Konfiguration der Absenderdomänenreputation für die ESA-AKTUALISIERUNG (April 2024)

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Überblick
- Konfigurieren
  - Domänenreputationsdienst-WebUI aktivieren
  - Domänenausnahmeliste
    - Erstellen einer Adressliste
    - Adressliste auf die globale SDR-Domänenausnahmeliste anwenden
    - Adressliste auf Content-/Nachrichtenfilter anwenden
    - Nachrichtenfilter
  - Erstellen eines Content-Filters zum Ausführen von Maßnahmen für das SDR-Verdict
  - Konfigurieren von SDR mithilfe von Nachrichtenfiltern
- Überprüfung
- Fehlerbehebung
  - Wichtiges Update für AsyncOS-Versionen nach 14
- Zugehörige Informationen

Einleitung

In diesem Dokument wird die SDR-Konfiguration (Sender Domain Reputation) für die E-Mail Security Appliance (ESA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ESA-Konzepte
- ESA-Konfiguration

- Allgemeine Kenntnisse der Funktionen/Merkmale der SEG, einschließlich; Mail Flow-Richtlinien, Nachrichtenfilter, Content-Filter, globale Domänenreputation.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AsyncOS für ESA 14.2 und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

1. SDR wurde als zusätzlicher Dienst zur Verbesserung der Spam-Phishing-Erkennung entwickelt.

2. SDR erfasst mehrere Header-Werte und lädt sie auf Talos Threat Intelligence Server hoch, wo die riesigen Talos-Ressourcen ein Urteil für jede Nachricht auf abgestufter Skala bestimmen.

3. Die in der Entscheidung enthaltenen Header-Werte sind:

- Umschlag von
- Von
- Antwort an
- DMAR-, DKIM- und SPF-Verifizierung (falls konfiguriert).
- Der (Benutzername-)Wert der E-Mail-Adresse wird optional aus den Headern "Von", "Umschlag von" und "Antwort an" übermittelt.
- Absender-IP
- Zeigt den Namen in den Headern "Von" und "Antwort an" an.

5. Die SDR-Suche wird für alle eingehenden Nachrichten durchgeführt.

6. Der SDR-Scan erfolgt unmittelbar nach der Annahme einer Nachricht durch das Simple Mail Transfer Protocol (SMTP).

7. Die SDR-Aktion kann in der anfänglichen Mail Flow Policy-Phase sowie bei den Optionen "Message Filter" und "Content Filter" ausgeführt werden.

8. Zu den konfigurierten Komponenten gehören:

- Domänenreputations-Dienst aktivieren
- Domänenausnahmelisten (optional)
    - Domänenausnahmeliste (global)
    - Domänenausnahmeliste, die nachrichten-/inhaltsfilterspezifisch verwendet.
    - Globale Aktion mit Domänenreparatur mithilfe von Mail Flow-Richtlinien.
    - Globale Aktion mit Domänenreputation, die auf SMTP-Konversationsebene Maßnahmen ergreift.
- Nachrichtenfilter oder Content-Filter

Konfigurieren

Domänenreputationsdienst-WebUI aktivieren

SDR kann entweder über die WebUI oder die CLI-Schnittstellen aktiviert werden.

WebUI:

1. Navigieren Sie zu Mail Security Services > Domain Reputation > Enable.

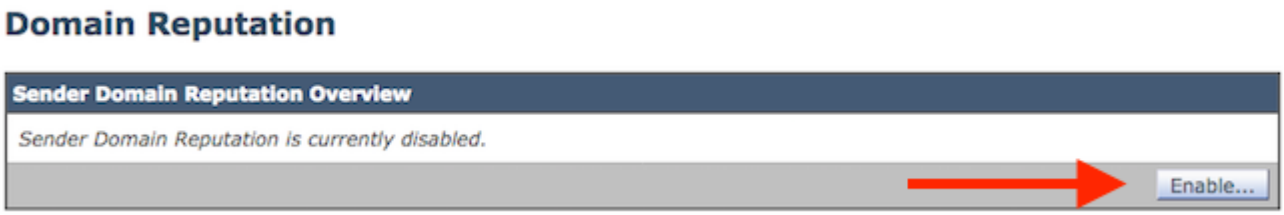
2. Klicken Sie auf das Kästchen neben Sender Domain Reputation Filtering aktivieren.

