보안 이메일의 TLD를 기반으로 이메일의 URL 차단

목차

소개

이 문서에서는 특정 TLD(top-level domain)를 기반으로 Cisco Secure Email에서 URL을 차단하는 방법을 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Secure Email을 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.

배경 정보

특정 TLD를 기준으로 URL을 차단하는 것은 이메일 시스템을 잠재적인 위협으로부터 보호하는 효과적인 방법이 될 수 있습니다. Cisco CES/ESA(Email Security Gateway)는 URL의 평판을 분석하고 다양한 기준에 따라 실행합니다.

그러나 회사 정책에서 특정 TLD를 차단해야 하는 경우 이 절차에서는 이메일 시스템의 필터 및 사

전을 사용하여 이를 달성하는 방법에 대해 설명합니다.

1단계. 필터 생성

전체 TLD를 차단하려면 먼저 이메일 시스템에 콘텐츠 필터를 만들어야 합니다. 이 필터는 제한하려는 TLD가 포함된 URL을 식별하고 차단합니다. 사전을 사용하여 TLD 목록을 관리하고 관련 정규식을 통합하여 이 프로세스를 개선할 수 있습니다. 이러한 정규식을 사전에 추가하면 필터링 기준을 효율적으로 관리하고 적용할 수 있습니다.

2단계. 정규식 사용

정규식(regex)은 URL의 특정 패턴을 식별하는 강력한 도구입니다.

TLD를 기반으로 URL을 효과적으로 차단하려면 이러한 정규식을 사전에 추가할 수 있습니다. 이 접근 방식을 사용하면 필터링 기준에 대한 손쉬운 관리 및 업데이트가 가능합니다.

1. HTTP 또는 HTTPS로 시작하는 URL 차단을 위한 정규식 punycode 도메인 지원 포함:

```
(?i)https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)
```

2. Punycode를 지원하는 이메일 형식을 사용하여 URL을 차단하는 정규식:

```
(?i)https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)
```

이러한 정규식을 사전에 추가하면 전자 메일 시스템이 지정된 TLD를 효율적으로 차단하도록 URL 필터링 프로세스를 간소화할 수 있습니다.

Dictionary Properties

Name: URL_TLD

Advanced Matching: ☐ Match whole words ☐ Case Sensitive

▷ Smart Identifiers: *Match specific patterns such as social security numbers and credit card numbers.*

Dictionary Number of terms: 2

Add Terms:

Separate multiple entries with line breaks.

