이메일 스푸핑 탐지 및 방지

목차

소개

이 문서에서는 Cisco Secure Email을 사용할 때 이메일 스푸핑을 탐지하고 방지하는 방법을 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- Cisco 보안 이메일

사용되는 구성 요소

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.

이 문서 정보

이 문서는 Cisco Secure Email을 구축하는 Cisco 고객, Cisco 채널 파트너 및 Cisco 엔지니어를 위한 것입니다. 이 문서에서는 다음 내용을 다룹니다.

- 이메일 스푸핑이란?
- 이메일 스푸핑 방어 워크플로
- 스푸핑 방지로 무엇을 더 할 수 있습니까?

이메일 스푸핑이란?

이메일 스푸핑은 이메일 헤더 위조이며 메시지가 실제 소스가 아닌 다른 사람이나 다른 곳에서 온 것으로 보입니다. 합법적이고 신뢰할 수 있는 출처에서 보낸 이메일이라고 생각될 때 해당 이메일을 열 가능성이 높기 때문에 이메일 스푸핑은 피싱 및 스팸 캠페인에 사용됩니다. 스푸핑에 대한 자세한 내용은 What is Email Spoofing 및 How to Detect It을 참조하십시오.

이메일 스푸핑은 다음 범주에 속합니다.

카테고리	설명	주요 대상
직접 도메인 스푸핑	Envelope From에서 유사한 도메인을 받는 사람의 도메인으로 가장합니다.	직원
표시 이름 속임수	From 헤더에는 조직의 임원 이름과 함께 합법적인 발신자가 표시됩니다. BEC(Business Email Compromise)라고도 합니다.	직원
브랜드 이름 가장	From 헤더에는 잘 알려진 조직의 브랜드 이름과 함께 합법적인 발신자가 표시됩니다.	고객/파트너
피싱 URL 기반 공격	민감한 데이터를 훔치거나 피해자로부터 정보를 로그인하려고 시도하는 URL이 포함된 이메일입니다. 링크를 클릭하여 계좌 정보를 확인하라는 은행의 위조 이메일이 피싱 URL 기반 공격의 예입니다.	직원/파트너
사촌 또는 유사시 도메인 공격	Envelope from 또는 From 헤더 값은 SPF(Sender Policy Framework), DKIM(DomainKeys Identified Mail) 및 DMARC(Domain-based Message Authentication, Reporting and Conformance) 검사를 우회하기 위해 실제 주소를 가장하는 유사한 발신자 주소를 표시합니다.	직원/파트너
어카운트 인계/손상된 어카운트	누군가에게 속한 실제 이메일 계정에 무단 액세스한 다음 합법적인 이메일 계정 소유자로서 다른 피해자에게 이메일을 보냅니다.	모두

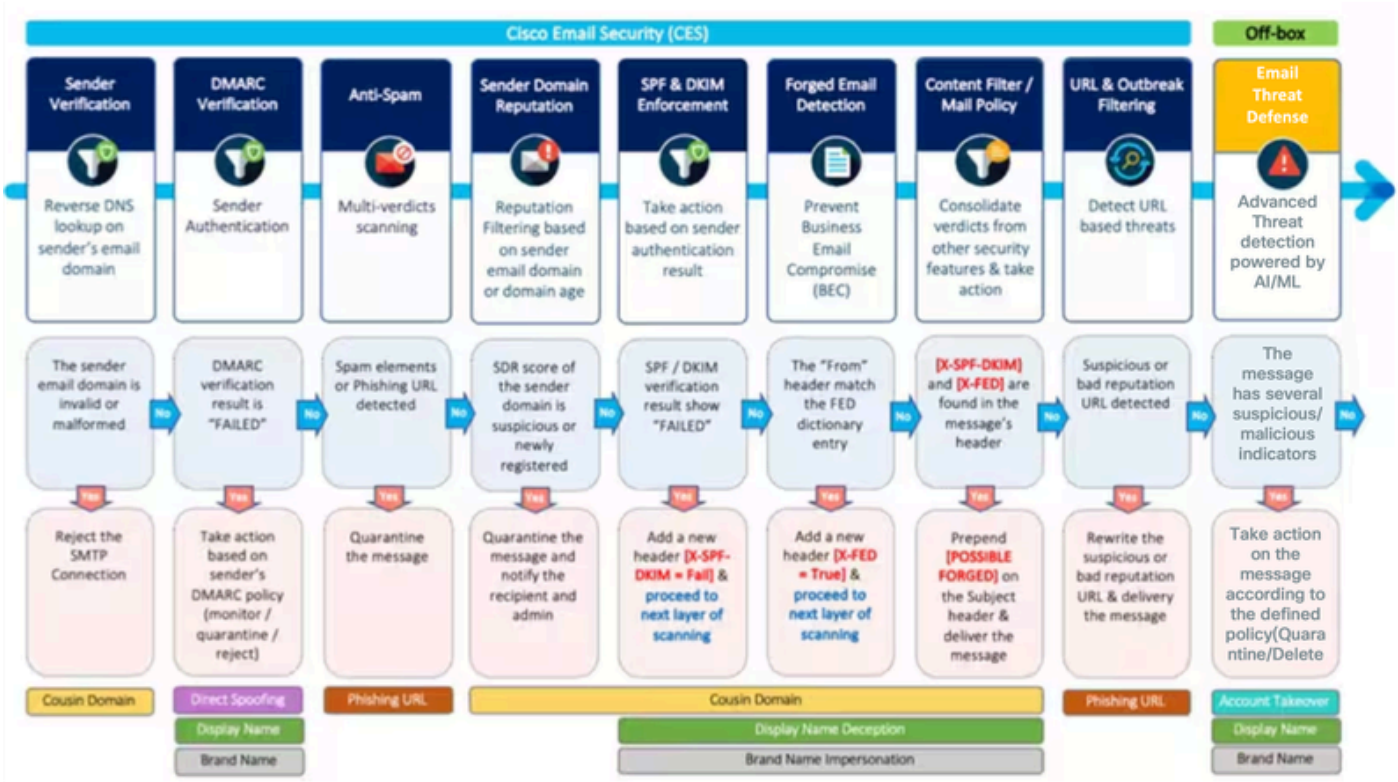
첫 번째 범주는 전자 메일의 인터넷 헤더에 있는 Envelope From 값에 있는 소유자의 도메인 이름 남용과 관련됩니다. Cisco Secure Email은 발신자 DNS(Domain Name Server) 확인을 통해 합법적인 발신자만 허용하는 방식으로 이 공격을 해결할 수 있습니다. DMARC, DKIM 및 SPF 확인을 사용하여 전체적으로 동일한 결과를 얻을 수 있습니다.

그러나 다른 범주는 발신자 이메일 주소의 도메인 부분을 일부만 위반합니다. 따라서 DNS 텍스트 레코드 또는 발신자 확인만 사용할 때는 쉽게 확인할 수 없습니다. 이러한 지능형 위협에 맞서기 위해서는 몇 가지 Cisco Secure Email 기능과 Cisco ETD(Secure Email Threat Defense)를 결합하는 것이 가장 좋습니다. 아시다시피 Cisco Secure Email의 관리 및 기능 컨피그레이션은 조직마다 다를 수 있으며, 부적절한 애플리케이션으로 인해 오탐이 발생할 수 있습니다. 따라서 조직의 비즈니스 요구 사항을 이해하고 기능을 맞춤화하는 것이 중요합니다.

이메일 스푸핑 방어 워크플로

도표(이미지 1)에는 스푸핑 공격을 모니터링, 경고 및 차단하는 모범 사례를 다루는 보안 기능이 나와 있습니다. 각 기능에 대한 자세한 내용은 이 문서에서 확인할 수 있습니다. 모범 사례는 이메일 스푸핑을 탐지하는 심층 방어 접근 방식입니다. 공격자는 시간이 지남에 따라 조직에 대한 방법을 변경할 수 있으므로 관리자는 모든 변경 사항을 모니터링하고 적절한 경고 및 적용을 확인해야 합니다.