3. Aktivieren Sie dieses Kontrollkästchen Zusätzliche Attribute einbeziehen: (Optional), wenn Sie den optionalen Header-Wert in die überprüften Daten einbeziehen möchten, um die Effizienz zu verbessern. Klicken Sie auf ? zu lernen.

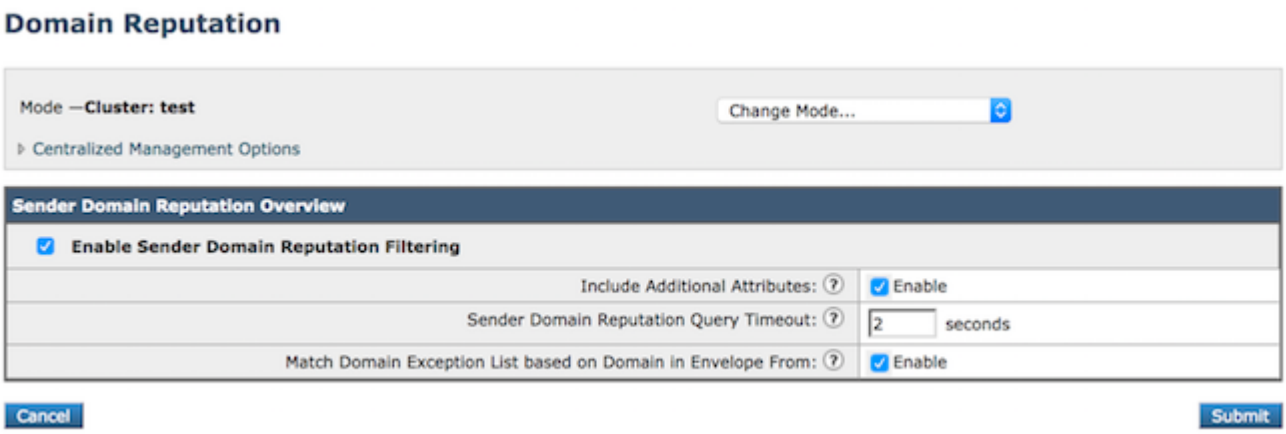
4. Aktivieren Sie dieses Kontrollkästchen Timeout für Absenderdomänenreputationsabfrage. Klicken Sie auf ? zu lernen.

5. Wählen Sie Domänenausnahmeliste basierend auf Domäne in Umschlag von - Aktiviert zuordnen.

6. Klicken Sie auf Senden > Übernehmen, wie in der Abbildung dargestellt.



Absender-Dienst (Domänenreputation)



Sicherheitsdienste > Domänenreputation

Domänenausnahmeliste

1. Die Domänenausnahmeliste kann die Absender-Domänenreputations-Suche für den eingehenden E-Mail-Fluss umgehen.

2. Die Domänenausnahmeliste kann an verschiedenen Standorten angewendet werden, um den E-Mail-Verkehr zu beeinflussen.

3. Die Anwendung Global kann auf alle gescannten E-Mails angewendet werden.

4. Die detailliertere Anwendung in Content-/Nachrichtenfiltern kann sich nur auf einen oder mehrere konfigurierte Filter auswirken.

5. Die Domänenausnahmeliste bietet zwei Optionen, um sowohl eine einfache als auch eine sicherere Option bereitzustellen.

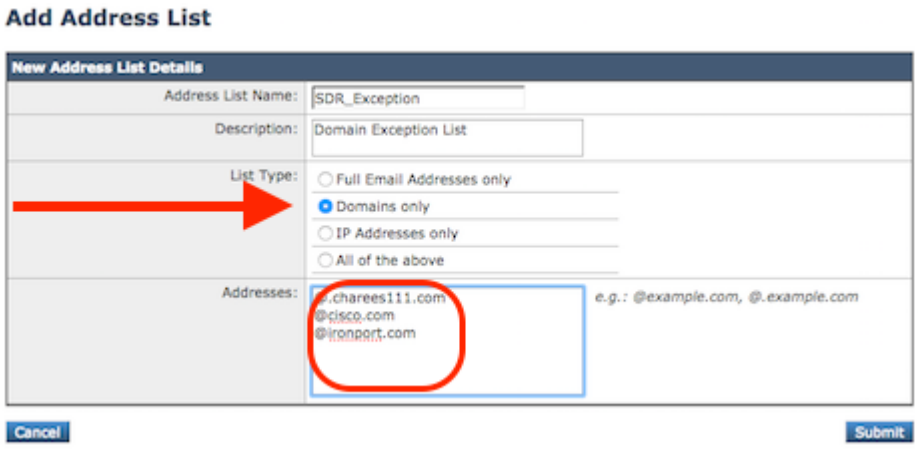
6. In diesem Dokument werden die Optionen beschrieben, mit denen SDR für eine Nachricht, die die Domänenausnahmeliste verwendet, erfolgreich umgangen werden kann.

