2024년 4월에 진행 중인 ESA 새로 고침에 대한 발신자 도메인 평판 구성

목차

소개

이 문서에서는 ESA(Email Security Appliance)의 SDR(Sender Domain Reputation) 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ESA 개념
- ESA 컨피그레이션

- SEG 기능/기능에 대한 일반 지식 메일 플로우 정책, 메시지 필터, 콘텐츠 필터, 글로벌 도메인 평판

사용되는 구성 요소

이 문서의 정보는 AsyncOS for ESA 14.2 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

1. SDR은 스팸 피싱 탐지를 개선하기 위한 부가 서비스로 개발되었습니다.

2. SDR은 여러 헤더 값을 캡처하여 Talos Threat Intelligence Server에 업로드합니다. 여기서 방대한 Talos 리소스는 단계별 규모에서 각 메시지의 판정을 결정합니다.

3. 결정에 포함된 헤더 값은 다음과 같습니다.

- 봉투 시작
- 발신
- 회신 대상
- DMAR, DKIM 및 SPF 확인(구성된 경우).
- 이메일 주소의 (사용자 이름) 값은 From, Envelope-From 및 Reply-To 헤더에서 선택적으로 제출됩니다
- 발신자 IP
- From 및 Reply-To 헤더에 이름을 표시합니다.

5. 모든 인바운드 메시지에 대해 SDR 검사가 수행됩니다.

6. SDR 스캔은 메시지의 SMTP(Simple Mail Transfer Protocol) 수락 직후 발생합니다.

7. SDR 조치는 메시지 필터 또는 콘텐츠 필터 옵션뿐만 아니라 초기 메일 플로우 정책 단계에서 수행할 수 있습니다.

8. 구성된 구성 요소는 다음과 같습니다.

- 도메인 평판 서비스 사용
- 도메인 예외 목록(선택 사항)
    - 도메인 예외 목록(전역)
    - 메시지/콘텐츠 필터 관련 도메인 예외 목록입니다.
    - 메일 플로우 정책을 사용하는 도메인 복구를 사용하는 전역 작업
    - Global Action with Domain Reputation SMTP 대화 수준에서 작업을 수행하는 중입니다.
- 메시지 필터 또는 콘텐츠 필터

구성

도메인 평판 서비스 WebUI 사용

SDR은 WebUI 또는 CLI 인터페이스에서 활성화할 수 있습니다.

웹 UI:

1. Mail Security Services(메일 보안 서비스) > Domain Reputation(도메인 평판) > Enable(활성화)로 이동합니다.

2. Enable Sender Domain Reputation Filtering(발신자 도메인 평판 필터링 활성화) 옆의 상자를 클릭합니다.

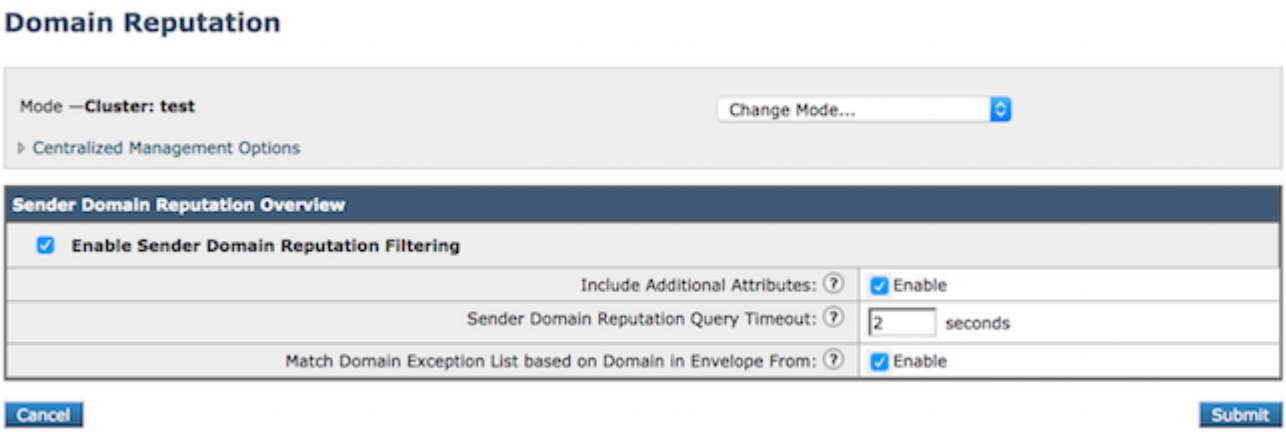
3. 효율성을 높이기 위해 선택된 데이터에 선택적 헤더 값을 포함시키려면 추가 속성 포함: (선택사항) 이 박스를 선택합니다. ? 알아보십시오.