이미지 1. Cisco Secure Email Spoof Defense 파이프라인



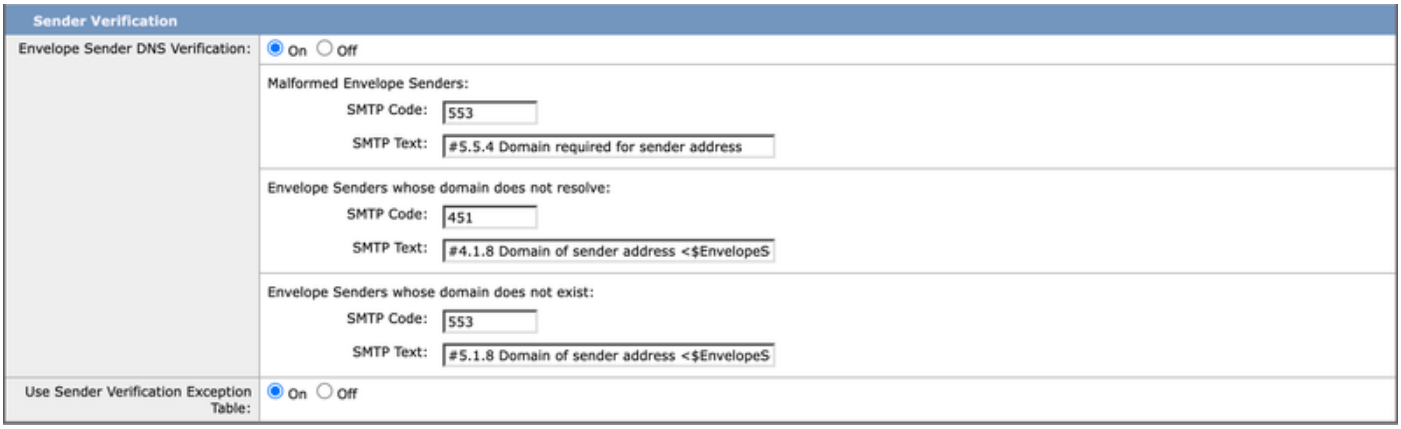
레이어 1: 발신자 도메인에 대한 유효성 검사

발신자 확인은 사촌 도메인 스푸핑과 같은 가짜 이메일 도메인에서 전송되는 이메일을 방지하기 위한 보다 간단한 방법입니다(예: c1sc0.com은 cisco.com의 사기꾼). Cisco Secure Email은 발신자 이메일 주소의 도메인에 대해 MX 레코드 쿼리를 만들고 SMTP 대화 중에 MX 레코드에 대해 A 레

코드 조회를 수행합니다. DNS 쿼리가 NXDOMAIN을 반환하면 도메인이 없는 것으로 간주할 수 있습니다. 확인되지 않은 발신자의 이메일이 수락되고 더 이상 처리되도록 공격자가 봉투 발신자의 정보를 위조하는 것은 일반적인 기술입니다. 발신자의 도메인 또는 IP 주소가 예외 테이블에 미리 추가되어 있지 않으면 Cisco Secure Email은 이 기능을 사용하는 확인 검사에 실패한 모든 수신 메시지를 거부할 수 있습니다.

권장 방법: 봉투 발신자 필드의 이메일 도메인이 유효하지 않은 경우 SMTP 대화를 거부하도록 Cisco Secure Email을 구성합니다. 메일 플로우 정책, 발신자 확인 및 예외 테이블을 구성하여 합법적인 발신자만 허용합니다(선택 사항). 자세한 내용은 Sender Verification(발신자 확인)을 사용하여 Spoof Protection(스푸핑 보호)을 참조하십시오.

이미지 2. 기본 메일 플로우 정책의 발신자 확인 섹션



레이어 2: DMARC를 사용하여 From 헤더 확인

DMARC 검증은 Direct Domain Spoofing에 맞서기 위한 훨씬 더 강력한 기능이며, Display Name(표시 이름) 및 Brand Impersonation(브랜드 가장) 공격도 포함합니다. DMARC는 SPF 또는 DKIM(도메인 소스 또는 시그니처 전송)으로 인증된 정보를 From 헤더의 최종 수신자에게 표시되는 정보와 연결하고 SPF 및 DKIM 식별자가 FROM 헤더 식별자와 일치하는지 확인합니다.

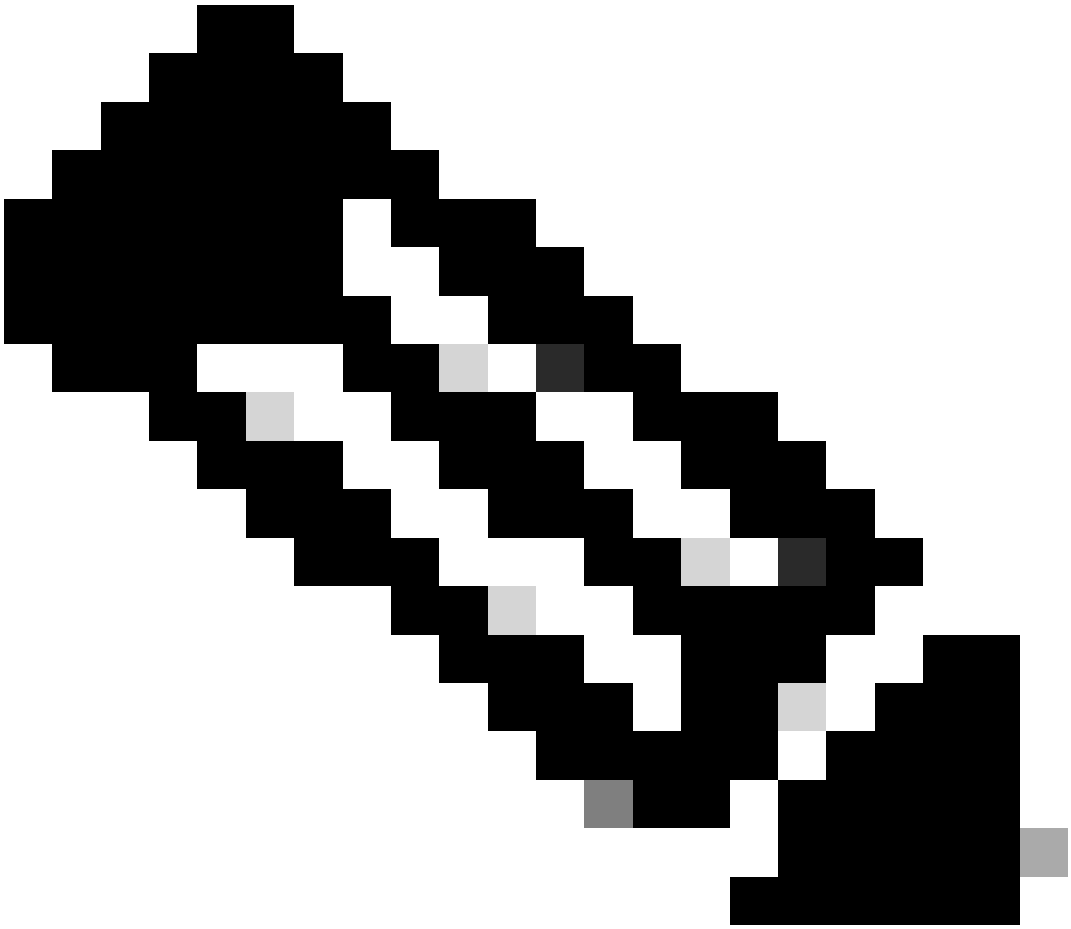
DMARC 확인을 통과하려면 수신 이메일이 이러한 인증 메커니즘 중 하나 이상을 통과해야 합니다. 또한 관리자는 Cisco Secure Email을 사용하여 DMARC 확인 프로필을 정의하여 도메인 소유자의 DMARC 정책을 재정의하고 집계(RUA) 및 오류/포렌식(RUF) 보고서를 도메인 소유자에게 전송할 수 있습니다. 이는 인증 구축을 강화하는 대신 도움이 됩니다.

권장 방법: 발신자가 권고하는 DMARC 정책 작업을 사용하는 기본 DMARC 프로필을 수정합니다. 또한 올바른 보고서 생성을 활성화하려면 DMARC 확인의 전역 설정을 편집해야 합니다. 프로필이 적절하게 구성되면 메일 플로우 정책 기본 정책에서 DMARC 확인 서비스를 활성화해야 합니다.