7. Anforderungen an Domänenausnahmelisten

Erstellen einer Adressliste

1. Navigieren Sie zu Mail-Policys > Adressliste > Adressliste hinzufügen > Name > Beschreibung > Listentyp: Nur Domänen.

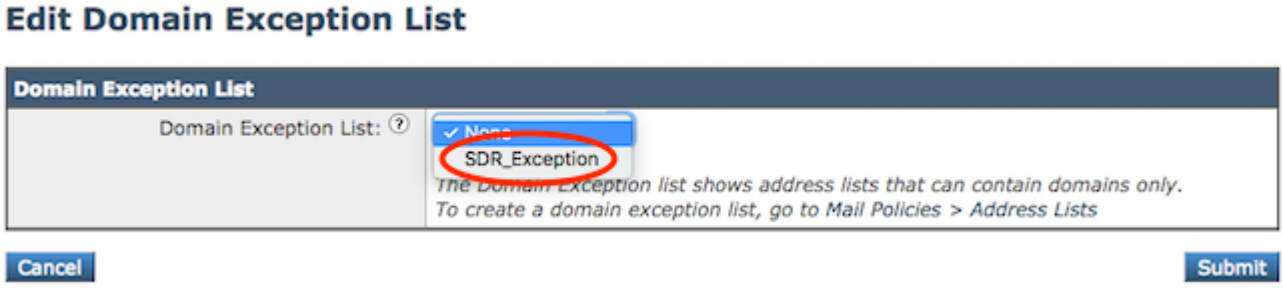
2. Fügen Sie jeden Domänennamen mit der Kommagetrennung hinzu.
3. Klicken Sie auf Senden und Änderungen bestätigen, wie im Bild dargestellt.



Adressliste, die auf die Domänenausnahmeliste angewendet werden soll

Adressliste auf die globale SDR-Domänenausnahmeliste anwenden

1. Navigieren Sie zu Security Services > Domain Reputation > Domain Exception List > Edit Settings > Domain Exception List (wählen Sie Ihre Liste aus).
2. Klicken Sie auf Senden und Änderungen bestätigen, wie im Bild dargestellt.



Wählen Sie aus dem Dropdown-Menü eine Adressliste aus.

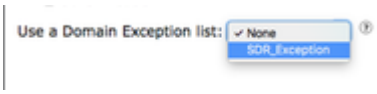
Adressliste auf Content-/Nachrichtenfilter anwenden

Filter für eingehende Inhalte:

1. Navigieren Sie zu Bedingung > URL-Reputation > Option für Bedrohungs-Feeds.

2. Reputation der Bedingungsdomäne

3. Klicken Sie hier:



Die Domänenausnahmeliste lässt Aktionen pro Richtlinie zu.

Nachrichtenfilter

Die Domänenausnahmelistenanwendung in Nachrichtenfiltern wäre als Option in einer Bedingung enthalten.

Anmerkung: Diese Beispiele enthalten die domain_exception_list als Teil der gesamten Bedingung.

---

1. sdr-reputation (['furchtbar', 'arm', 'befleckt', 'schwach', 'unbekannt', 'neutral', 'gut'], domain_exception_list)
2. sdr-age ("days", <, 5, domain_exception_list)
3. sdr-unscannable (domain_exception_list)

Eine ausführlichere Erläuterung und Beispiele der Anwendung für Nachrichtenfilter finden Sie in den ESA-Benutzerhandbüchern unter den Überschriften:

- Domänenreputations-Regel für ETF
- Filtern von Nachrichten auf Basis der Absenderdomänenreputation, die den Nachrichtenfilter verwendet