4. 이 상자를 선택합니다. 발신자 도메인 평판 쿼리 시간 초과. 다음을 클릭합니다? 알아보십시오.

5. Envelope From - Enabled(사용)의 도메인에 따라 도메인 예외 목록 일치를 선택합니다.

6. 이미지에 표시된 대로 Submit(제출) > Commit(커밋)을 클릭합니다.

Sender(Domain Reputation) 서비스



보안 서비스 > 도메인 평판

도메인 예외 목록

1. 도메인 예외 목록은 인바운드 메일 흐름에 대해 발신자 도메인 평판 검사를 우회할 수 있습니다.

2. 도메인 예외 목록은 메일 흐름에 영향을 주기 위해 다른 위치에 적용할 수 있습니다.

3. 글로벌 애플리케이션은 스캔되는 모든 메일에 적용할 수 있습니다.

4. 콘텐츠/메시지 필터 내의 더 자세한 애플리케이션은 구성된 필터에만 영향을 줄 수 있습니다.

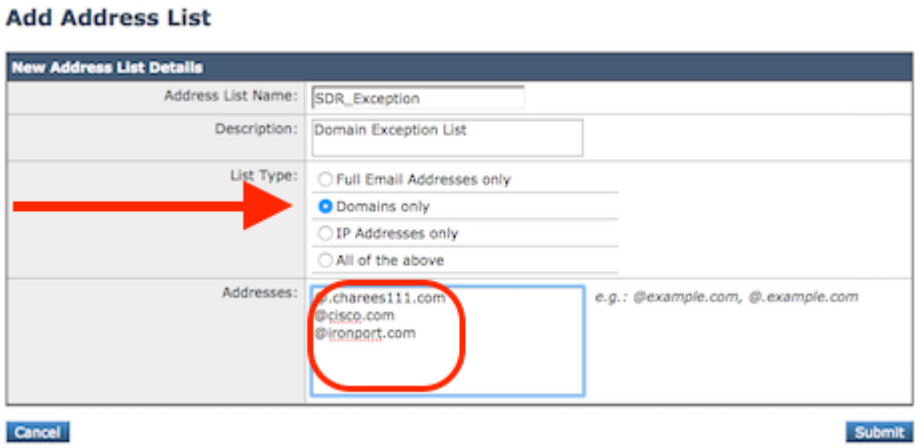
5. 도메인 예외 목록에는 간단한 옵션과 더 안전한 옵션을 모두 제공하는 두 가지 옵션이 있습니다.

6. 이 문서에서는 도메인 예외 목록을 사용하는 메시지에 대해 SDR을 성공적으로 우회하기 위한 옵션에 대해 설명합니다.

7. 도메인 예외 목록 요구 사항 설명

주소 목록 만들기

1. Mail Policies(메일 정책) > Address List(주소 목록) > Add Address List(주소 목록 추가) > Name(이름) > Description(설명) > List Type(목록 유형)으로 이동합니다. 도메인만.
2. 각 도메인 이름을 쉼표로 구분하여 추가합니다.
3. 그림과 같이 Submit and Commit Changes(변경 사항 제출 및 커밋)를 클릭합니다.