이미지 3. DMARC 확인 프로필

Create DMARC Verification Profile

Profile Name:	DEFAULT
Message Action when the Policy in DMARC Record is Reject:	○ No Action ○ Quarantine to: ACCOUNT_TAKEOVER (centralized) ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC unauthenticated mai
Message Action when the Policy in DMARC Record is Quarantine:	○ No Action ◉ Quarantine to: Policy (centralized)
Message Action for Temporary Failure:	◉ Accept ○ Reject SMTP Code: 451 SMTP Response: #4.7.1 Unable to perform DMARC v
Message Action for Permanent Failure:	○ Accept ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC verification failed.



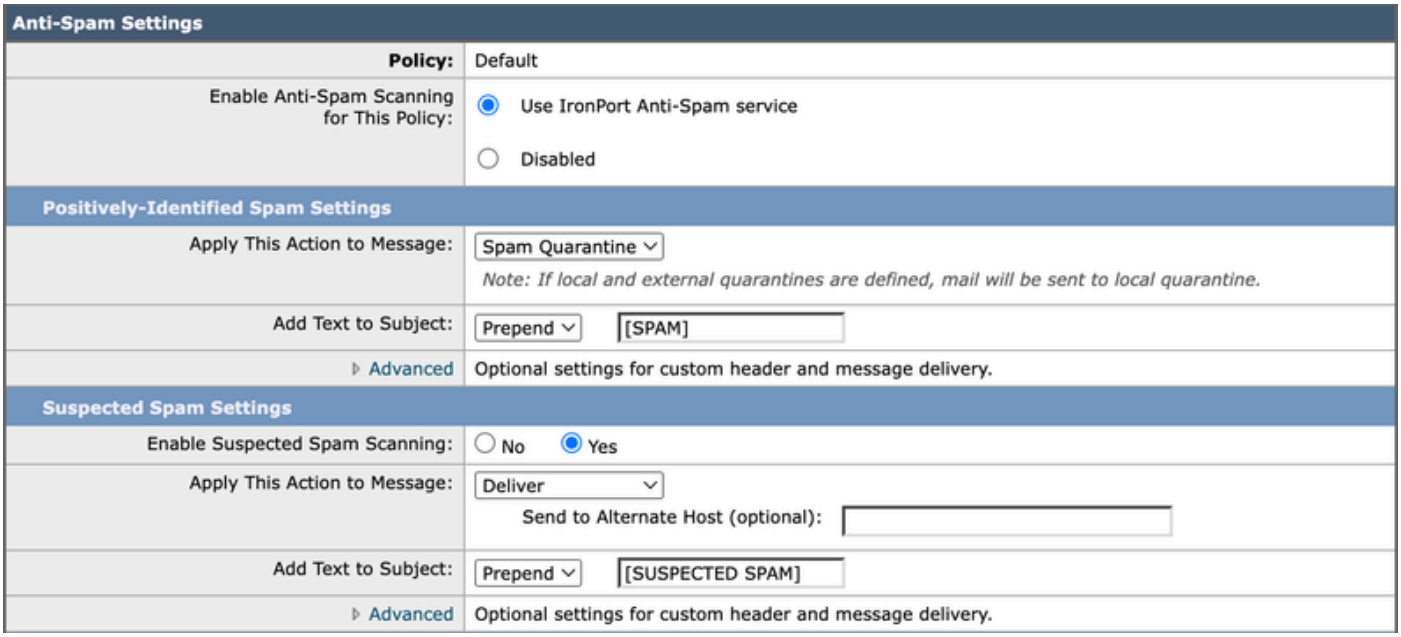
참고: DMARC는 Cisco Domain Protection과 같은 도메인 모니터링 툴과 함께 도메인 소유자를 전송하여 구현해야 합니다. 적절하게 구현되면 Cisco Secure Email의 DMARC 시행을 통해 무단 발신자 또는 도메인으로부터 직원에게 전송되는 피싱 이메일을 차단할 수 있습니다. Cisco Domain Protection에 대한 자세한 내용은 Cisco Secure Email Domain Protection At-A-Glance 링크를 참조하십시오.

레이어 3: 스팸 발송자가 스푸핑된 이메일을 전송하지 못하도록 방지

스푸핑 공격은 스팸 캠페인의 또 다른 일반적인 형태가 될 수 있습니다. 따라서 스팸/피싱 요소가 포함된 사기성 이메일을 효과적으로 식별하여 긍정적으로 차단하려면 안티스팸 보호를 활성화하는 것이 중요합니다. 안티스팸은 이 문서에서 자세히 설명한 다른 모범 사례 작업과 결합되어 합법적인 이메일을 잃지 않고 최상의 결과를 제공합니다.

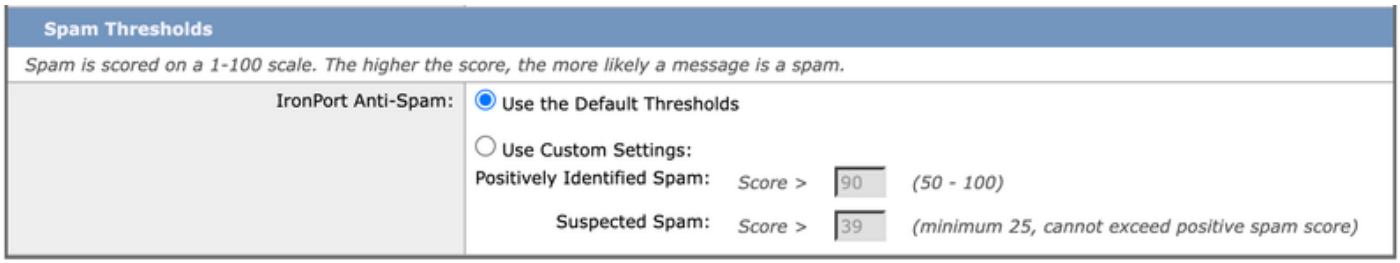
권장 방법: 기본 메일 정책에서 안티스팸 검사를 활성화하고 스팸 설정을 긍정적으로 식별하도록 격리 조치를 설정합니다. 스팸 메시지의 최소 검사 크기를 전체적으로 2M 이상으로 늘립니다.

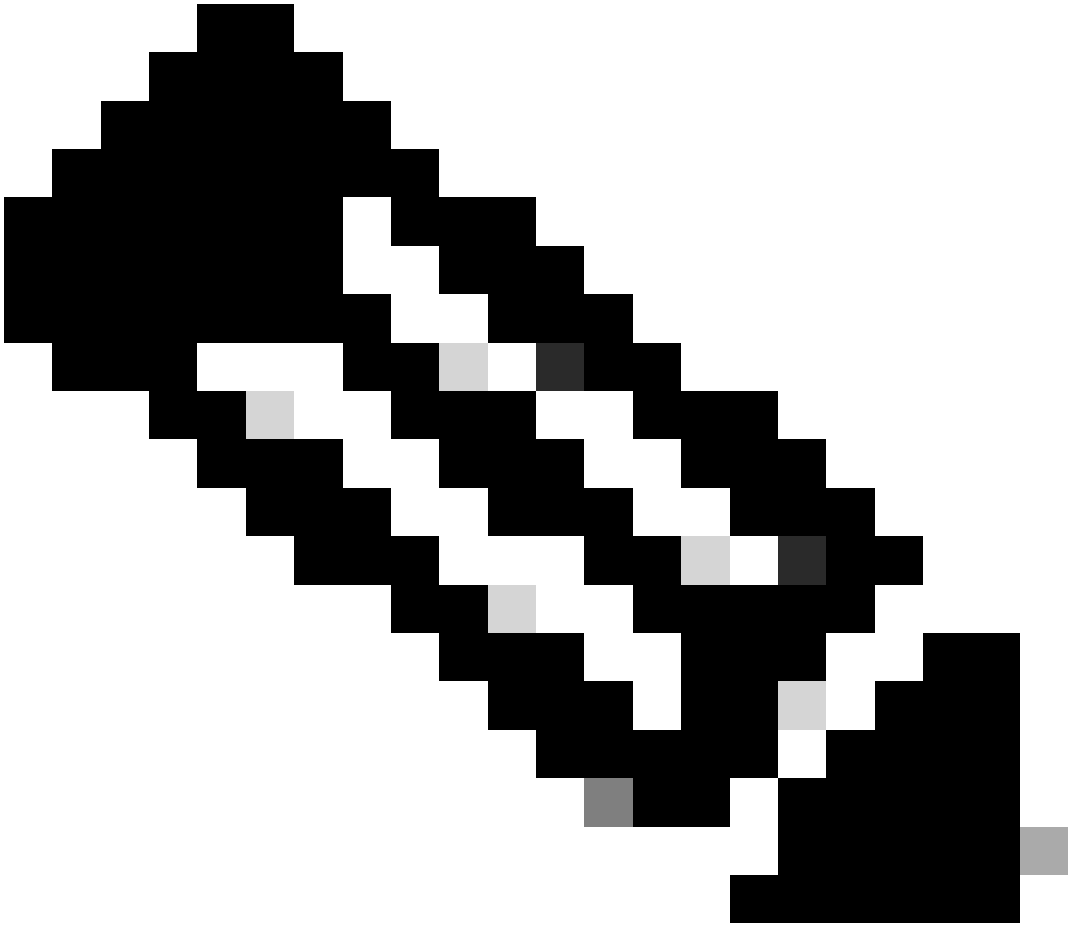
이미지 4. 기본 메일 정책의 안티스팸 설정



스팸 임계값을 Positive(양성) 및 Suspected(의심) 스팸에 맞게 조정하여 민감도를 높이거나 낮출 수 있습니다(이미지 5). 그러나 Cisco는 관리자가 이 작업을 수행하지 않도록 권장하며 Cisco에서 별도로 지시하지 않는 한 기본 임계값만 기준으로 사용하도록 권장하지 않습니다.