Erstellen eines Content-Filters zum Ausführen von Maßnahmen für das SDR-Verdict

1. SDR ist nur für den eingehenden Mail-Fluss aktiviert.
2. Name der SDR-Bedingung: Domänenreputation.
3. Sie können mehrere Bedingungen erstellen, um verschiedene Ergebnisse zu kombinieren.
4. Die Domänenreputationsbedingung enthält 2 verschiedene Prüfungen, die jeweils mehrere Optionen enthalten:

- Absenderdomänenreputation
  - Reputations-Verdict der Absenderdomäne
  - Alter der Absenderdomäne

    - Absenderdomänenreputation nicht durchsuchbar
- Feeds zu externen Bedrohungen
    - Ermöglicht die Verwendung der heruntergeladenen Inhaltslisten der Bedrohungs-Feeds, um nach denselben Domänen-Headern zu suchen, die für SDR gesammelt wurden.

✎ Anmerkung: Diese Optionen in der Domänenreputationsbedingung können sich visuell ändern, je nachdem, welche Optionen für die jeweilige Auswahl verfügbar sind.

---

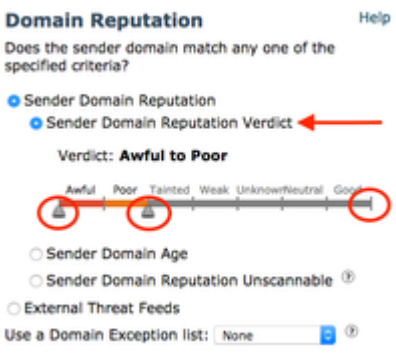
5. Die letzte Option in der Domänenreputationsbedingung ist die Domänenausnahmeliste.

6. Die Funktion Domain Exception List (Domänenausnahmeliste), die einer Adressliste zugeordnet ist, erweitert die Kontrolle über die Anwendung der Aktion, indem die Liste auf die detailliertere Mail Policy Level der Nachrichtenverarbeitung angewendet wird.

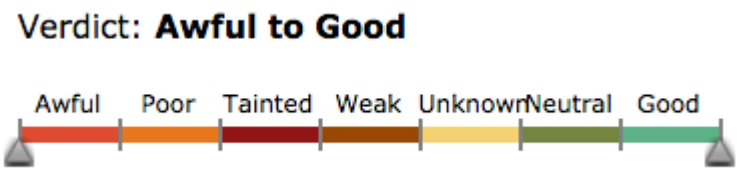
7. Navigieren Sie zu Mail Policy > Incoming Content Filters > Add Filter > Add Condition > Domain Reputation.

8. Bedingung 1: Reputations-Verdict der Absenderdomäne

- Scheußlich, arm, gehackt, schwach, unbekannt, neutral, gut
- Enthält gleitende dreieckige Markierungen, um den Bereich auszuwählen, den Sie anpassen möchten.
- Die Werte Schrecklich und Schlecht sind die empfohlenen Werte, um Maßnahmen zu ergreifen.
- Die Nachrichten, die mit "Schrecklich" und "Schlecht" übereinstimmen, können eine zusätzliche Kategorie, einen zusätzlichen Wert, wie z. B. Spam oder Malicious, aufweisen, die in der Nachrichtenverfolgung angezeigt werden kann.



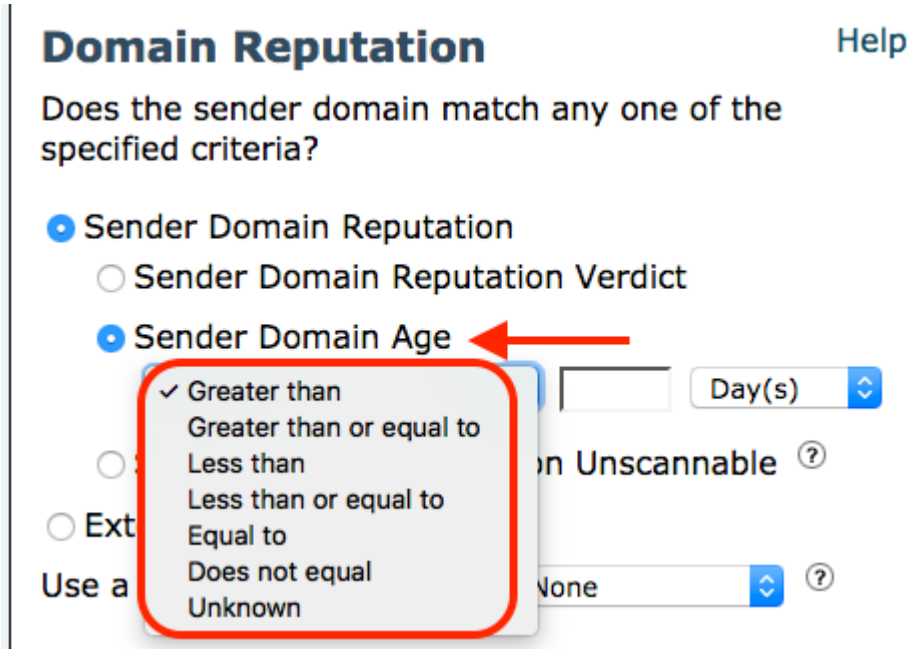
SDR-Verdict-Schieberegler mit einstellbarem Bereich.