Weight: 1

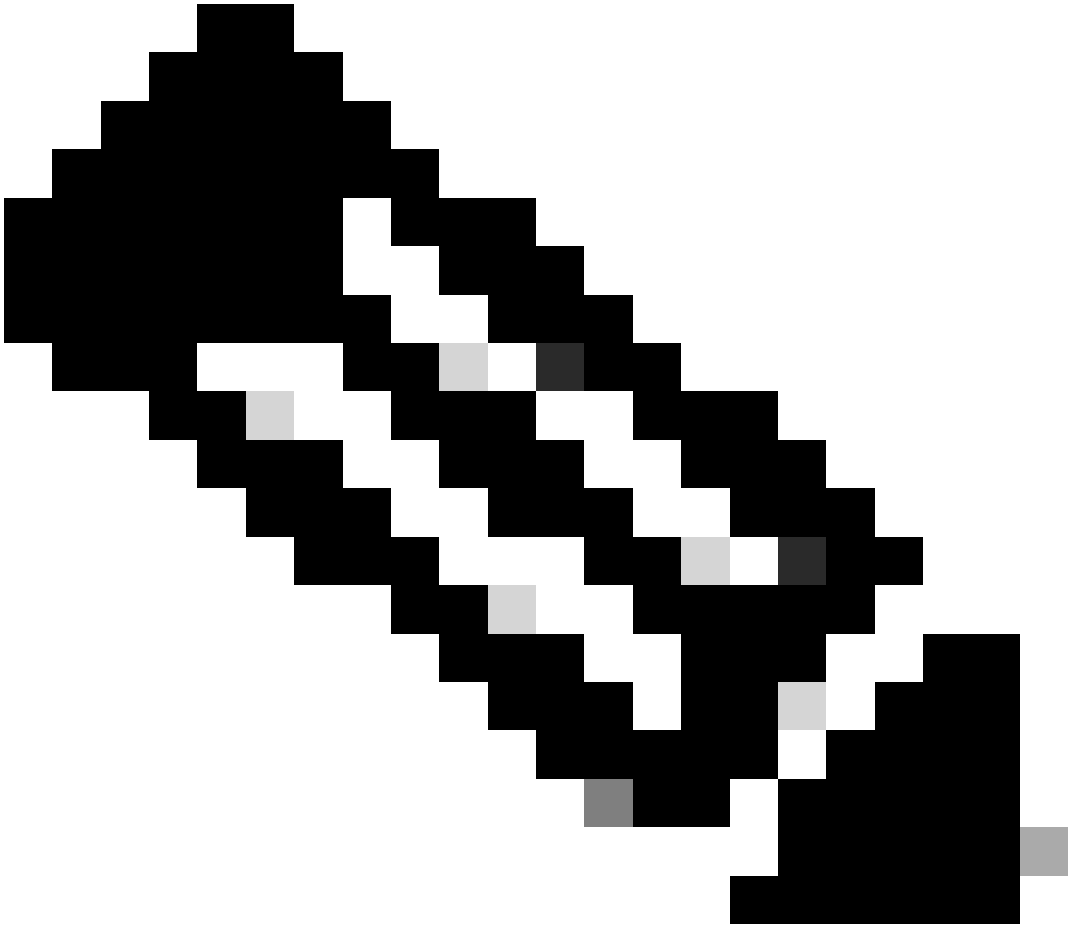
Add

Displaying 1 - 2 of 2 items
Page 1 of 1

<< Previous 1 Next >> 10

Term	Weight	Delete
https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)	1	
https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)	1	

Cancel Submit



참고: U+2215(∕) 및 U+2044(⁄) 같은 유니코드 문자를 고려해야 하는 경우 정규식을 추가로 조정해야 할 수 있습니다.

3단계. 모니터 모드에서 테스트

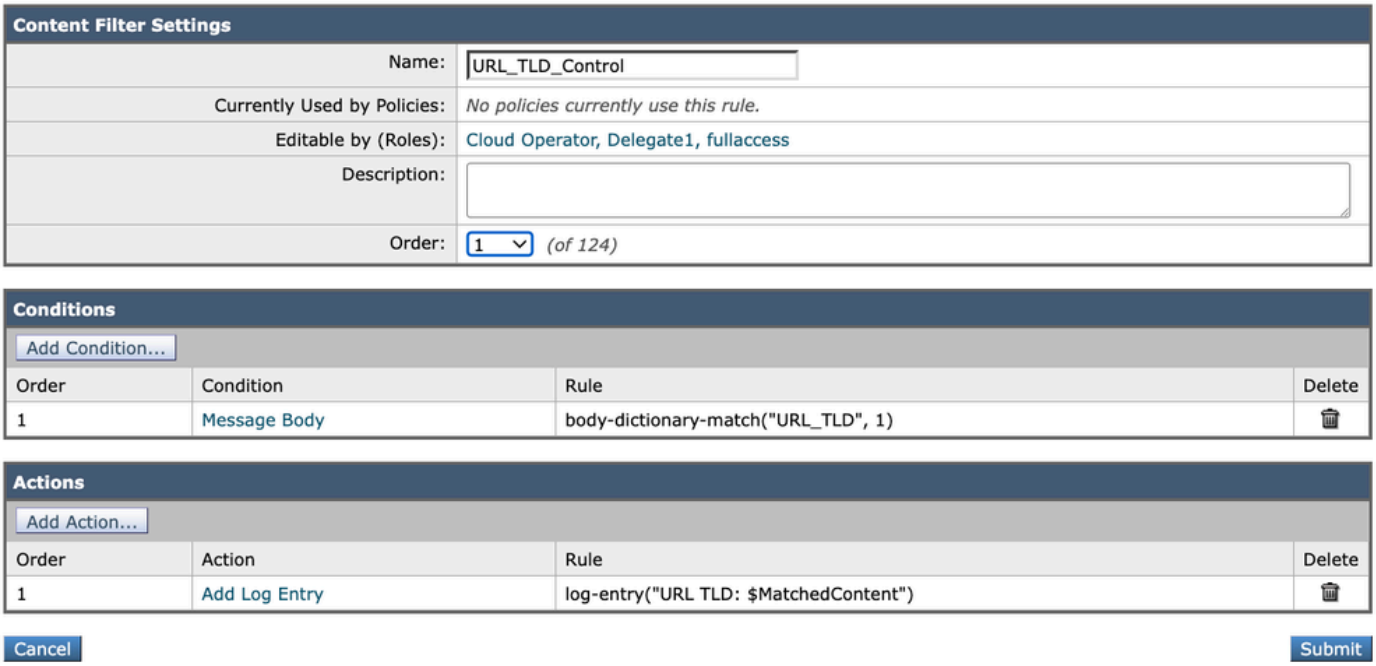
프로덕션 환경에서 이러한 필터를 구현하기 전에 모니터 모드에서 사용하는 것이 좋습니다. 이 접근 방식을 사용하면 이메일을 즉시 차단하지 않고도 필터의 효과를 평가할 수 있으므로 이메일 시스템에 의도하지 않은 중단을 방지할 수 있습니다.

