驗證14.2.0 AsyncOS升級上的發件人域信譽更改

目錄

簡介

本檔案介紹內部部署、虛擬環境(ESA)和雲環境(CES)的安全電子郵件平台上的發件人域信譽(SDR)變更。

問：在SDR AsyncOS 14.2.0上進行了哪些更改？

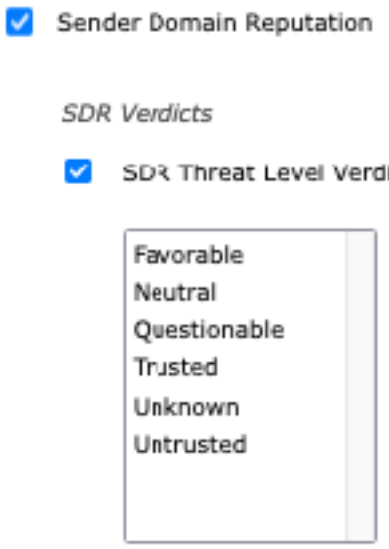
> **警告：在升級到14.2時，會自動更改針對受汙染和/或弱判定的「拒絕」操作的SDR配置。該配置會將ESA SDR配置更改為在中性威脅級別拒絕。**

1)SDR舊版裁決更改當前命**名為**威脅級別的裁決，如下圖所示：

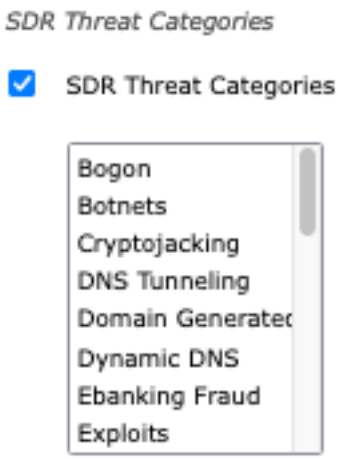
Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **附註**：這是使用不同判定判定判定機制的SDR掃描行為的改變。對於每組發件人資訊，切勿期望判定結果與舊解決方案相匹配。

2)由SDR的高級條件「郵件跟蹤」替換為所示的清單：



3)SDR威脅類**別銀**行欺詐**改為**電子銀行欺詐，如下圖所示：



附註：**所有**「不可信」未列出類別，但SDR類別(如「*垃圾郵件*」、「*惡意*」等)標籤為**Untrusted或Jubble**。

4)mail_logs包含用於SDR裁決的額外日誌行，如果發件人信譽未被拒絕，則在**From** logline之後寫入該日誌。第二行SDR顯示在郵件日誌中。

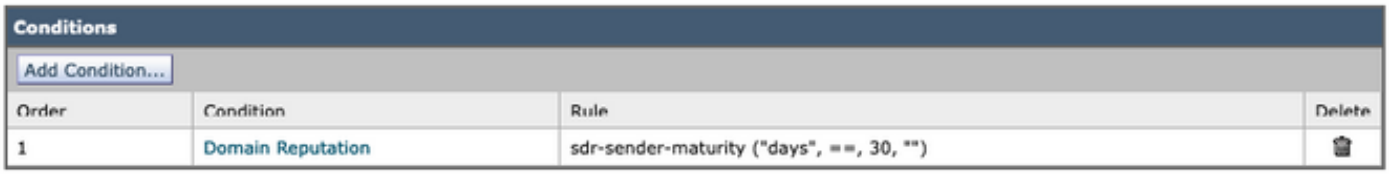
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat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

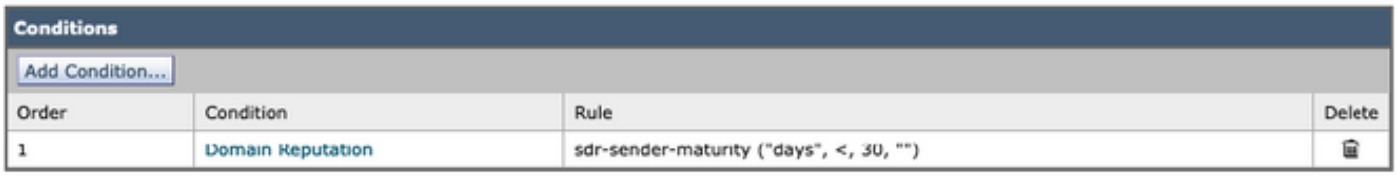
=

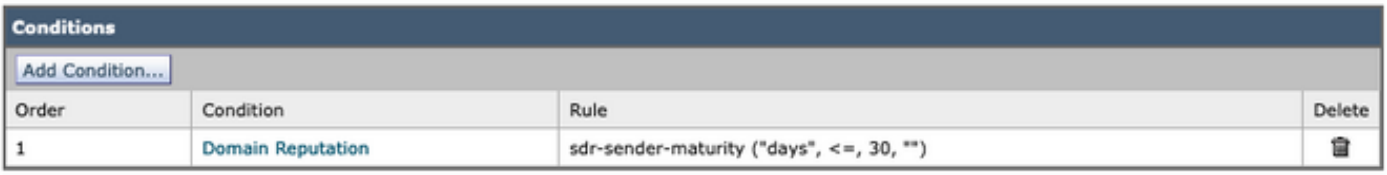
5)在全域性設定中配置為拒絕的SDR發生在SMTP會話的信封階段，該階段正好在傳送來自報頭的信封之後，並且還沒有傳送其他資料。

```
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)由於「Cisco bug ID CSCwb32685」上提供的預期行為，以及此處的現場通知：FN - 72389 — 思科安全電子郵件網關：Talos域年齡更新,不得使用過濾器中的三個條件：**小於**、**等於**和**小於等於**，否則命中一個或多個策略的所有域都匹配條件，如下圖所示：







> **注意**：發件人成熟度設定為30天的限制，超過此限制後，域被視為電子郵件發件人成熟，但未提供進一步詳細資訊。

相關資訊

Cisco Secure Email AsyncOS 14.2版本說明。

Cisco Secure Email and Web Manager AsyncOS 14.2版本說明。

公告：FN - 72389 — 思科安全電子郵件網關：Talos域期限更新