이미지 5. 기본 메일 정책의 안티스팸 임계값 설정





참고: Cisco Secure Email은 스팸 포착률(가장 공격적인 포착률)을 높이기 위해 안티스팸 엔진과 다른 조합을 제공하는 애드온 IMS(Intelligent Multi-Scan) 엔진을 제공합니다.

레이어 4: 이메일 도메인을 통해 악의적인 발신자 확인

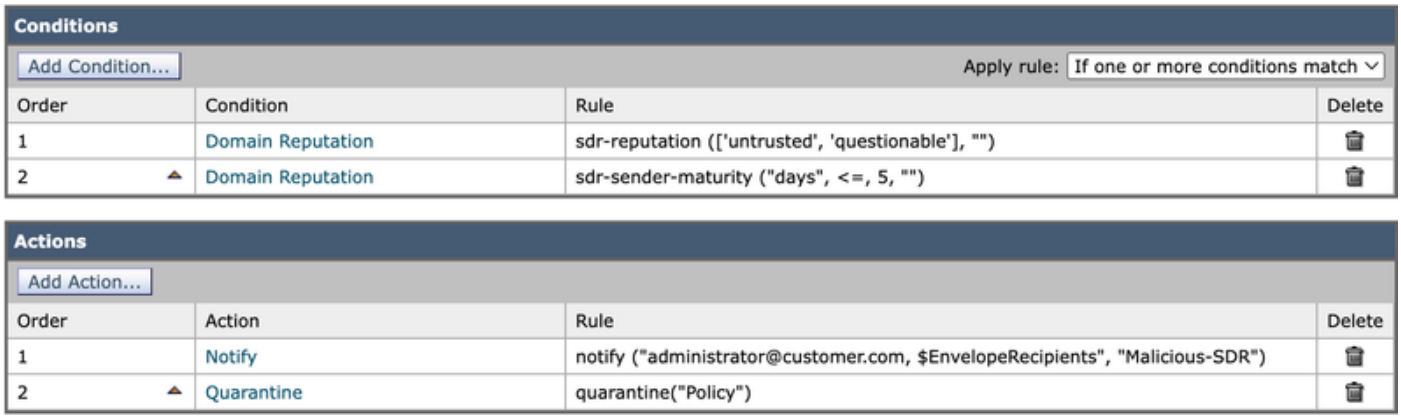
Cisco Talos Sender Domain Reputation(SDR)은 이메일 봉투 및 헤더의 도메인을 기반으로 이메일 메시지에 대한 평판 판정을 제공하는 클라우드 서비스입니다. 도메인 기반 평판 분석을 통해 공유 IP 주소, 호스팅 또는 인프라 공급업체의 평판을 뛰어넘어 스팸 포착률을 높일 수 있습니다. 대신 FQDN(정규화된 도메인 이름)과 관련된 기능 및 SMTP(Simple Mail Transfer Protocol) 대화 및 메시지 헤더의 기타 발신자 정보를 기반으로 판정을 도출합니다.

Sender Maturity는 발신자의 평판을 확립하는 데 필수적인 기능입니다. Sender Maturity는 여러 정보 소스를 기반으로 스팸 분류에 대해 자동으로 생성되며 Whois 기반 도메인 기간과 다를 수 있습니다. Sender Maturity는 30일 한도로 설정되며, 이 한도를 초과하는 도메인은 이메일 발신자로 성숙된 것으로 간주되며 추가 세부 정보는 제공되지 않습니다.

권장 방법: SDR 평판 판정이 Untrusted/Questions에 속하거나 Sender Maturity가 5일 이하인 전송

도메인을 캡처하는 수신 콘텐츠 필터를 만듭니다. 권장 조치는 메시지를 격리하고 이메일 보안 관리자 및 원래 수신자에게 알리는 것입니다. SDR 구성 방법에 대한 자세한 내용은 Cisco Email Security Update(버전 12.0): Sender Domain Reputation(SDR)에서 Cisco 비디오를 참조하십시오.

이미지 6. 알림 및 격리 작업이 포함된 SDR 평판 및 도메인 기간에 대한 콘텐츠 필터.



Conditions

Add Condition... | Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	Domain Reputation	sdr-reputation (['untrusted', 'questionable'], "")	
2	Domain Reputation	sdr-sender-maturity ("days", <=, 5, "")	

Actions

Add Action...

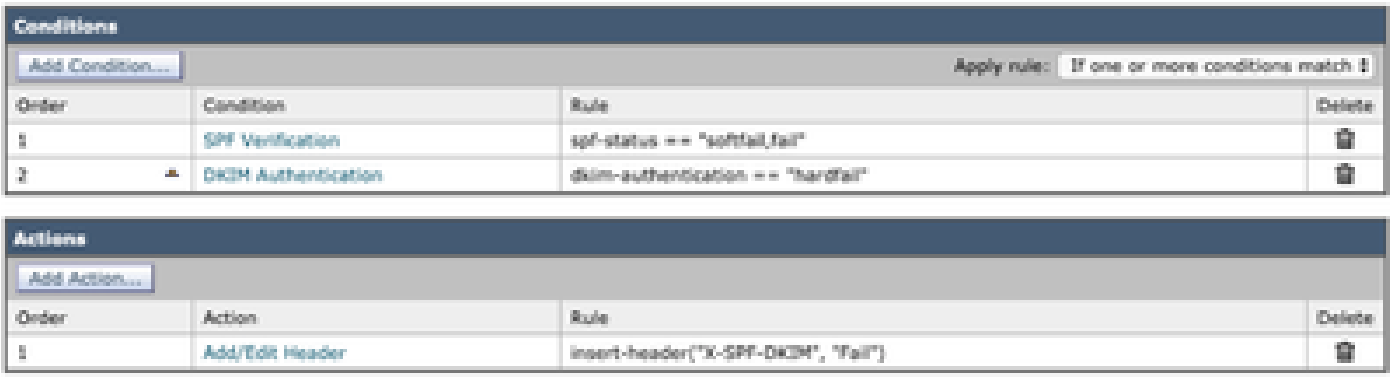
Order	Action	Rule	Delete
1	Notify	notify ("administrator@customer.com, $EnvelopeRecipients", "Malicious-SDR")	
2	Quarantine	quarantine("Policy")	

레이어 5: SPF 또는 DKIM 확인 결과로 오탐 감소

대부분의 공격 유형에 대해 다중 레이어 스푸핑 이메일 탐지 기능을 구축하려면 SPF 또는 DKIM 확인(둘 다 또는 둘 중 하나)을 적용하는 것이 중요합니다. Cisco에서는 최종 작업(삭제 또는 격리 등)을 수행하는 대신 SPF 또는 DKIM 확인에 실패한 메시지에 [X-SPF-DKIM]과 같은 새 헤더를 추가하고, 스푸핑 이메일의 탐지율 향상을 위해 나중에 다루는 FED(Forged Email Detection) 기능을 사용하여 결과를 공동 적용할 것을 권장합니다.

권장 방법: 이전 검사를 통과한 각 수신 메시지의 SPF 또는 DKIM 확인 결과를 검사하는 콘텐츠 필터를 만듭니다. SPF 또는 DKIM 확인에 실패하고 다음 스캐닝 레이어인 FED(Forged Email Detection)로 전달되는 메시지에 새 X-헤더(예: X-SPF-DKIM=Fail)를 추가합니다.

