Controleer de wijziging in de bestandsindeling voor het verzendende domein op 14.2.0 AsyncOS-upgrade

Inhoud

Inleiding

In dit document worden de wijzigingen beschreven in Sender Domain Reputation (SDR) op het Secure Email Platform (Secure Email Platform) voor een virtuele omgeving (ESA) en een cloudomgeving (CES).

Q. Wat zijn de wijzigingen die zijn aangebracht op SDR AsyncOS 14.2.0?

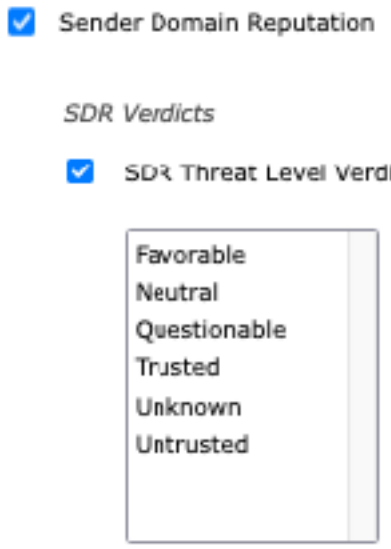
> **Waarschuwing**: **SDR-configuraties van afstotingen voor gestreden en/of zwakke vonnissen worden automatisch na een upgrade gewijzigd naar 14.2. De configuratie verandert de ESR-configuratie om deze op een neutraal Threat-niveau af te wijzen.**

1) SDR Verouderde beschikkingen tot wijziging van vonnissen die nu **bedreigingsniveaus** zijn genoemd, zoals in de afbeelding:

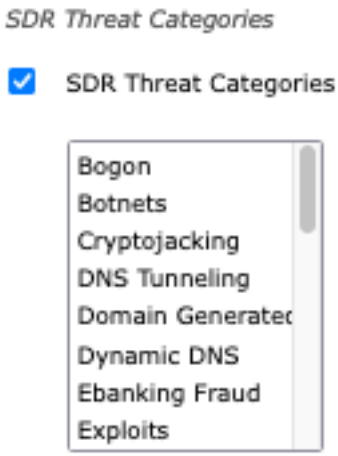
Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **Opmerking:** Dit is een verandering in SDR scangedrag met een ander beslissingsmechanisme. U mag niet verwachten dat het vonnis overeenkomt met de oude oplossing voor elke verzameling senderinformatie.

2) "Berichttracering" door de geavanceerde conditie van SDR wordt vervangen door de lijst die wordt weergegeven:



3) SDR. Threat Category **Banking Fraud** wordt veranderd in **Ebanking Fraud**, zoals getoond in de afbeelding:



Opmerking: Alle onvertrouwde categorieën zijn niet in de lijst opgenomen, maar SDR-categorieën zoals '*spam*', '*kwaadaardig*', enzovoort, worden aangeduid als **onbetrouwbaar** of **twijfelachtig**.

4) mail_logs bevat een extra loglijn voor SDR-vonnissen, deze wordt geschreven na **From** logline als de afzenders reputatie niet wordt verworpen. Er verschijnt een tweede SDR-regel in de maillogs.

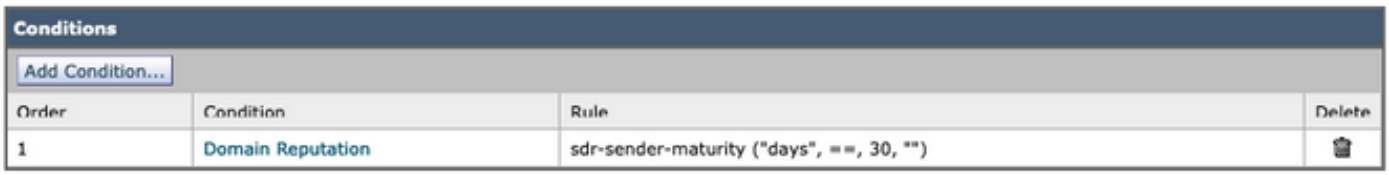
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat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

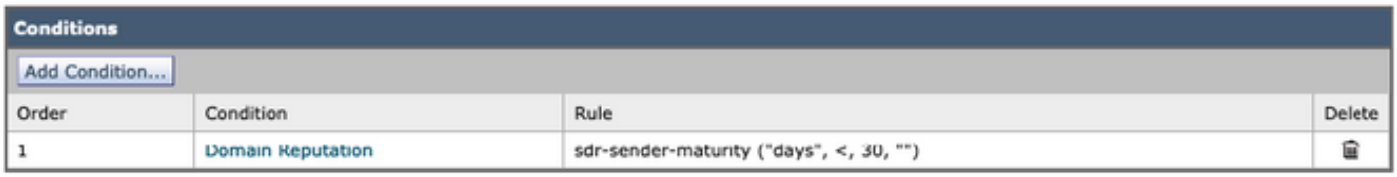
```
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain:
cisco.com
Info: MID 11 SDR: Tracker Header :
629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOtRVhrhSJWgCv2NjL/JQMsjH5QzZw=
=
```

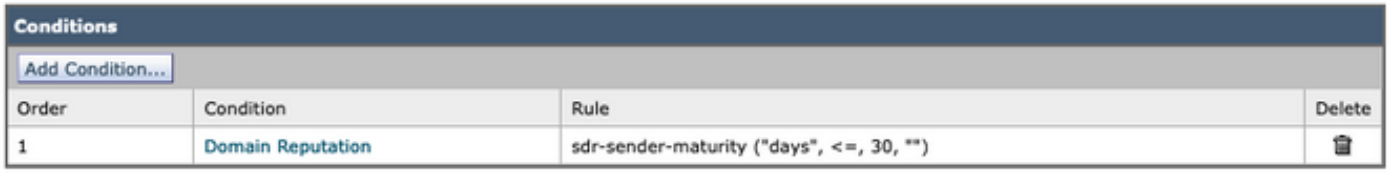
5) SDR, ingesteld om in de mondiale instellingen af te wijzen, vindt plaats in de envelopfase van het gesprek dat is net nadat de envelop van de kop wordt verstuurd en er nog geen andere gegevens worden verstuurd.

```
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) Vanwege het verwachte gedrag zoals uitgelegd op 'Cisco bug ID CSCwb32685' en hier melding uit het veld: FN - 72389 - Cisco beveiligde e-mailgateway: Talos Domain Age Update u moet de drie voorwaarden in uw filters niet gebruiken: **minder dan**, **gelijk aan**, en **minder dan en gelijk aan** , anders voldoen alle domeinen die het beleid of beleid beïnvloeden aan de voorwaarden, zoals getoond in de afbeelding:







> **Opmerking**: Verzendtermijn is vastgesteld op 30 dagen en buiten deze limiet wordt een domein beschouwd als volgroeid als e-mailverzender en er worden geen verdere details verstrekt.

Gerelateerde informatie

Cisco Secure E-mail asynchrone/synchrone OS 14.2 release-opmerkingen

Cisco Secure E-mail en Web Manager AsyncOS 14.2 release-opmerkingen

Field Notice: FN - 72389 - Cisco beveiligde e-mailgateway: Talos Domain Age Update