Vollständige Ansicht der SDR-Verdict-Folienleiste.

9. Bedingung 2: Absenderdomänenalter.

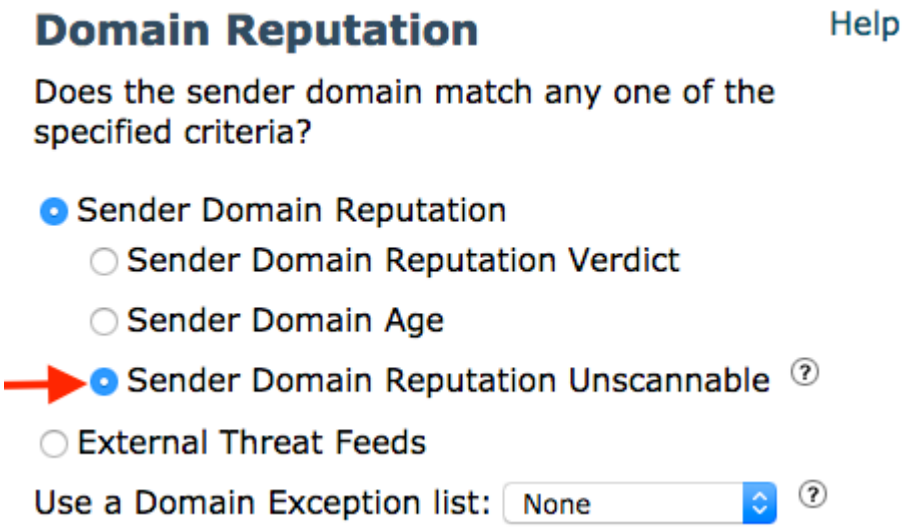
- Das Alter der Domäne kann mit einem höheren Risiko oder einer seit langem bestehenden Zuverlässigkeit in Verbindung gebracht werden.
- Die Möglichkeit einer Domain mit einem Alter von weniger als 10 Tagen kann riskanter sein.



Absenderdomänenalter. Niedrigere Werte bedeuten mehr Risiko.

