

Vérifier la modification de la réputation de domaine de l'expéditeur lors de la mise à niveau AsyncOS 14.2.0

Table des matières

[Introduction](#)


[Q. Quelles sont les modifications apportées à SDR AsyncOS 14.2.0 ?](#)

[Informations connexes](#)

Introduction


Ce document décrit les modifications apportées à pour Sender Domain Reputation (SDR) sur la plate-forme de messagerie sécurisée pour les environnements sur site, virtuels (ESA) et cloud (CES).

Q. Quelles sont les modifications apportées à SDR AsyncOS 14.2.0 ?

 Avertissement : les configurations SDR de l'action Reject pour les verdicts Tainted et/ou Weak sont automatiquement modifiées lors de la mise à niveau vers 14.2. La configuration modifie la configuration du SDR ESA pour qu'elle soit rejetée au niveau de menace neutre.

1) Verdicts hérités SDR changement de verdicts maintenant nommés niveaux de menace, comme le montre l'image :

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

 Remarque : il s'agit d'un changement dans le comportement de balayage SDR avec un mécanisme de décision de verdict différent. Vous ne devez pas vous attendre à ce que le verdict corresponde à l'ancienne solution pour chaque ensemble d'informations d'expéditeur.

2) « Suivi des messages » par la condition avancée de SDR est remplacé par la liste ci-dessous :

