas como **Não confiável** ou **Questionável**.

4) mail_logs contém uma linha de log adicional para vereditos SDR, ela é escrita após **From** logline se a reputação do remetente não for rejeitada. Uma segunda linha SDR aparece nos logs de e-mail.

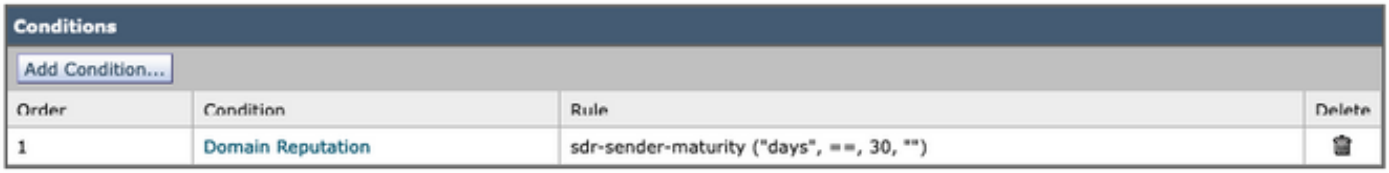
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain:
cisco.com
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: cisco.com, header-from: cisco.com, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected
```

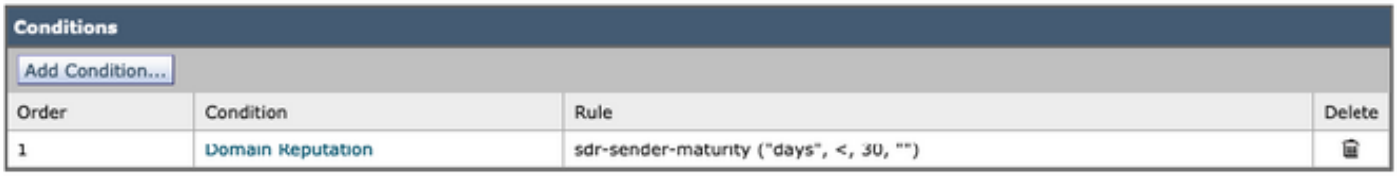
```
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain:
cisco.com
Info: MID 11 SDR: Tracker Header :
629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOtRVhrhSJWgCv2NjL/JQMsjH5QzZw=
=
```

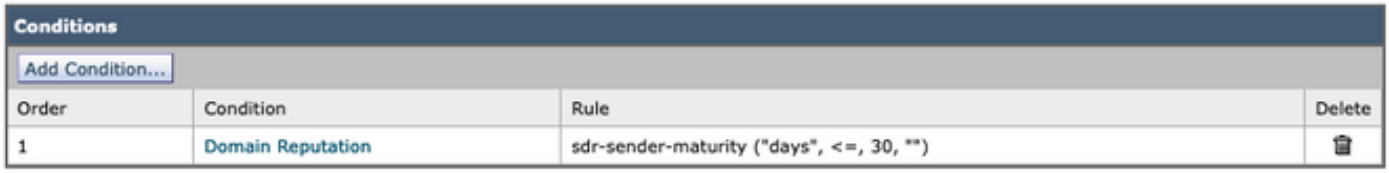
5) O SDR configurado para rejeitar nas configurações globais ocorre na fase de envelope da conversação SMTP, que ocorre logo após o envelope do cabeçalho ser enviado e nenhum outro dado ser enviado ainda.

```
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.com, env-from: lana.cf, header-from: Not Present, reply-to: Not Present
Info: MID 9364 SDR: Consolidated Sender Threat Level: Untrusted, Threat Category: N/A, Suspected
Domain(s) : lana.cf. Sender Maturity: 1 day for domain: lana.cf
Info: MID 9364 ICID 79 Receiving Failed: Message rejected by Sender Domain Reputation engine
Info: MID 9364 SDR: Tracker Header :
629d5de5_JxmxzLXzbSob4h6Tqmxj2QFeN6eeb3J8CJ2zj9h8XgF/+e0YQVxd05lnVSwX9Gh37ISaiDHc0SJ5eRdyLYasmQ=
=
Info: MID 9364 Subject ""
Info: Message aborted MID 9364 Receiving aborted
Info: Message finished MID 9364 aborted
```

6) Devido ao comportamento esperado explicado conforme fornecido em 'ID de bug da Cisco CSCwb32685' **e aqui** Nota de campo: FN - 72389 - Cisco Secure Email Gateway: Atualização da idade do domínio do Talos você não deve usar as três condições em seus filtros: **menor que**, **igual a**, e **menor que e igual a**, caso contrário, todos os domínios que atingem a política ou políticas correspondem às condições, como mostrado na imagem:







> **Observação**: a Maturidade do remetente é definida para um limite de 30 dias e, além desse limite, um domínio é considerado maduro como um remetente de e-mail e nenhum outro detalhe é fornecido.

Informações Relacionadas

Notas de versão do Cisco Secure Email AsyncOS 14.2.

Notas de versão do Cisco Secure Email and Web Manager AsyncOS 14.2.

Nota de campo: FN - 72389 - Cisco Secure Email Gateway: Atualização da idade do domínio do Talos