모니터 모드에서는 URL이 지정된 기준과 일치하는 인스턴스를 로깅하므로 사용자는 결과를 관찰하고 필요한 조정을 수행할 수 있습니다. 이를 용이하게 하기 위해 일치하는 URL에 대한 관련 정보를 캡처하는 로그 항목 작업을 구성할 수 있습니다. 예를 들어 다음 로그 항목 작업을 사용할 수 있습니다.

```
log-entry("URL TLD: $MatchedContent")
```

이 작업은 필터 기준과 일치하는 특정 콘텐츠를 로깅하여 필터가 활성 상태일 경우 차단될 URL에 대한 유용한 정보를 제공합니다. 이러한 로그를 검토하여 정규식과 사전 항목을 세부 조정하여 합법적인 이메일에 영향을 주지 않고 원하는 URL을 정확하게 캡처할 수 있습니다.

또한 일정 기간 동안 로그를 모니터링하면 필터의 성능 영향을 평가하고 필요에 따라 최적화할 수 있습니다. 필터가 의도한 대로 작동하고 있다고 확신하면 모니터 모드에서 활성 차단 모드로 전환할 수 있습니다.



성능 고려 사항

정규식을 광범위하게 사용하면 이메일 시스템의 성능에 영향을 줄 수 있습니다. 따라서 필요에 따라 테스트하고 최적화하는 것이 필수적이다.

결론

특정 TLD에 따라 URL을 차단하면 이메일 시스템의 보안을 강화할 수 있습니다. 특히 .zip과 .mov 등 구글이 선보인 새로운 TLD는 인기 있는 파일 확장자와의 유사성으로 인해 보안 문제가 제기돼 왔다. 필터를 신중하게 테스트하고 성능에 미치는 영향을 고려하는 것은 효율적이고 안전한 시스템을 유지하는 데 도움이 됩니다.

Google Registry는 8개의 새로운 TLD를 발표했습니다. .dad, .phd, .prof, .esq, .foo, .zip, .mov 및 .nexus. 그러나 .zip과 .mov는 널리 사용되는 파일 확장자와 유사하기 때문에 특히 관심을 끌었고, 보안 조치에서 이러한 파일을 다루는 것이 중요합니다.

.zip TLD의 보안 영향에 대한 자세한 정보는 Talos Intelligence 블로그 게시물을 참조하십시오. ZIP TLD 정보 누수. 이 리소스는 이러한 TLD와 관련된 잠재적 위험에 대한 추가 컨텍스트를 제공하고 적절한 필터링 전략 구현의 중요성을 강조합니다.

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.