10. Bedingung 3: Absenderdomänenreputation kann nicht gescannt werden.

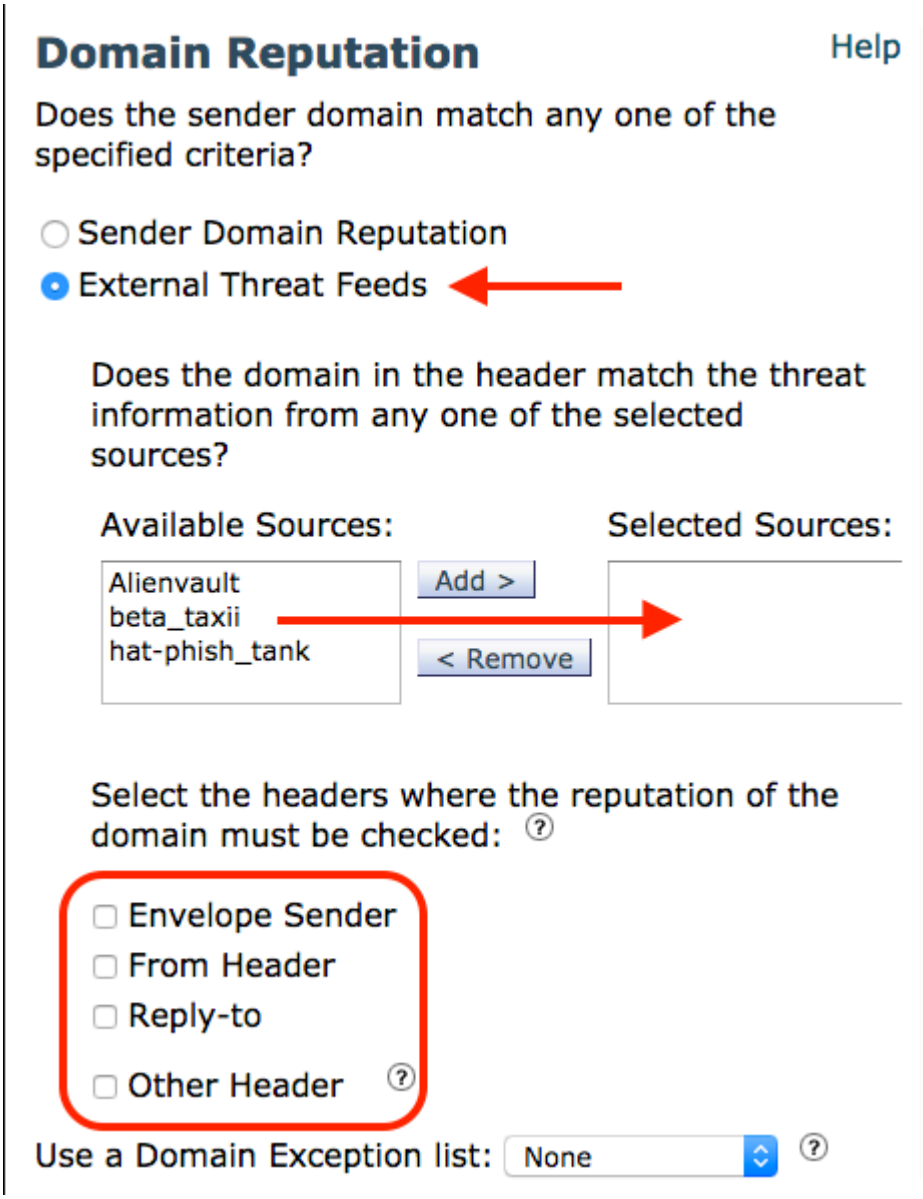
- Bieten Sie Administratoren die Möglichkeit, Maßnahmen zu ergreifen, wenn kein Urteil eingeholt werden kann.



SZR nicht scanbar

11. Bedingung 4: Externe Feeds zu Bedrohungen

- Die in SDR-Scanning enthaltenen Header können auch mit individuell heruntergeladenen STIX/TAXII-Inhalten gescannt werden.
- Die Feeds zu externen Bedrohungen werden hier ausführlicher behandelt. Feeds zu externen Bedrohungen.

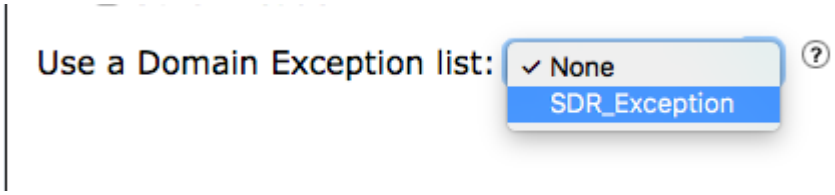


Externe Bedrohungs-Feeds können verwendet werden, um dieselben Header zu durchsuchen, die auch für SDR verwendet werden.

- [Email Security Appliance - Benutzerhandbücher]

12. Bedingung 5: Domänenausnahmeliste verwenden.

- Die Verwendung der Domänenausnahmeliste innerhalb des Inhaltsfilters bietet mehr Kontrolle als die globale Liste.



Die Domänenausnahmeliste lässt Aktionen pro Richtlinie zu.

13. Die Aktion in Verbindung mit diesen Bedingungen kann von minimal bis extrem reichen und es hängt von den gewünschten Ergebnissen des Administrators.