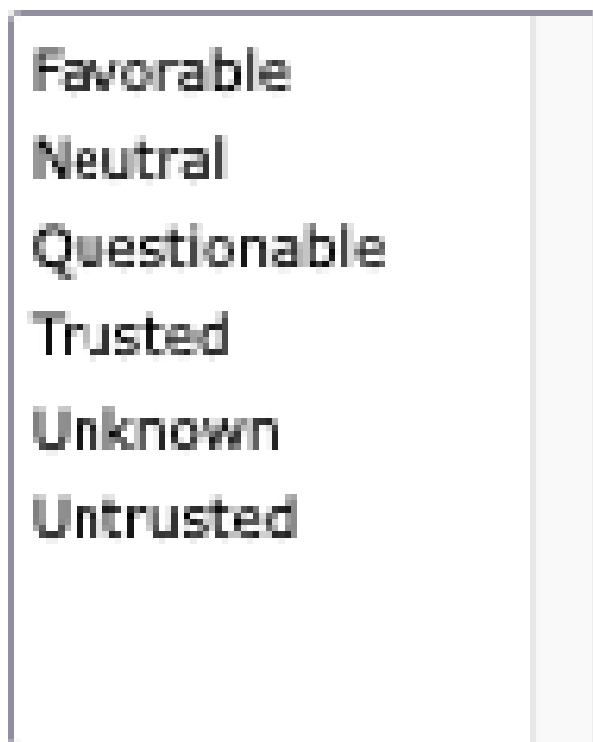


Sender Domain Reputation

SDR Verdicts



SDR Threat Level Verdicts

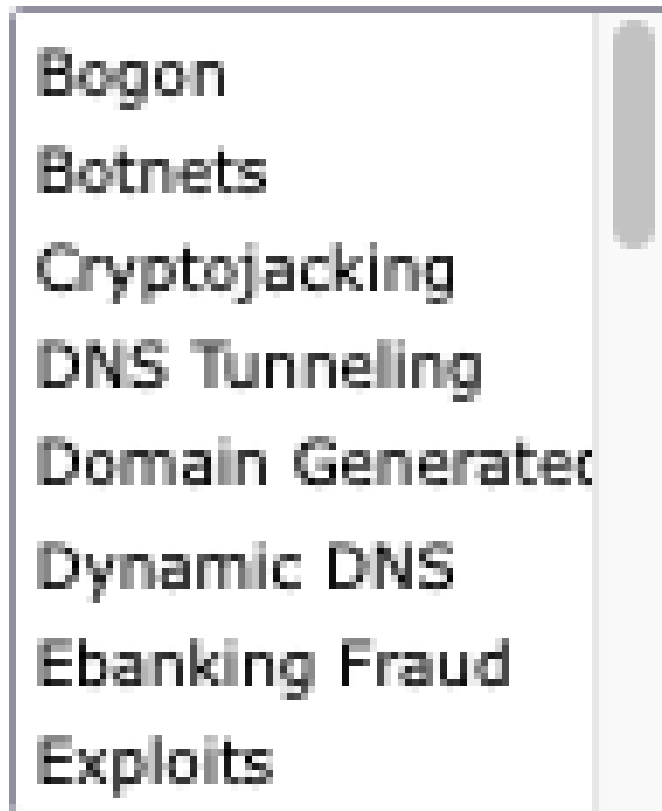



3) Catégorie de menace DTS Fraude bancaire est remplacé par Ebanking Fraud, comme le montre l'image :

SDR Threat Categories



SDR Threat Categories



 Remarque : Toutes les catégories non approuvées ne sont pas répertoriées, mais les catégories SDR telles que « spam », « malveillant », etc., sont signalées comme étant non approuvées ou douteuses.

4) mail_logs contient une ligne de journal supplémentaire pour les verdicts SDR, elle est écrite après la connexion From si la réputation de l'expéditeur n'est pas rejetée. Une deuxième ligne SDR apparaît dans les journaux de messagerie.

<#root>

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:

Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s):

Info: MID 11 ICID 19884 RID 0 To: test@cisco.com
Info: MID 11 Message-ID 'op.1m7bljrr8qfre9@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:

Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s)
Info: MID 11 SDR: Tracker Header : 629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc730fsh9YLwqvKidy3M/WEb0fkQpw00t

5) SDR configuré pour rejeter dans les paramètres globaux se produit à la phase d'enveloppe de la conversation SMTP qui est juste après l'envoi de l'enveloppe de l'en-tête et aucune autre donnée n'est encore envoyée.

<#root>

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
Info: MID 9364

SDR: Consolidated Sender Threat Level: Untrusted, Threat Category: N/A, Suspected Domain(s) : lana.cf. S

Info: MID 9364 ICID 79 Receiving Failed: Message rejected by Sender Domain Reputation engine
Info: MID 9364 SDR: Tracker Header : 629d5de5_JxmxzLXzbSob4h6Tqmxj2QFeN6eeb3J8CJ2zj9h8XgF/+e0YQVxd051nV
Info: MID 9364

Subject ""

Info:


Message aborted MID 9364 Receiving aborted


Info: Message finished MID 9364 aborted

6) En raison du comportement attendu expliqué comme indiqué sur « ID de bogue Cisco CSCwb32685 » et ici Avis de champ : FN - 72389 - Cisco Secure Email Gateway : Talos Domain Age Update vous ne devez pas utiliser les trois conditions dans vos filtres : inférieur, égal à, et inférieur et égal à, sinon tous les domaines qui correspondent à la politique ou aux politiques correspondent aux conditions, comme indiqué dans l'image :

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	Domain Reputation	sdr-sender-maturity ("days", "=", 30, "")	

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	Domain Reputation	sdr-sender-maturity ("days", "<", 30, "")	

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	Domain Reputation	sdr-sender-maturity ("days", <=, 30, "")	

 Remarque : la maturité de l'expéditeur est limitée à 30 jours. Au-delà de cette limite, un domaine est considéré comme arrivé à maturité en tant qu'expéditeur d'e-mail et aucun autre détail n'est fourni.

Informations connexes

[Notes de version de Cisco Secure Email AsyncOS 14.2.](#)

[Notes de version de Cisco Secure Email and Web Manager AsyncOS 14.2.](#)

[Avis de champ : FN - 72389 - Cisco Secure Email Gateway : mise à jour de l'âge du domaine Talos](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.