Überprüfung der Änderung der Absenderdomänenreputation für das AsyncOS-Upgrade 14.2.0

Inhalt

Einleitung

Dieses Dokument beschreibt die Änderungen in für Sender Domain Reputation (SDR) auf der Secure E-Mail-Plattform für die lokale, virtuelle Umgebung (ESA) und Cloud-Umgebung (CES).

Frage: Welche Änderungen werden an SDR AsyncOS 14.2.0 vorgenommen?

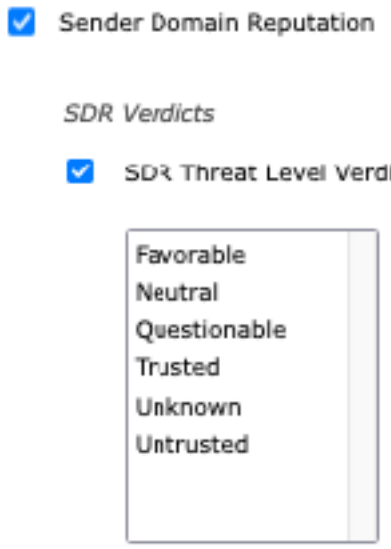
> **Warnung: Die SDR-Konfigurationen der Ablehnungsaktion für Angehobene und/oder schwache Verdicts werden beim Upgrade auf 14.2 automatisch geändert. Die Konfiguration ändert die ESA SDR-Konfiguration so, dass sie auf Ebene der neutralen Bedrohungen abgelehnt wird.**

1) Änderungen von Verdicts-Verdicts in SDR, die jetzt als **Bedrohungsstufen** bezeichnet werden, wie im Bild gezeigt:

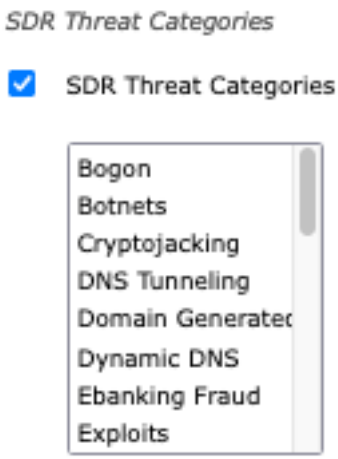
Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **Anmerkung:** Dies ist eine Änderung des SDR-Scan-Verhaltens mit einem anderen Entscheidungsmechanismus. Sie dürfen nicht erwarten, dass das Urteil mit der alten Lösung für alle Absenderinformationen übereinstimmt.

2) "Nachrichtenverfolgung" durch den erweiterten Zustand von SDR wird durch die angezeigte Liste ersetzt:



3) SZR-Gefahrenkategorie "**Bankbetrug"** wird zu "**Bankbetrug"** geändert, wie im Bild gezeigt:



Anmerkung: Alle nicht vertrauenswürdigen Personen haben keine Kategorie aufgelistet, jedoch werden SDR-Kategorien wie "*Spam*," "*bösartig*" usw. als **nicht vertrauenswürdig** oder **fraglich** gekennzeichnet.

4) mail_logs enthält eine zusätzliche Protokollzeile für SDR-Verdicts, wird sie nach **From** logline geschrieben, wenn die Reputation des Absenders nicht abgelehnt wird. Eine zweite SDR-Zeile wird in den Mail-Protokollen angezeigt.

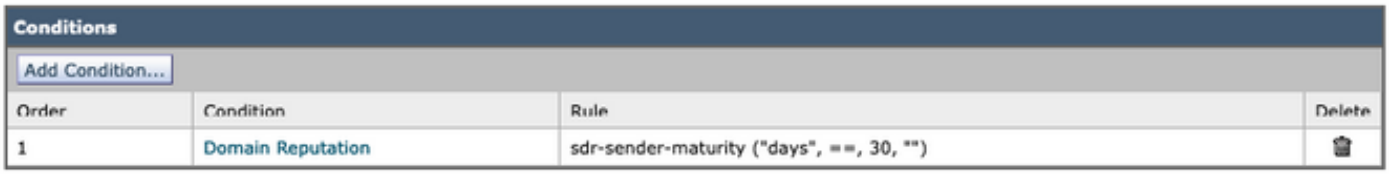
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat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

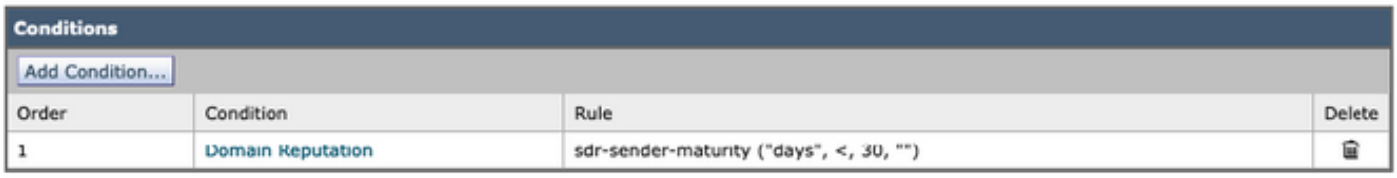
```
cisco.com
Info: MID 11 SDR: Tracker Header :
629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOtRVhrhSJWgCv2NjL/JQMsjH5QzZw=
=
```

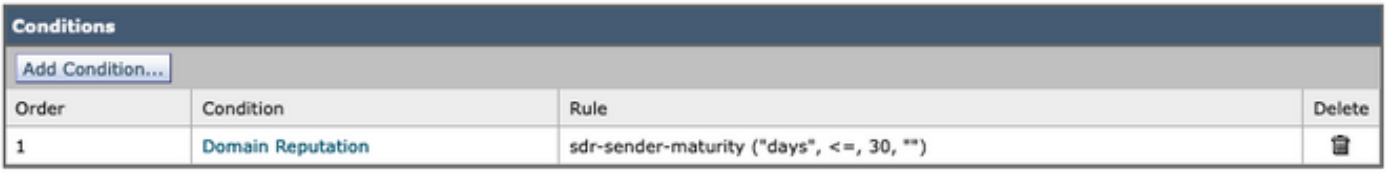
5) SDR, der für die Ablehnung in den globalen Einstellungen konfiguriert wurde, wird in der Umschlagphase der SMTP-Konversation ausgeführt, die unmittelbar nach dem Senden des Umschlags aus dem Header erfolgt und noch keine weiteren Daten gesendet werden.

```
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) Aufgrund des erwarteten Verhaltens, wie unter "Cisco Bug ID CSCwb32685" und hier Problemhinweis erläutert: FN - 72389 - Cisco Secure Email Gateway: Talos Domain Age Update Sie dürfen die drei Bedingungen in Ihren Filtern nicht verwenden: **kleiner als**, **gleich** und **kleiner als und gleich**, ansonsten stimmen alle Domänen, die die Richtlinie oder Richtlinien treffen, mit den Bedingungen überein, wie im Bild gezeigt:







> **Hinweis**: Die Absenderreife ist auf eine Obergrenze von 30 Tagen begrenzt. Eine Domäne gilt als reif für E-Mail-Absender, und es werden keine weiteren Details angegeben.

Zugehörige Informationen

Versionshinweise zu Cisco Secure Email AsyncOS 14.2

Versionshinweise für Cisco Secure Email und Web Manager AsyncOS 14.2

Problemhinweis: FN - 72389 - Cisco Secure Email Gateway: Aktualisierung des Talos-Domänenzeitalters