도메인 예외 목록에 적용할 주소 목록

주소 목록을 SDR 글로벌 도메인 예외 목록에 적용

1. Security Services(보안 서비스) > Domain Reputation(도메인 평판) > Domain Exception List(도메인 예외 목록) > Edit Settings(설정 수정) > Domain Exception List(도메인 예외 목록)(목록 선택)로 이동합니다.
2. 그림과 같이 Submit and Commit Changes(변경 사항 제출 및 커밋)를 클릭합니다.

드롭다운에서 주소 목록을 선택합니다.

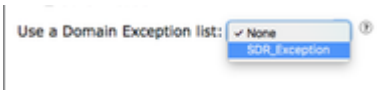
콘텐츠/메시지 필터에 주소 목록 적용

수신 콘텐츠 필터:

1. Condition(조건) > URL Reputation(URL 평판) > Threat Feeds Option(위협 피드 옵션)으로 이동합니다.

2. 조건 도메인 평판

3. 여기를 클릭하십시오.



Domain Exception List(도메인 예외 목록)는 정책 작업별로 허용됩니다.

메시지 필터

메시지 필터 내의 도메인 예외 목록 애플리케이션은 조건 내의 옵션으로 포함됩니다.

참고: 이러한 샘플은 전체 조건의 일부로 domain_exception_list를 포함합니다.

---

1. sdr-reputation(['지독한', '나쁜', '오염된', '약한', '알 수 없는', '보통', '좋은'], domain_exception_list)
2. sdr-age("days", <, 5, domain_exception_list)
3. sdr 검사 불가(domain_exception_list)

메시지 필터 애플리케이션에 대한 보다 포괄적인 설명과 샘플은 ESA User Guides(ESA 사용 설명서) 아래의 제목에서 찾을 수 있습니다.

- ETF에 대한 도메인 평판 규칙
- 메시지 필터를 사용하는 발신자 도메인 평판을 기준으로 메시지 필터링

콘텐츠 필터를 만들어 SDR 판정에 대한 조치를 취합니다.

1. SDR은 수신 메일 흐름에 대해서만 활성화됩니다.
2. SDR 조건 이름: 도메인 평판.
3. 여러 조건을 만들어 서로 다른 결과를 결합할 수 있습니다.
4. Domain Reputation Condition(도메인 평판 조건)에는 각각에 대한 여러 옵션이 포함된 서로 다른 두 개의 검사가 포함되어 있습니다.

- 발신자 도메인 평판
  - 발신자 도메인 평판 판정
  - Sender Domain Age(발신자 도메인 기간)
  - Sender Domain Reputation 검사 불가
- 외부 위협 피드
  - SDR에 대해 수집된 동일한 도메인 헤더를 기준으로 스캔하기 위해 다운로드된 위협 피드 콘텐츠 목록을 사용할 수 있습니다.

✎ 참고: Domain Reputation Condition(도메인 평판 조건) 내의 이러한 옵션은 각 선택 항목에 대해 서로 다른 옵션을 기반으로 시각적으로 변경할 수 있습니다.

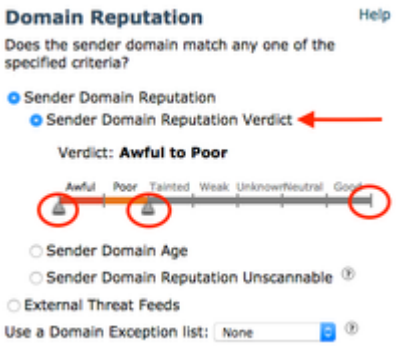
5. 도메인 평판 조건의 마지막 옵션은 도메인 예외 목록입니다.

6. 주소 목록과 연결된 도메인 예외 목록 기능은 메시지 처리의 더 세부적인 메일 정책 수준에 목록을 적용하여 작업 적용에 대한 제어를 추가합니다.

