Verifica della modifica della reputazione del dominio mittente all'aggiornamento AsyncOS 14.2.0

Sommario

Introduzione

Questo documento descrive le modifiche in per Sender Domain Reputation (SDR) sulla piattaforma Secure Email per ambienti locali, virtuali (ESA) e cloud.

D. Quali sono le modifiche apportate a SDR AsyncOS 14.2.0?

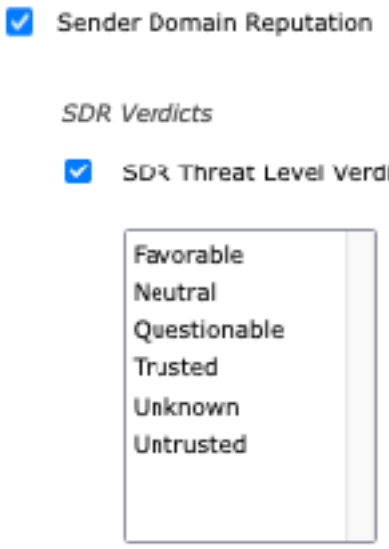
> **Avviso: Le configurazioni SDR dell'azione Rifiuta per Verdetti con e/o deboli modifiche vengono automaticamente modificate al momento dell'aggiornamento alla versione 14.2. La configurazione dell'SDR ESA viene modificata in Rifiuta a livello di minaccia neutra.**

1) I Verdetti Legacy SDR cambiano i verdetti ora chiamati **Livelli di Minaccia**, come mostrato nell'immagine:

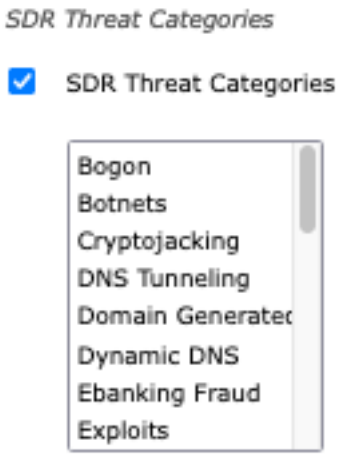
Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **Nota:** Si tratta di un cambiamento nel comportamento di scansione dei DSP con un meccanismo di decisione del verdetto diverso. Non devi aspettarti che il verdetto corrisponda alla vecchia soluzione per ogni set di informazioni sul mittente.

2) "Message Tracking" (Verifica messaggi) con la condizione avanzata di SDR è sostituita dall'elenco seguente:



3) La categoria di rischio SDR **Frode bancaria** è stata modificata in **Frode bancaria**, come mostrato nell'immagine:



Nota: Per tutti gli elementi non attendibili non è elencata una categoria, tuttavia le categorie SDR, ad esempio *spam*, *dannoso* e così via, sono contrassegnate come **non attendibili** o **discutibili**.

4) mail_logs contiene una riga di registro aggiuntiva per i verdetti SDR, viene scritta dopo **From** logline se la reputazione dei mittenti non viene rifiutata. Nei log di posta viene visualizzata una seconda riga SDR.

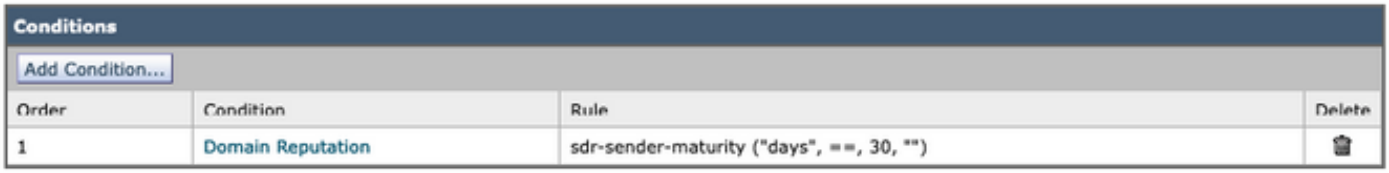
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat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

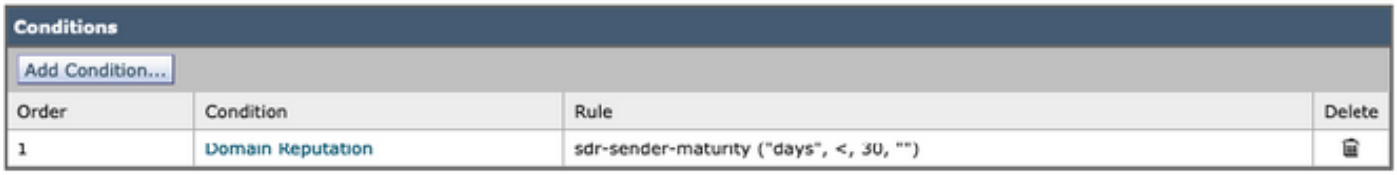
```
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain:
cisco.com
Info: MID 11 SDR: Tracker Header :
629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOtRVhrhSJWgCv2NjL/JQMsjH5QzZw=
=
```

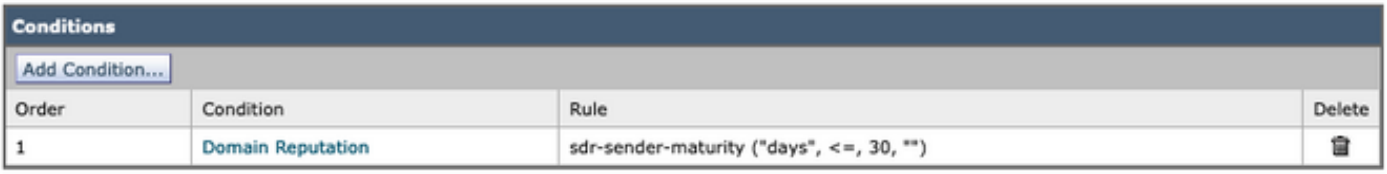
5) SDR configurato per il rifiuto nelle impostazioni globali si verifica nella fase envelope della conversazione SMTP che si trova subito dopo l'invio della busta dall'intestazione e nessun altro dato è ancora stato inviato.

```
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) A causa del comportamento previsto, descritto nel documento "Cisco bug ID CSCwb32685" e qui la notifica sul campo: FN - 72389 - Cisco Secure Email Gateway: Aggiornamento età dominio talos non utilizzare le tre condizioni nei filtri: **minore**, **uguale a**, **minore e uguale a**, altrimenti tutti i domini interessati dal criterio o dai criteri soddisfano le condizioni, come mostrato nell'immagine:







> **Nota**: la scadenza del mittente è impostata su un limite di 30 giorni e oltre questo limite, un dominio è considerato maturo come mittente di posta elettronica e non vengono forniti ulteriori dettagli.

Informazioni correlate

Note sulla release di Cisco Secure Email AsyncOS 14.2.

Note sulla release di Cisco Secure Email e Web Manager AsyncOS 14.2.

Field Notice: FN - 72389 - Cisco Secure Email Gateway: Aggiornamento età dominio Talos