이미지 7. 실패한 SPF 또는 DKIM 결과가 있는 메시지를 검사하는 콘텐츠 필터



Conditions

Add Condition... | Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	SPF Verification	spf-status == "softfail,fail"	
2	DKIM Authentication	dkim-authentication == "hardfail"	

Actions

Add Action...

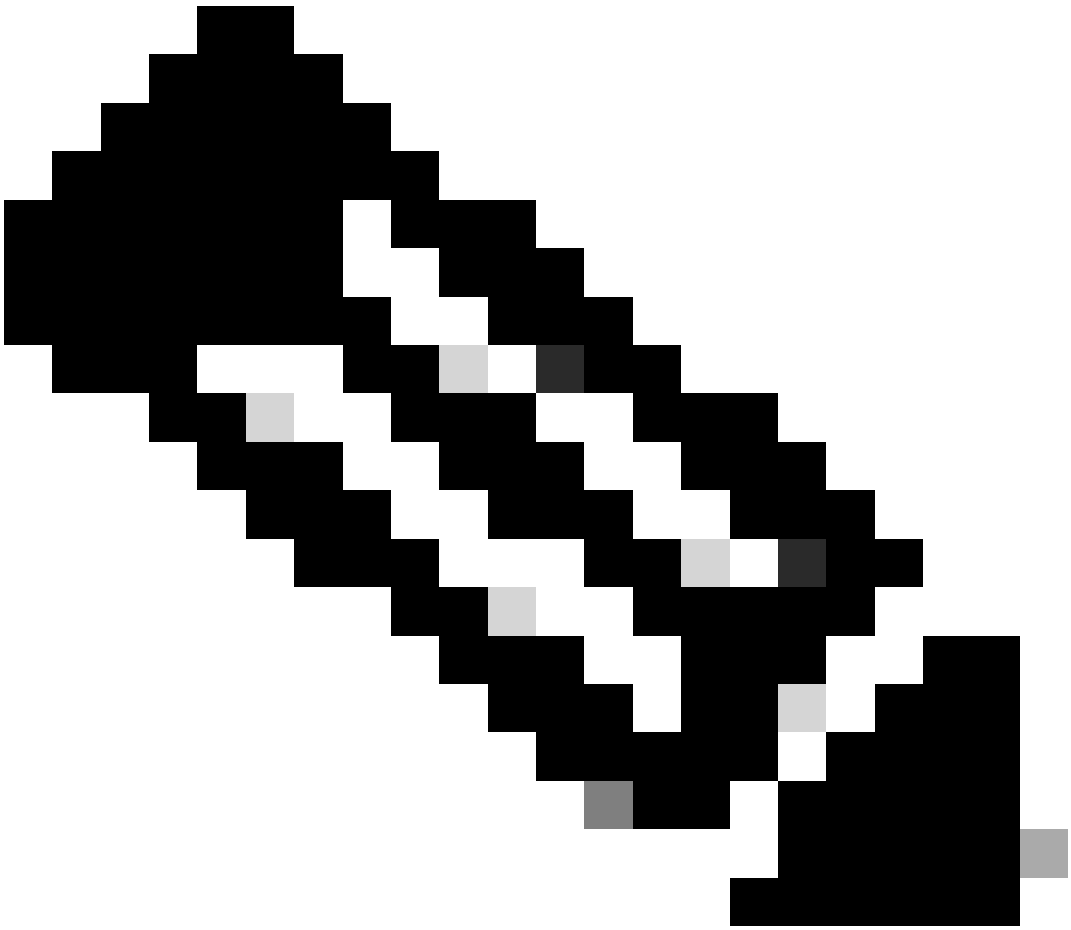
Order	Action	Rule	Delete
1	Add/Edit Header	insert-header("X-SPF-DKIM", "Fail")	

레이어 6: 위조된 발신자 이름이 있는 메시지 탐지

SPF, DKIM 및 DMARC 검증을 보완하는 FED(Forged Email Detection)는 이메일 스푸핑에 대한 또 다른 중요한 방어선입니다. FED는 메시지 본문의 From 값을 남용하는 스푸핑 공격을 해결하는 데 이상적입니다. 조직 내에서 임원 이름을 이미 알고 있는 경우 이러한 이름의 사전을 만든 다음 콘텐츠 필터에서 FED 조건으로 해당 사전을 참조할 수 있습니다. 또한 경영진 이름과 별도로 DNSTWIST(DNSTWIT)를 사용하여 유사 도메인 스푸핑에 대해 매칭하여 도메인을 기반으로 사촌

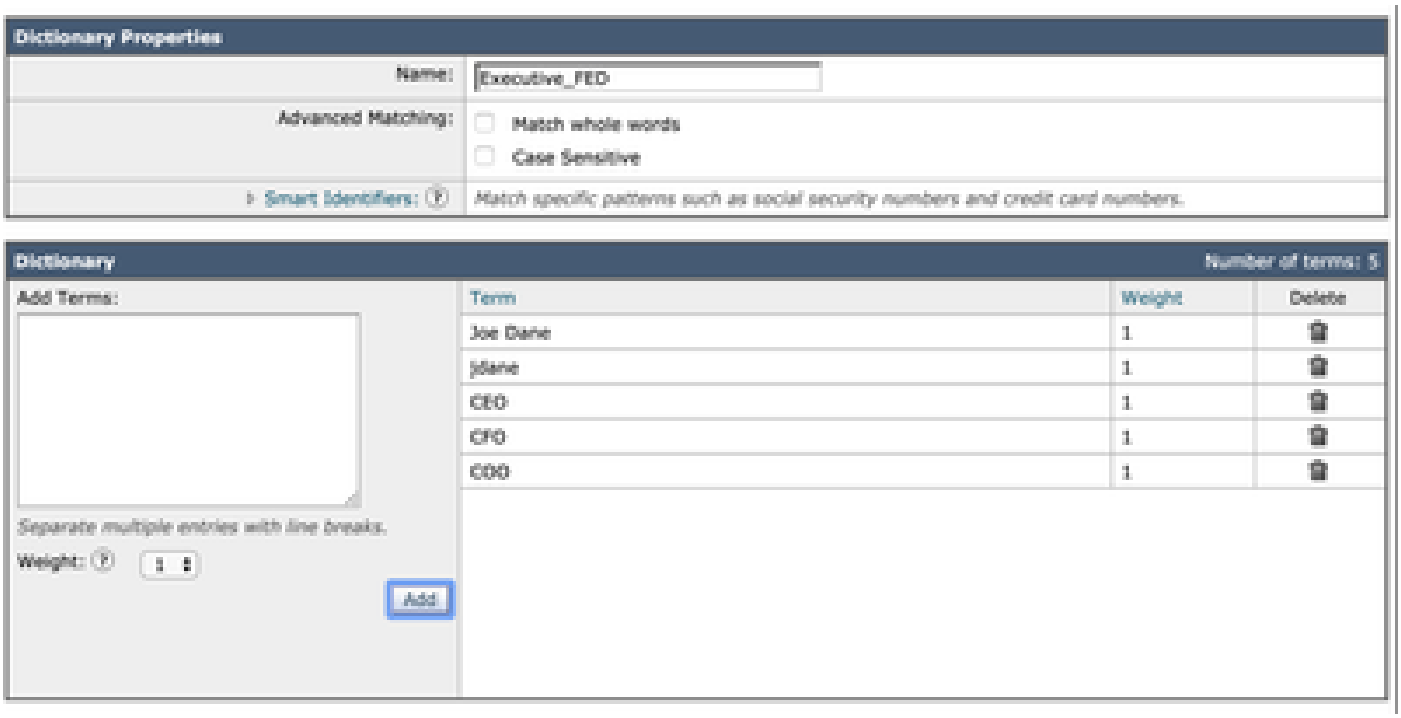
또는 유사 도메인 사전을 만들 수 있습니다.

권장 방법: 조직 내에서 메시지가 위조될 가능성이 높은 사용자를 식별합니다. 임원을 설명하는 사용자 지정 사전을 만듭니다. 모든 경영진 이름에 대해 사전에는 사용자 이름과 가능한 모든 사용자 이름이 용어로 포함되어야 합니다(이미지 8). 사전이 완료되면 콘텐츠 필터에서 위조된 이메일 탐지를 사용하여 수신 메시지의 From 값을 이러한 사전 항목과 일치시킵니다.