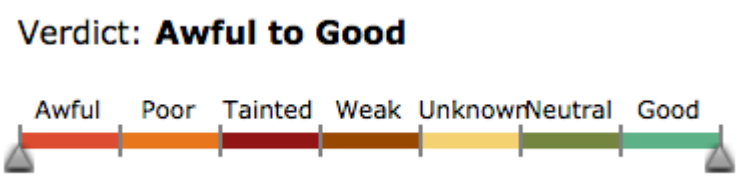
7. Mail Policy(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터) > Add Filter(필터 추가) > Add Condition(조건 추가) > Domain Reputation(도메인 평판)으로 이동합니다.

8. 조건 1 Sender Domain Reputation 판정

- 지독함, 가난함, 오염됨, 약함, 알 수 없음, 중립, 좋음
- 일치시키려는 범위를 선택할 수 있는 슬라이딩 삼각형 마커가 포함되어 있습니다.
- '지독한 상태'와 '나쁜 상태'는 작업을 수행하는 데 권장되는 값입니다.
- Tradal(지독한 상태) 및 Poor(불량한 상태)와 일치하는 메시지에는 Message Tracking(메시지 추적) 내에서 Spam(스팸) 또는 Malicious(악의적인 표시)와 같은 추가 Category(범주)가 있을 수 있습니다.



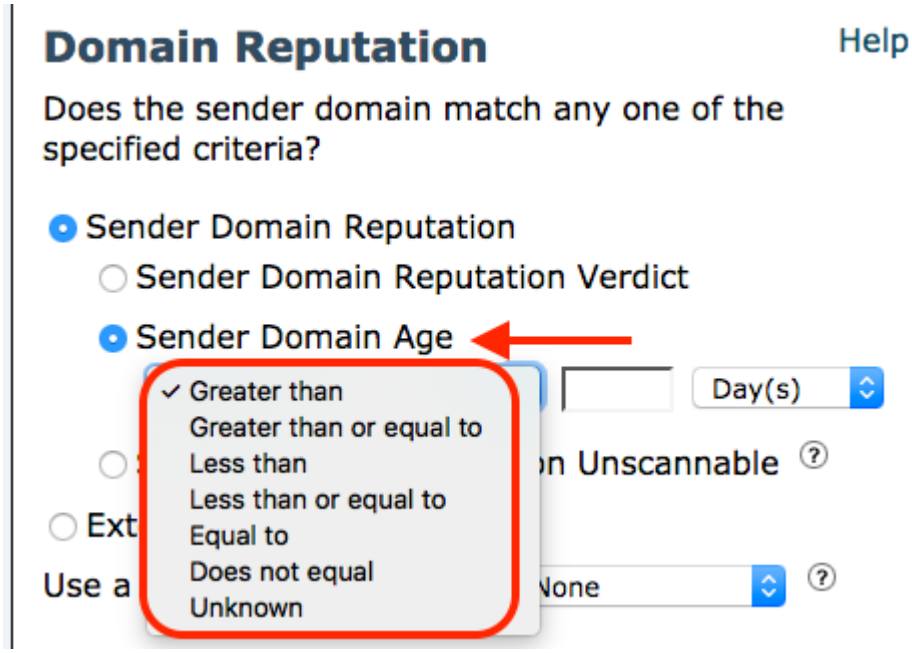
SDR 판정 조정 범위 슬라이드 막대



SDR 판정 슬라이드 막대의 전체 보기

9. 조건 2 발신자 도메인 기간.