14. Einige der beliebtesten Aktionen sind aufgeführt:

- Quarantäne/In Quarantäne kopieren
- Verwerfen
- Fügen Sie dem Betreff oder Text der Nachricht einen Haftungsausschluss oder eine Warnung hinzu.
- Erstellen Sie einen Protokolleintrag, um ein bestimmtes Wort, einen bestimmten Satz oder einen bestimmten Wert für die Nachrichtenverfolgungsprotokolle zu generieren.

Konfigurieren von SDR mithilfe von Nachrichtenfiltern

1. Die ESA-Benutzerhandbücher eignen sich hervorragend für Syntax, Definitionen und Beispiele von Nachrichtenfiltern.
2. Suchen Sie im Benutzerhandbuch nach dieser Überschrift, um zusätzliche Inhalte für Nachrichtenfilter zu erhalten, die über die hier bereitgestellten Informationen hinausgehen.

- Filtern von Nachrichten basierend auf der Absenderdomänenreputation mit dem Nachrichtenfilter

3. Diese Bedingungen sind mit dem SDR-Nachrichtenfilter verknüpft:

- if sdr-reputation (['awful', 'poor'] >>> Alle Werte hierfür umfassen: Scheußlich, arm, gehackt, schwach, unbekannt, neutral, gut
- if sdr-reputation (['awful', 'poor'], "<domain_exception_list>") >>> Dies beinhaltet die Verwendung einer Domänenausnahmeliste
- if sdr-age (<"unit">, <"operator"> <"actual value">) >> Verweisen Sie auf das Benutzerhandbuch für die Definition des "operators".
    - if (sdr-age ("unknown", "") >> unit = unknown. Die übrigen Werte werden durch "" ersetzt.
    - beispiel: if (sdr-age ("months", <, 1, "")). >> Einheit = Tage, Monate, Jahre. Operator = < (kleiner als). Istwert = 1
- if sdr-unscannable (<'domain_exception_list'>) >> Wie dargestellt, wenn die Meldung zu unscannable führt. In diesem Beispiel wird auch die Bedingung der Domänenausnahmeliste berücksichtigt.
- if (sdr-unscannable ("") >>> In diesem Beispiel ist die Ausnahmeliste nicht enthalten. Der Wert wird ersetzt durch ("")

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Sobald der SDR-Dienst aktiviert wurde, zeigen mail_logs und die Nachrichtenverfolgung die SDR: Protokolleinträgen.

1. mail_logs enthält die Bewertung der gesammelten SDR-Daten.

2. Die Bewertung wird frühzeitig im Mail-Fluss bestimmt, bevor die Mail Policy bestimmt wird.

3. Die für das Urteil getroffenen Maßnahmen werden zum Zeitpunkt der Nachrichtenfilter- und Content-Filter-Aktionen ausgeführt.

<#root>

xxx.com>

mail_logs sample including SDR verdict

```
Tue Dec 3 15:22:44 2019 Info: New SMTP ICID 5539460 interface Data 1 (10.10.10.170) address 55.1.x.y re
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 ACCEPT SG Production_INBOUND match xxx1.xxx.com SBRS 2.5 cou
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SHA
Tue Dec 3 15:22:44 2019 Info: Start MID 3291517 ICID 5539460
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 From: <customer@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 RID 0 To: <owner@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 IncomingRelay(PROD_TO_BETA): Header Received found, IP 172.20
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Message-ID '<mail>'
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Subject "You\\'ve Been Nominated for inclusion with Who\\'s W
```

Tue Dec 3 15:22:44 2019 Info: MID 3291517 SDR: Domains for which SDR is requested: reverse DNS host: Not

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Consolidated Sender Reputation: Awful, Threat Category: M

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Tracker Header : 5Zrl76622ZDGPsS6cByUUXq7LTXXS3/wonoZb5cG

```
Tue Dec 3 15:22:46 2019 Info: MID 3291517 ready 10011 bytes from <owner@xxx.com>
Tue Dec 3 15:22:46 2019 Info: MID 3291517 Custom Log Entry: MF_URL_Category_all HIT
Tue Dec 3 15:22:46 2019 Info: MID 3291517 matched all recipients for per-recipient policy DEFAULT in th
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim verdict using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: CASE spam positive
```

```
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim AV verdict using Sophos CLEAN
Tue Dec 3 15:22:47 2019 Info: MID 3291517 antivirus negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 AMP file reputation verdict : SKIPPED (no attachment in messa
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: GRAYMAIL negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 Custom Log Entry: SDR_Verdict_matched_Awful_Poor
Tue Dec 3 15:22:47 2019 Info: Start MID 3291519 ICID 0
```