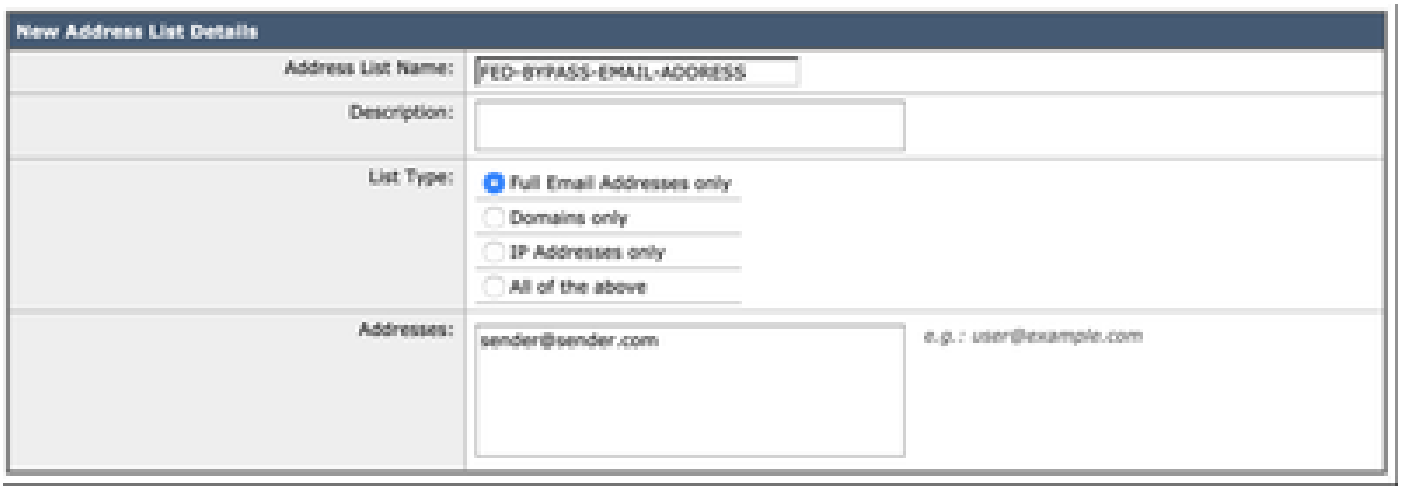
> 참고: 대부분의 도메인이 등록 순열이 아닌 것을 고려하면 DNS 발신자 확인은 도메인으로부터 보호합니다. 사전 항목을 사용하도록 선택하는 경우 등록된 도메인에만 주의를 기울여야 하며, 사전당 500~600개의 항목을 초과하지 않아야 합니다.

이미지 8. 위조 이메일 탐지를 위한 맞춤형 디렉토리



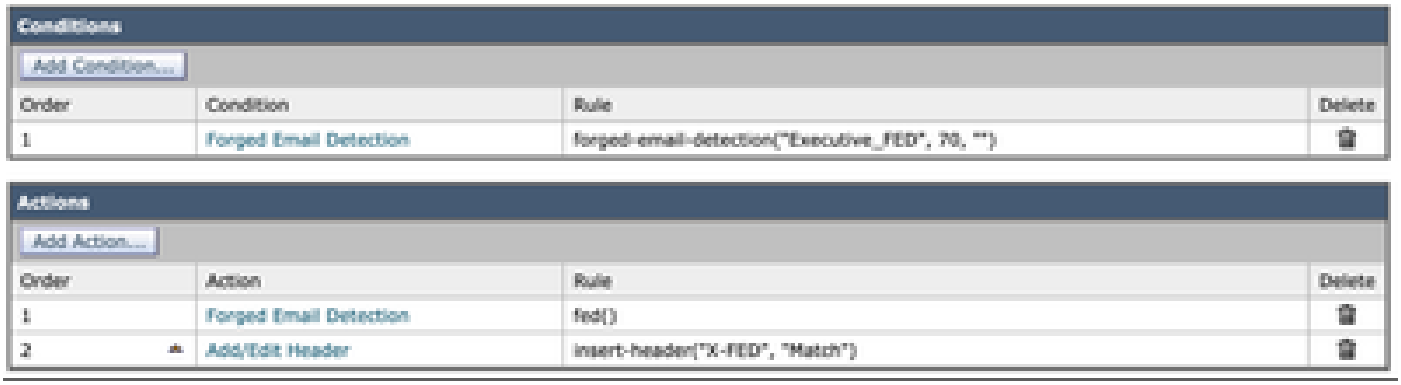
Envelope Send(봉투 전송)에서 이메일 도메인에 대한 예외 조건을 추가하여 FED 검사를 우회하는 것은 선택 사항입니다. 또는 Fromheader(이미지 9)에 표시되는 이메일 주소의 목록으로 FED 검사를 우회하도록 사용자 지정 주소 목록을 생성할 수 있습니다.

이미지 9. FED 검사를 우회할 주소 목록 생성



Forged Email Detection(위조된 이메일 탐지) 독점 작업을 적용하여 From(발신) 값을 제거하고 메시지 받은 편지함에서 실제 봉투 발신자 이메일 주소를 검토합니다. 그런 다음 최종 작업을 적용하는 대신 조건과 일치하는 메시지에 새 X-헤더(예: X-FED=Match)를 추가하고 메시지를 다음 검사 계층으로 계속 전달합니다(이미지 10).

이미지 10. FED에 대한 권장 콘텐츠 필터 설정

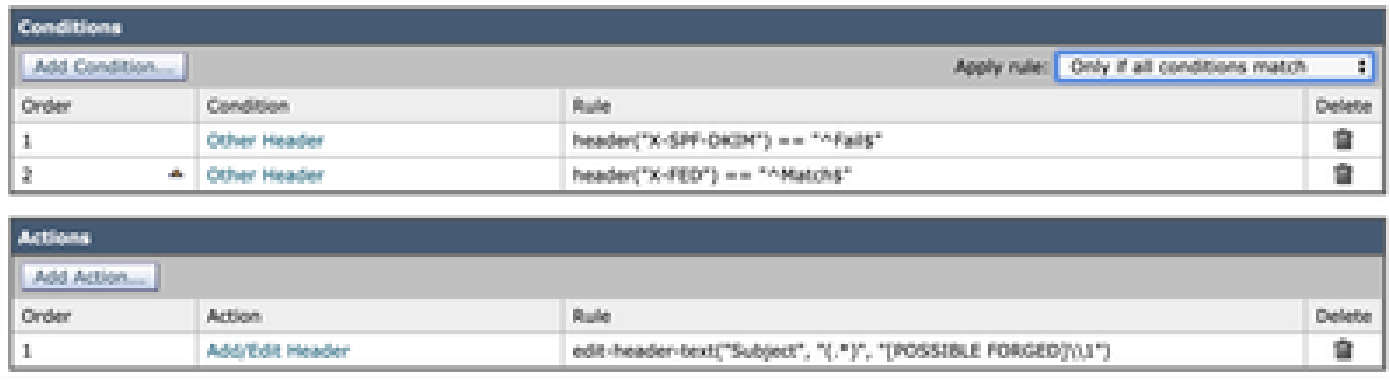


레이어 7: 스푸핑 이메일 확인

실제 스푸핑 캠페인을 식별하는 것은 SPF/DKIM Enforcemen 및 FE에서 생성되는 X-헤더 정보와 같은 파이프라인의 다양한 보안 기능의 다른 판정을 참조하여 더 효과적입니다. 예를 들어 관리자는 실패한 SPF/DKIM 확인 결과(X-SPF-DKIM=Fail) 및 FED 사전 항목과 일치하는 From 헤더(X-FED=Match)로 인해 두 새 X-헤더가 모두 추가된 메시지를 식별하기 위한 콘텐츠 필터를 만들 수 있습니다.

권장 조치는 메시지를 격리하여 수신자에게 알리거나, 원본 메시지를 계속해서 전달할 수 있지만 [POSSIBLE FORGED] 단어를 제목 줄에 경고로 추가하는 것입니다(그림 11).