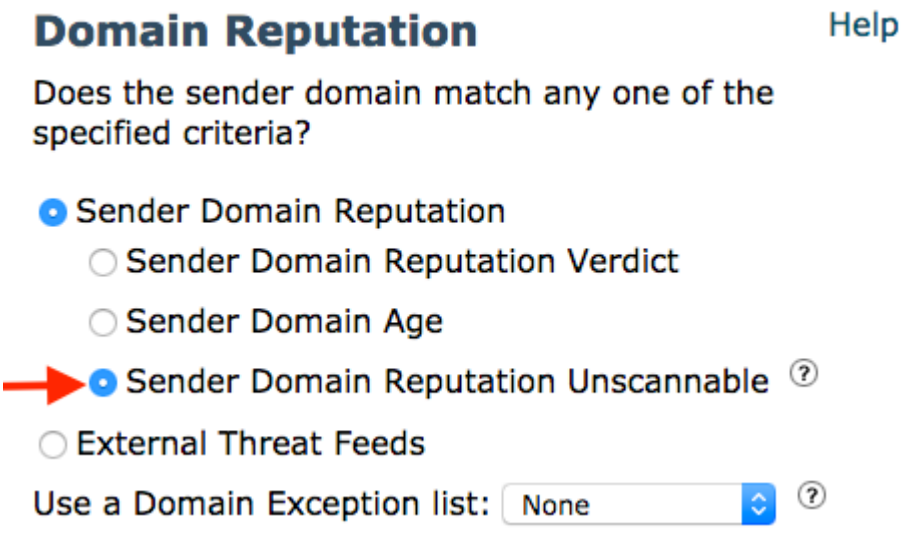
- 도메인의 사용 연한은 더 많은 위험이나 오래 전부터 확립된 신뢰성과 연관될 수 있습니다.
- 사용 기간이 10일 미만인 도메인의 가능성은 더 위험할 수 있습니다.



발신자 도메인 기간. 값이 낮을수록 위험도가 높습니다.

10. 조건 3 발신자 도메인 평판 검사를 수행할 수 없습니다.

- 판정을 얻을 수 없는 경우 관리자가 조치를 취할 수 있는 옵션을 제공합니다.

