验证14.2.0 AsyncOS升级上的发件人域信誉更改

目录

简介

本文档介绍在内部、虚拟环境(ESA)和云环境(CES)的安全邮件平台上对发件人域信誉(SDR)的更改。

问：对SDR AsyncOS 14.2.0进行了哪些更改？

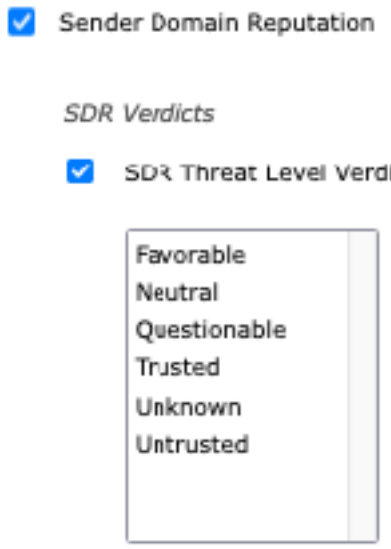
> **警告：升级到14.2时，对受污染和/或弱判定的拒绝操作的SDR配置将自动更改。该配置将ESA SDR配置更改为在中性威胁级别拒绝。**

1)现在名为Threat Levels的SDR传统判定更改，如图所示：

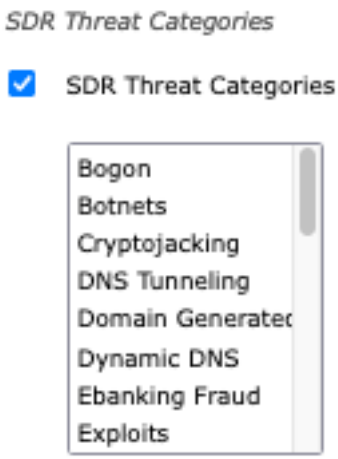
Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **注意**：这是SDR扫描行为的变化，其判定决策机制不同。您不能期望裁决与每组发件人信息的旧解决方案相匹配。

2)将SDR的高级条件“消息跟踪”替换为如下列表：



3)SDR威胁类别银行**欺诈**变为电子**银行**欺诈，如图所示：



注意：所有不可信(Untrusted)都没有列出类别，但SDR类别(如“*spam*”、“*malicio*”等)被标记为“不可信”(Untrusted)或“*Possible*)。

4)mail_logs包含SDR判定的附加日志行，如果发件人信誉未被拒绝，则**在**From logline后写入该日志行。邮件日志中显示第二个SDR行。

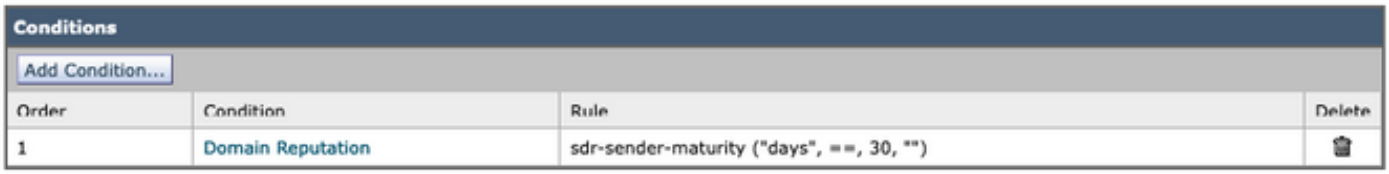
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat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

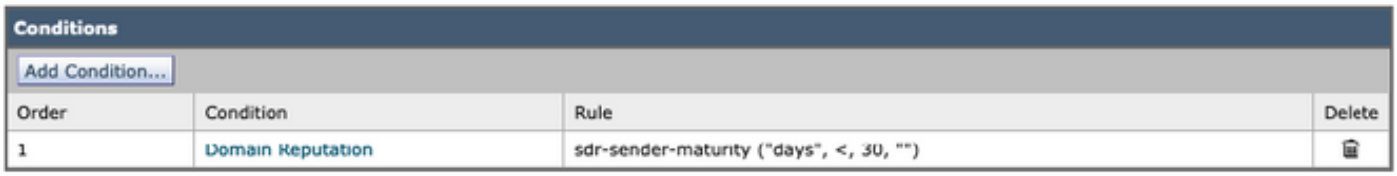
=

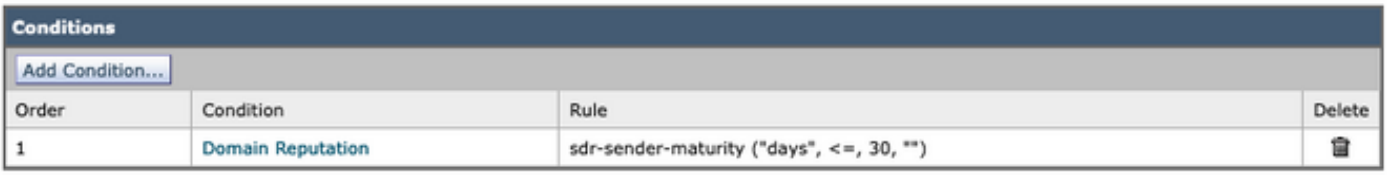
5)在全局设置中配置为拒绝的SDR发生在SMTP会话的信封阶段，该阶段恰好在从信头发送信封之后，且尚未发送任何其他数据。

```
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)由于“Cisco Bug ID CSCwb32685”和此处的“Field Notice”中所述的预[期行为，](#)请注意[:FN - 72389 — 思科安全电子邮件网关：Talos域年龄更](#)新不得在过滤器中使用以下三种条件：**小于**、**等于**和小于**等于**，否则，命中策略或策略的所有域都匹配条件，如图所示：







> **注意**：发件人成熟度设置为30天的限制，超过此限制，域被视为电子邮件发件人的成熟域，不提供进一步的详细信息。

相关信息

[思科安全邮件AsyncOS 14.2版本说明。](#)

[思科安全电邮和Web Manager AsyncOS 14.2版本说明。](#)

[Field Notice：FN - 72389 — 思科安全电子邮件网关：Talos域年龄更新](#)