이미지 11. 모든 X-헤더를 단일(최종) 규칙으로 결합

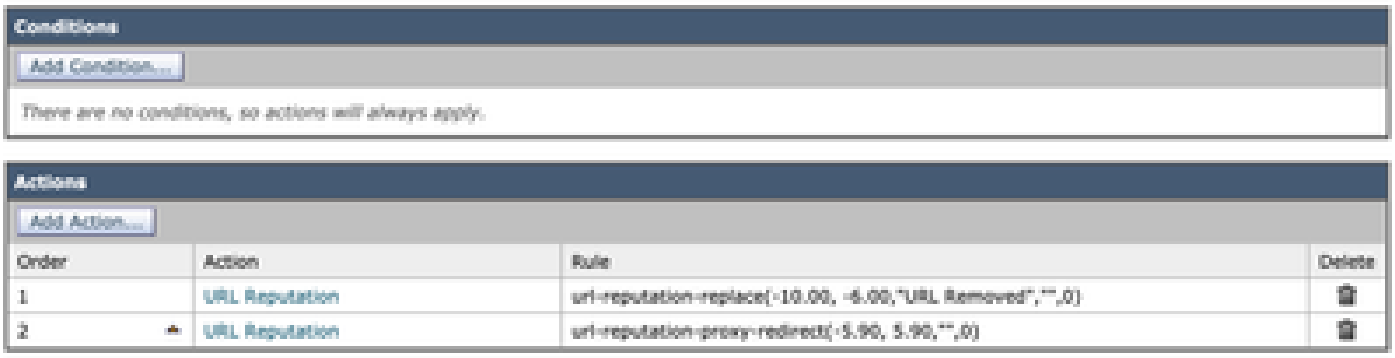


레이어 8: 피싱 URL로부터 보호

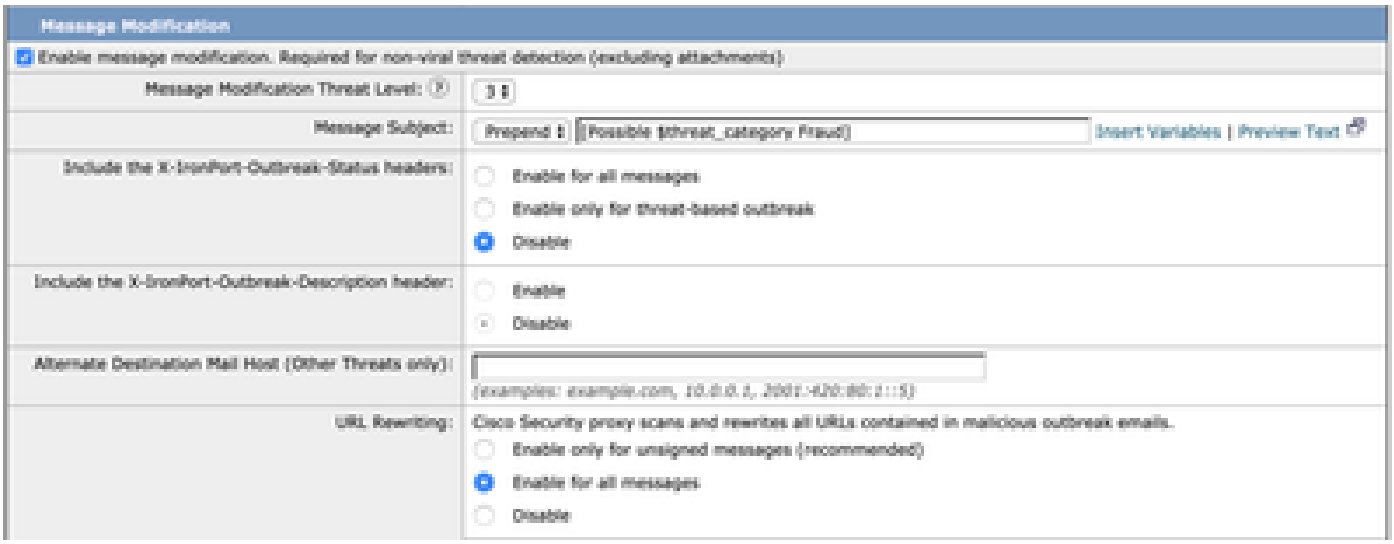
피싱 링크에 대한 보호는 Cisco Secure Email의 URL 및 Outbreak Filtering에 통합됩니다. 혼합 위협은 스푸핑과 피싱 메시지를 결합하여 표적에 더 합법적인 것처럼 보이게 합니다. Outbreak Filtering을 활성화하는 것은 이러한 위협을 실시간으로 탐지, 분석 및 차단하는 데 매우 중요합니다. URL 평판은 안티스팸 엔진 내부에서 평가되며 스팸 탐지를 위한 결정의 일부로 사용될 수 있다는 점을 알아두는 것이 좋습니다. Anti-Spam 엔진이 URL이 스팸인 메시지를 중지하지 않으면 보안 파이프라인의 후단에서 URL 및 Outbreak Filtering으로 평가됩니다.

권장 사항: 악의적인 평판 점수가 있는 URL을 차단하고 중립 평판 점수가 있는 URL을 Cisco Security Proxy(이미지 12)로 리디렉션하는 콘텐츠 필터 규칙을 만듭니다. 메시지 수정을 활성화하여 Threat Outbreak Filter를 활성화합니다. URL 재작성을 통해 의심스러운 URL을 Cisco Security Proxy(이미지 13)에서 분석할 수 있습니다. 자세한 내용은 Configure [URL Filtering for Secure Email Gateway and Cloud Gateway를 참조하십시오.]

이미지 12. URL 평판에 대한 콘텐츠 필터



이미지 13. Outbreak Filtering에서 URL 재작성 활성화



레이어 9: Cisco ETD(Secure Email Threat Defense)로 스푸핑 탐지 기능 강화

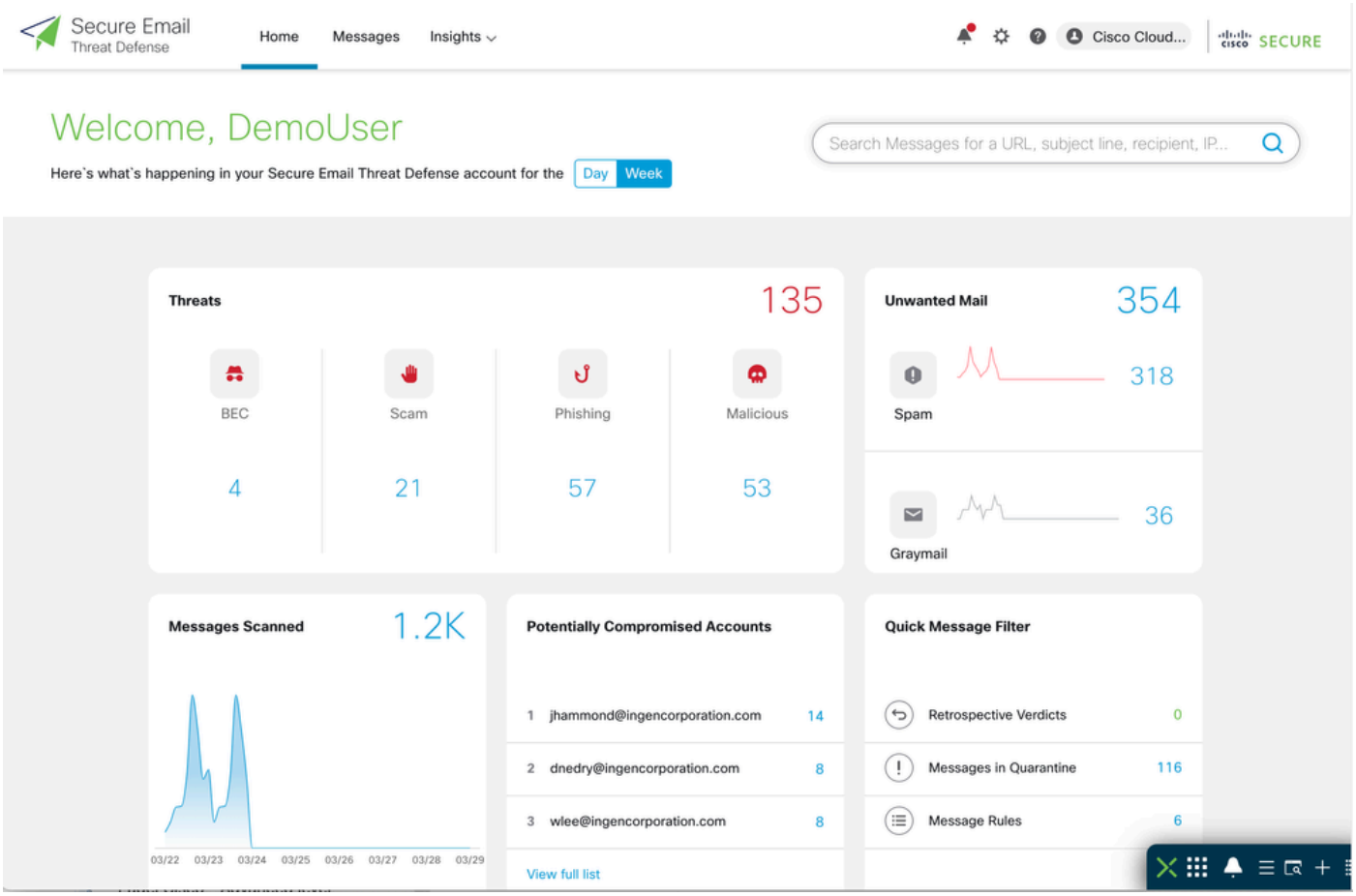
Cisco는 Cisco Talos의 탁월한 위협 인텔리전스를 활용하는 클라우드 네이티브 솔루션인 Email Threat Defense를 제공합니다. API 지원 아키텍처를 통해 응답 시간을 단축하고, 내부 이메일을 비롯한 완전한 이메일 가시성, 더 나은 상황 정보를 위한 대화 보기, Microsoft 365 사서함에 숨어 있는 위협을 자동 또는 수동으로 해결할 수 있는 도구를 제공합니다. 자세한 내용은 Cisco Secure Email Threat Defense 데이터 시트를 참조하십시오.