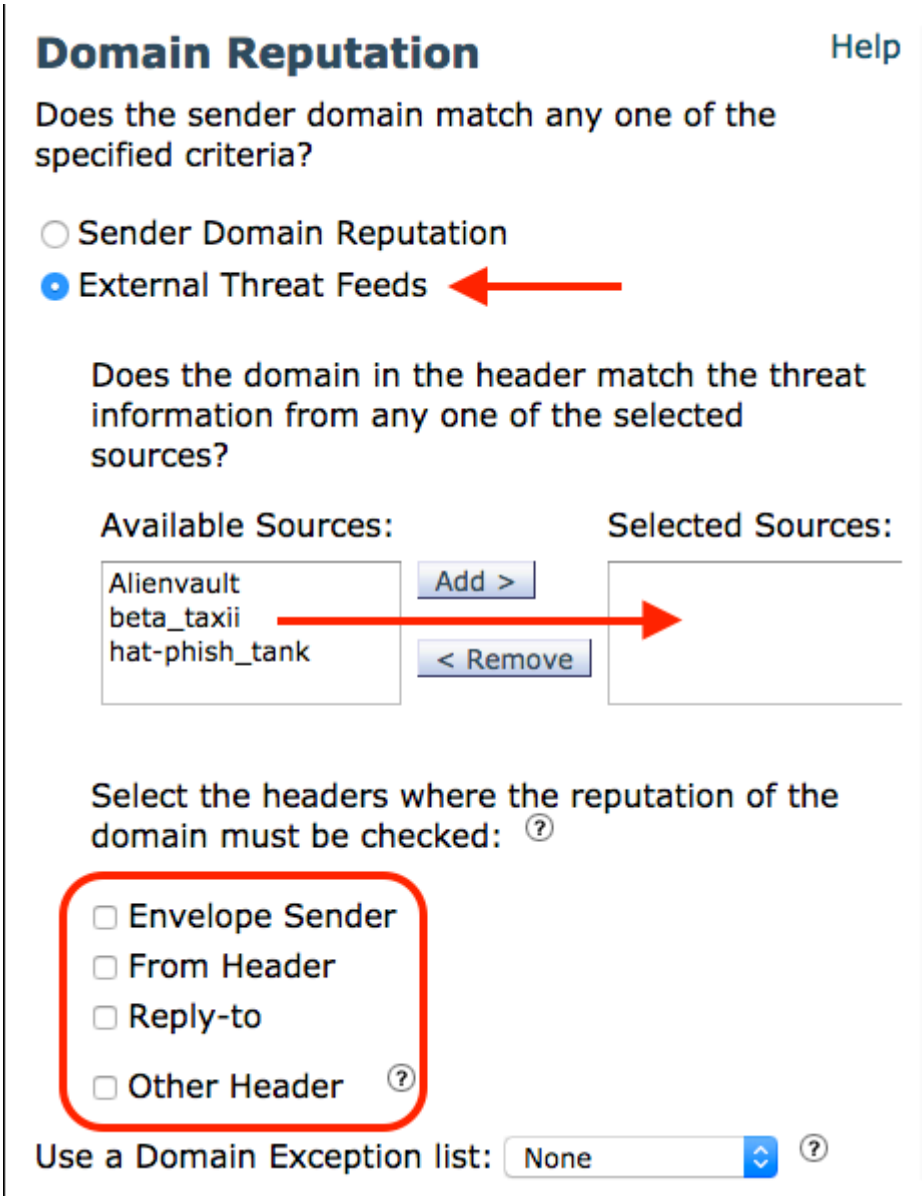


SDR 검사 불가

11. 조건 4 외부 위협 피드

- SDR 검사에 포함된 헤더는 맞춤형 다운로드 STIX/TAXII 콘텐츠로 검사할 수도 있습니다.

- 외부 위협 피드에 대해서는 여기에서 자세히 설명합니다. [외부 위협 피드]

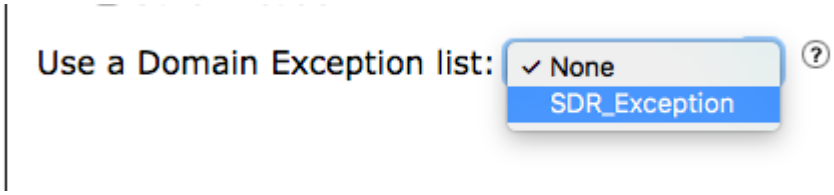


외부 위협 피드를 사용하여 SDR에 사용된 것과 동일한 헤더를 스캔할 수 있습니다.

- [Email Security Appliance 사용 설명서]

12. 조건 5 도메인 예외 목록을 사용합니다.

- 콘텐츠 필터 내에서 도메인 예외 목록을 사용하면 전역 목록보다 더 많은 컨트롤을 추가할 수 있습니다.



Domain Exception List(도메인 예외 목록)는 정책 작업별로 허용됩니다.

13. 이러한 조건과 결합된 조치는 최소한에서 최대한까지 가능하며 관리자의 원하는 결과에 따라 달라집니다.

14. 인기 있는 몇 가지 조치는 다음과 같습니다.

- 쿼런틴/쿼런틴에 복사
- 삭제
- 메시지의 제목 또는 본문에 면책조항이나 경고를 추가합니다.
- 메시지 추적 로그에 대한 특정 단어, 구문 또는 값을 생성하려면 Log Entry를 생성합니다.

메시지 필터 사용을 통해 SDR 구성

1. ESA 사용 설명서는 메시지 필터 구문, 정의 및 예제에 대한 훌륭한 소스입니다.
2. 여기에 제공된 정보 이외의 메시지 필터에 대한 추가 콘텐츠는 사용 설명서에서 이 헤딩을 검색합니다.

- 메시지 필터를 사용하여 발신자 도메인 평판을 기준으로 메시지 필터링

3. 다음 조건은 SDR 메시지 필터와 연결됩니다.

- sdr-reputation(['지독한', '나쁜'] >>>에 대한 모든 값은 다음과 같습니다. 지독함, 가난함, 오염됨, 약함, 알 수 없음, 중립, 좋음
- sdr-reputation(['지독한', '나쁜'], "<domain_exception_list>") >>>인 경우 도메인 예외 목록을 사용합니다.
- sdr-age(<'unit'>, <'operator'> <'actual value'>) >>> "operator" 정의에 대한 사용 설명서를 참조하십시오.
  - if (sdr-age ("unknown", "")) >>> unit = unknown입니다. 나머지 값은 ""로 바뀝니다.
  - 예: if (sdr-age ("months", <, 1, "")). >> unit = 일, 월, 년 연산자 = <(보다 작음). 실제 값 = 1
- sdr-unscannable (<'domain_exception_list'>) >>> 메시지가 표시되면 검사할 수 없는 것입니다. 이 샘플에는 도메인 예외 목록 조건도 포함됩니다.
- if (sdr-scannable ("")) >>> 이 샘플은 예외 목록을 포함하지 않습니다. 값이 ("")로 바뀝니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

SDR 서비스가 활성화되면 mail_logs 및 Message Tracking(메시지 추적)은 SDR을 표시합니다. 로그 항목.