4. Einfache grep-Befehle, um die Häufigkeit oder das Vorhandensein bestimmter Urteile zu überprüfen.

- >> grep "Absenderreputation: Schrecklich" mail_logs
- >> grep "Absenderreputation: Schlecht" mail_logs

5. Außerdem können mithilfe des CLI-Befehls findevent in Verbindung mit dem MID-Wert E-Mail-Protokolldetails abgerufen werden.

```
xxx.com> grep "SDR: Domain Reputation.*Poor" mail_logs
Tue Dec 3 11:07:01 2019 Info: MID 3265844 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
Tue Dec 3 12:57:28 2019 Info: MID 3277401 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
```

```
xxx.com> grep "SDR: Domain Reputation.*Awful" mail_logs
Tue Dec 3 10:24:08 2019 Info: MID 3261075 SDR: Consolidated Sender Reputation: Awful, Threat Category: N
Tue Dec 3 15:18:27 2019 Info: MID 3291182 SDR: Consolidated Sender Reputation: Awful, Threat Category: N
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. Keine SZR: Protokolle in den Mail-Protokollen oder der Nachrichtenverfolgung.

- SDR-Protokolle können immer für Nachrichten vorhanden sein, die eine ACCEPT Mail Flow Policy durchlaufen.
- Stellen Sie sicher, dass der Service wie in den ersten Schritten dieses Leitfadens beschrieben aktiviert wurde.

2. Zeitüberschreitung bei SZR:

- Stellen Sie sicher, dass der Cisco Cloud-Server für SDR offen und verfügbar ist.
- v2.sds.cisco.com
- Ein sehr allgemeiner Test kann mithilfe des Telnet aus der CLI durchgeführt werden.

- Wenn ein Banner angezeigt wird, kann die grundlegende Verfügbarkeit bestätigt werden.
    - CLI > telnet v2.sds.cisco.com 443 (dies kann nur einen bestimmten Zeitpunkt überprüfen.)
- Überprüfen Sie die Protokolle anderer Dienste, um festzustellen, ob bei der Kommunikation mit internetbasierten Diensten Fehler auftreten können.
- CLI > zeigt Warnmeldungen an, um nach weiteren Anzeichen für Kommunikationsfehler zu suchen.
- Vor 13.5 AsyncOS verwenden SDR und URL-Filterung beide v2.sds.cisco.com.
    - Eine Überprüfung des CLI-Befehls für die URL-Filterung > websecuritydiagnostics kann eine Validierung ermöglichen, wenn der Netzwerkpfad Latenz enthält.
- Überprüfen Sie die Einstellung für das Reputations-Timeout der Absenderdomäne, und stellen Sie fest, ob der Wert um 1-10 Sekunden erhöht werden kann. Navigieren Sie zu Security Services > Domain Reputation > Edit > Sender Domain Reputation Query Timeout:2.

Der Standardwert ist 2 Sekunden und die maximale Einstellung ist 10 Sekunden.

Wichtiges Update für AsyncOS-Versionen nach 14

Nach der Umstellung kann der Hostname v2.sds.cisco.com weiterhin verfügbar sein, kann aber nicht mehr für URL-Filterung und SDR optimiert werden.

Sie müssen diese Hostnamen und IP-Adressen auf Ihrer Firewall für ausgehenden TCP-Port-443-Datenverkehr zulassen.

Hostnamen:

- serviceconfig.talos.cisco.com
- grpc.talos.cisco.com
- email-sender-ip-rep-grpc.talos.cisco.com

IP-Adressbereiche:

- 146.112.62.0/24
- 146.112.63.0/24
- 146.112.255.0/24
- 146.112.59.0/24
- 2a04:e4c7:ffff::/48
- 2a04:e4c7:fffe::/48

Dies sind Cisco Talos Intelligence Services-Endpunkte, die zum Abrufen der IP-Reputation, der URL-Reputation und -Kategorie sowie zum Senden von Details zu den Serviceprotokollen verwendet werden.

Zugehörige Informationen

- ESA-Bedienungsanleitungen
- ESA-Versionshinweise
- ESA-CLI-Referenzhandbücher
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.