Cisco Secure Email Threat Defense는 발신자 인증 및 BEC 탐지 기능을 사용하여 피싱을 차단합니다. 머신 러닝과 인공 지능 엔진이 통합되어 로컬 신원 및 관계 모델링과 실시간 행동 분석을 결합하여 신원 기만 기반 위협으로부터 보호합니다. 조직 내에서 그리고 개인 간에 신뢰받는 이메일 동작을 모델링합니다. Email Threat Defense는 다른 주요 기능 중에서 다음과 같은 이점을 제공합니다.

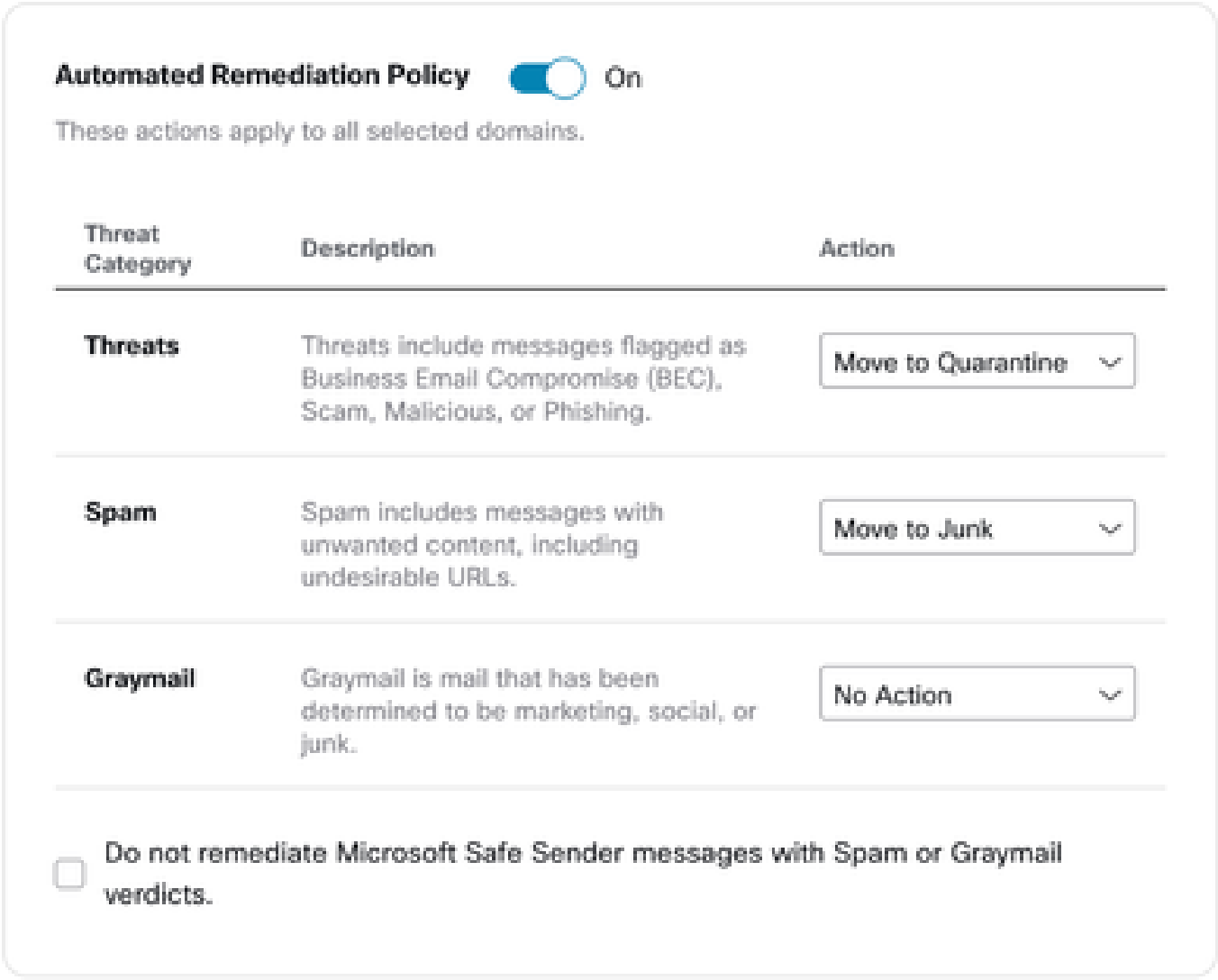
- 지능형 위협 탐지 기능으로 알려진 위협, 새로운 위협, 표적 위협을 찾아냅니다.
- 악의적인 기술을 식별하고 특정 비즈니스 위험에 대한 컨텍스트를 확보합니다.
- 위험한 위협을 신속하게 검색하고 실시간으로 치료합니다.
- 검색 가능한 위협 텔레메트리를 활용하여 위협을 분류하고 조직의 어느 부분이 공격에 가장 취약한지 파악합니다.

그림 14. Cisco Secure Email Threat Defense는 조직이 어떻게 표적이 되고 있는지에 대한 정보를

제공합니다.



이미지 15. Cisco Email Threat Defense 정책 설정은 메시지가 선택한 위협 카테고리와 일치하는지 여부를 자동으로 결정합니다



스푸핑 방지 기능으로 무엇을 더 할 수 있습니까?

많은 스푸프는 다음과 같은 몇 가지 간단한 예방 조치로 해결할 수 있지만 이에 국한되지는 않습니다.

- HAT(Host Access Table)에 나열된 도메인을 극소수의 핵심 비즈니스 파트너로 제한합니다.
- SPOOF_ALLOW 발신자 그룹을 생성하고 모범 사례 링크에 제공된 지침을 사용하는 경우 해당 발신자 그룹의 구성원을 지속적으로 추적 및 업데이트합니다.
- 그레이메일 탐지를 활성화하고 스팸 격리에 배치합니다.

그러나 무엇보다도 SPF, DKIM 및 DMARC를 활성화하고 적절하게 구현해야 합니다. 그러나 SPF, DKIM 및 DMARC 레코드 게시에 대한 지침은 이 문서의 범위를 벗어납니다. 이에 대한 내용은 이메일 인증 모범 사례: SPF, DKIM 및 DMARC를 구축하는 최적의 방법 백서를 참조하십시오.

여기에서 설명하는 스푸핑 캠페인과 같은 이메일 공격을 해결하는 데 따르는 과제를 이해합니다. 이러한 모범 사례 구현에 대해 문의 사항이 있는 경우 Cisco 기술 지원에 문의하여 케이스를 여십시오. 또는 Cisco 어카운트 팀에 솔루션 및 설계 지침을 문의하십시오. Cisco Secure Email에 대한 자세한 내용은 Cisco Secure Email 웹 사이트를 참조하십시오.

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.