1. mail_logs에는 수집된 SDR 데이터의 점수가 포함됩니다.

2. 이 점수는 메일 정책을 결정하기 전에 메일 흐름의 초기에 결정됩니다.

3. 판정에서 수행한 작업은 메시지 필터 및 콘텐츠 필터 작업 시 발생합니다.

<#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. 특정 판정의 빈도 또는 존재 여부를 확인하기 위한 단순 grep 명령

- >> grep "Sender Reputation: Traddy" mail_logs
- >> grep "Sender Reputation: 불량" mail_logs

5. 또한 MID 값과 함께 CLI findevent 명령을 사용하면 메일 로그 세부사항을 얻을 수 있습니다.

```
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: I
Tue Dec 3 15:18:27 2019 Info: MID 3291182 SDR: Consolidated Sender Reputation: Awful, Threat Category: I
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

1. SDR 없음: mail_logs 또는 Message Tracking 내에 있는 로그

- SDR 로그는 ACCEPT 메일 플로우 정책을 통과하는 메시지에 대해 항상 존재할 수 있습니다.
- 이 가이드의 초기 단계에 제시된 대로 서비스가 활성화되었는지 확인합니다.

2. SDR 시간 초과:

- SDR용 Cisco 클라우드 서버가 열려 있고 사용 가능한지 확인합니다.
- v2.sds.cisco.com
- 매우 일반적인 테스트는 CLI에서 텔넷을 사용하여 수행할 수 있습니다.
- 배너가 나타나면 기본 연결성을 확인할 수 있습니다.
  - CLI > telnet v2.sds.cisco.com 443(특정 시점만 확인할 수 있음)
- 다른 서비스의 로그를 확인하여 인터넷 기반 서비스에 잠재적인 통신 장애가 있는지 확인합니다.
- CLI > displayalerts(경고 표시)를 클릭하여 추가 통신 실패 징후를 확인합니다.
- 13.5 AsyncOS 이전에는 SDR 및 URL 필터링이 모두 v2.sds.cisco.com을 사용합니다.

    - URL Filtering CLI 명령 > websecuritydiagnostics를 검사하면 네트워크 경로에 레이턴시가 포함된 경우 일부 검증을 제공할 수 있습니다.
- Sender Domain Reputation Timeout Setting(발신자 도메인 평판 시간 제한 설정)을 확인하고 값을 1~10초 범위에서 늘릴 수 있는지 확인합니다. Security Services(보안 서비스) > Domain Reputation(도메인 평판) > Edit(편집) > Sender Domain Reputation Query Timeout(발신자 도메인 평판 쿼리 시간 제한)으로 이동합니다.

기본값은 2초이며 최대 설정은 10초입니다.

14 이상 버전의 AsyncOS에 대한 중요 업데이트

전환 후에도 호스트 이름 v2.sds.cisco.com은 계속 사용할 수 있지만 URL 필터링 및 SDR 모두에 대해 더 이상 최적화할 수 없습니다.

아웃바운드 TCP 포트 443 트래픽에 대해 방화벽에서 이러한 호스트 이름 및 IP 주소를 허용해야 합니다.

호스트 이름:

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

IP 주소 범위:

- 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

IP 평판, URL 평판 및 카테고리를 가져오고 서비스 로그 세부 정보를 전송하는 데 사용되는 Cisco Talos Intelligence Services 엔드포인트입니다.

관련 정보

- ESA 사용 설명서
- ESA 릴리스 정보
- ESA CLI 참조 가이드
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.