14.2.0 AsyncOSアップグレードでの送信者ドメインレピュテーションの変更の確認

内容

概要

このドキュメントでは、オンプレミス、仮想環境(ESA)、およびクラウド環境(CES)向けのセキュアEメールプラットフォームでの送信者ドメインレピュテーション(SDR)の変更点について説明します。

Q. SDR AsyncOS 14.2.0での変更点は何ですか。

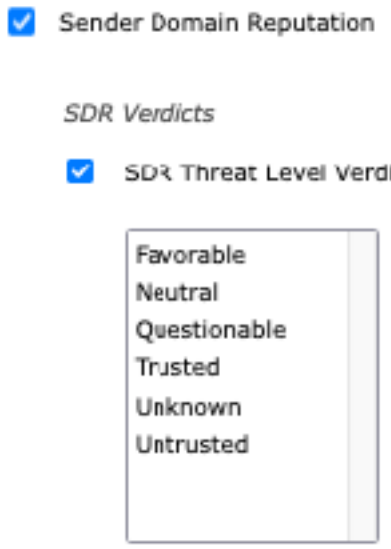
> **警告：汚染された判定および/または脆弱な判定に対する拒否アクションのSDR設定は、14.2へのアップグレード時に自動的に変更されます。この設定により、ESA SDR設定が二ュートラル脅威レベルで拒否するように変更されます。**

1) SDRレガシー判定Threat Levelsという名前の判定の変更（図を参照）

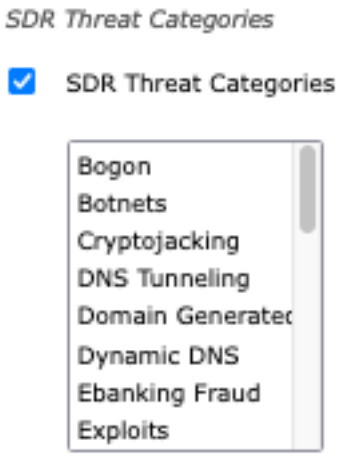
Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **注：**これは、異なる判定決定メカニズムによるSDRスキャン動作の変更です。すべての送信者情報のセットに対して、判定が古いソリューションと一致することを期待しないでください。

2) SDRの拡張条件による「メッセージトラッキング」は、次のリストに置き換えられます。



3) SDR Threat Category **Banking Fraudは、次の図に示すように、Ebanking Fraudに変更されています。**



注：すべての信頼できないにはカテゴリがリストされていませんが、「*spam*」、「*malicious*」などのSDRカテゴリには、*信頼できないまたは疑わしい*というフラグが付いています。

4) mail_logsにはSDR判定用の追加のログ行が含まれています。送信者のレピュテーションが拒否されない場合、この行は**From**ログラインの後に書き込まれます。メールログに2番目のSDR行が表示されます。

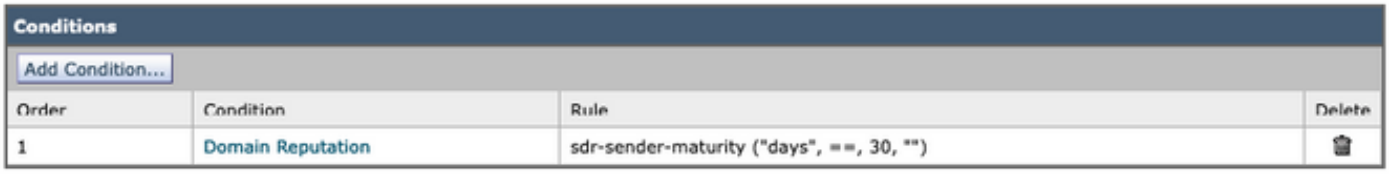
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat 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
```

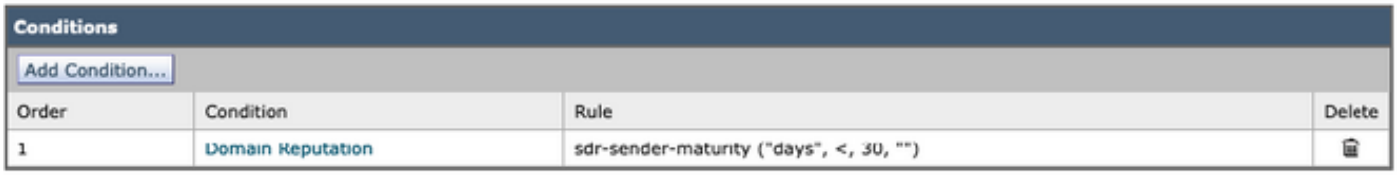
```
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain:
cisco.com
Info: MID 11 SDR: Tracker Header :
629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOtRVhrhSJWgCv2NjL/JQMsjH5QzZw=
=
```

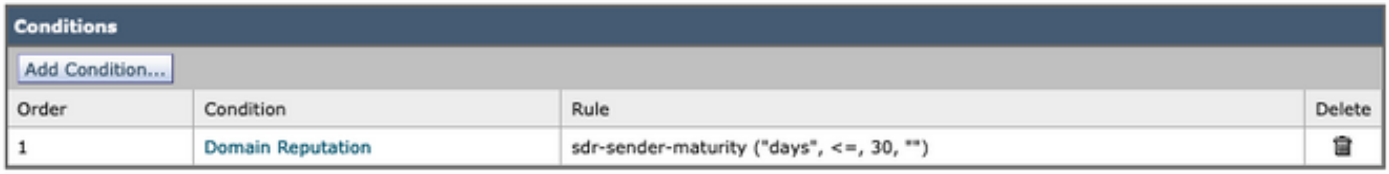
5)グローバル設定で拒否するように設定されたSDRは、ヘッダーからのエンベロープが送信された直後のSMTPカンバセーションのエンベロープフェーズで発生し、他のデータはまだ送信されません。

```
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)「Cisco Bug ID CSCwb32685」および次のField Noticeで説明されているように、予期される動作が原因です。FN72389:Cisco Secure Email Gateway:Talos Domain Age Update：フィルタで次の3つの条件を使用しないでください。less than、equal to、およびless than and equal toの各ポリシーに一致するドメインは、次の図に示すように条件に一致します。







注：送信者の成熟度は30日の制限に設定されており、この制限を超えると、ドメインは電子メール送信者として成熟したと見なされ、詳細は提供されません。

関連情報

Cisco Secure Email AsyncOS 14.2リリースノート

『Cisco Secure Email and Web Manager AsyncOS 14.2 Release notes』

重要なお知らせ：FN72389:Cisco Secure Email Gateway:Talosドメインの有効期間の更新