E-Mail-Spoofing erkennen und verhindern

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie E-Mail-Spoofing bei Verwendung von Cisco Secure Email erkennen und verhindern.

Voraussetzungen

Anforderungen

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

- Sichere E-Mail von Cisco

Verwendete Komponenten

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.

Informationen zu diesem Dokument

Dieses Dokument richtet sich an Cisco Kunden, Cisco Channel-Partner und Cisco Techniker, die Cisco Secure Email bereitstellen. Dieses Dokument behandelt folgende Themen:

- Was ist Email Spoofing?
- E-Mail-Spoofing-Abwehrworkflow
- Was können Sie noch mit Spoofing-Prävention tun?

Was ist E-Mail-Spoofing

E-Mail-Spoofing ist eine Fälschung von E-Mail-Headern, bei der die Nachricht von einer anderen Person oder einem anderen Ort als der tatsächlichen Quelle stammt. E-Mail-Spoofing wird in Phishing- und Spam-Kampagnen verwendet, da die Wahrscheinlichkeit höher ist, eine E-Mail zu öffnen, wenn sie der Meinung sind, dass sie von einer legitimen, vertrauenswürdigen Quelle gesendet wurde. Weitere Informationen zu Spoofing finden Sie unter Was ist E-Mail-Spoofing und Wie erkennt man es.

E-Mail-Spoofing ist in folgende Kategorien unterteilt:

Kategorie	Beschreibung	Hauptziel
Direct Domain Spoofing	Imitieren Sie eine ähnliche Domäne im Umschlag von als Domäne des Empfängers.	Mitarbeiter
Namensdeklaration anzeigen	Der Von-Header zeigt einen legitimen Absender mit dem Namen einer Organisation. Sie werden auch als Business Email Compromise (BEC) bezeichnet.	Mitarbeiter
Identitätswechsel bei Markennamen	Der Von-Header zeigt einen legitimen Absender mit dem Markennamen einer bekannten Organisation.	Kunden/Partner
URL-basierter Phishing-Angriff	Eine E-Mail mit einer URL, die versucht, vertrauliche Daten zu stehlen oder sich beim Opfer anzumelden. Eine gefälschte E-Mail von einer Bank, in der Sie aufgefordert werden, auf einen Link zu klicken und Ihre Kontodetails zu	Mitarbeiter/Partner

	überprüfen, ist ein Beispiel für einen URL-basierten Phishing-Angriff.	
Cousin oder Look-alike Domain Attack	Der Header-Wert für den Umschlag von oder aus zeigt eine ähnliche Absenderadresse an, die eine echte Absenderadresse imitiert, um SPF- (Sender Policy Framework), DKIM- (Domain Keys Identified Mail) und DMARC-Prüfungen (Domain-based Message Authentication, Reporting and Conformance) zu umgehen.	Mitarbeiter/Partner
Kundenübernahme/kompromittierter Kunde	Sie erhalten unbefugten Zugriff auf ein echtes E-Mail-Konto, das jemandem gehört, und senden dann E-Mails an andere Opfer als rechtmäßigen E-Mail-Kontoinhaber.	Jeden

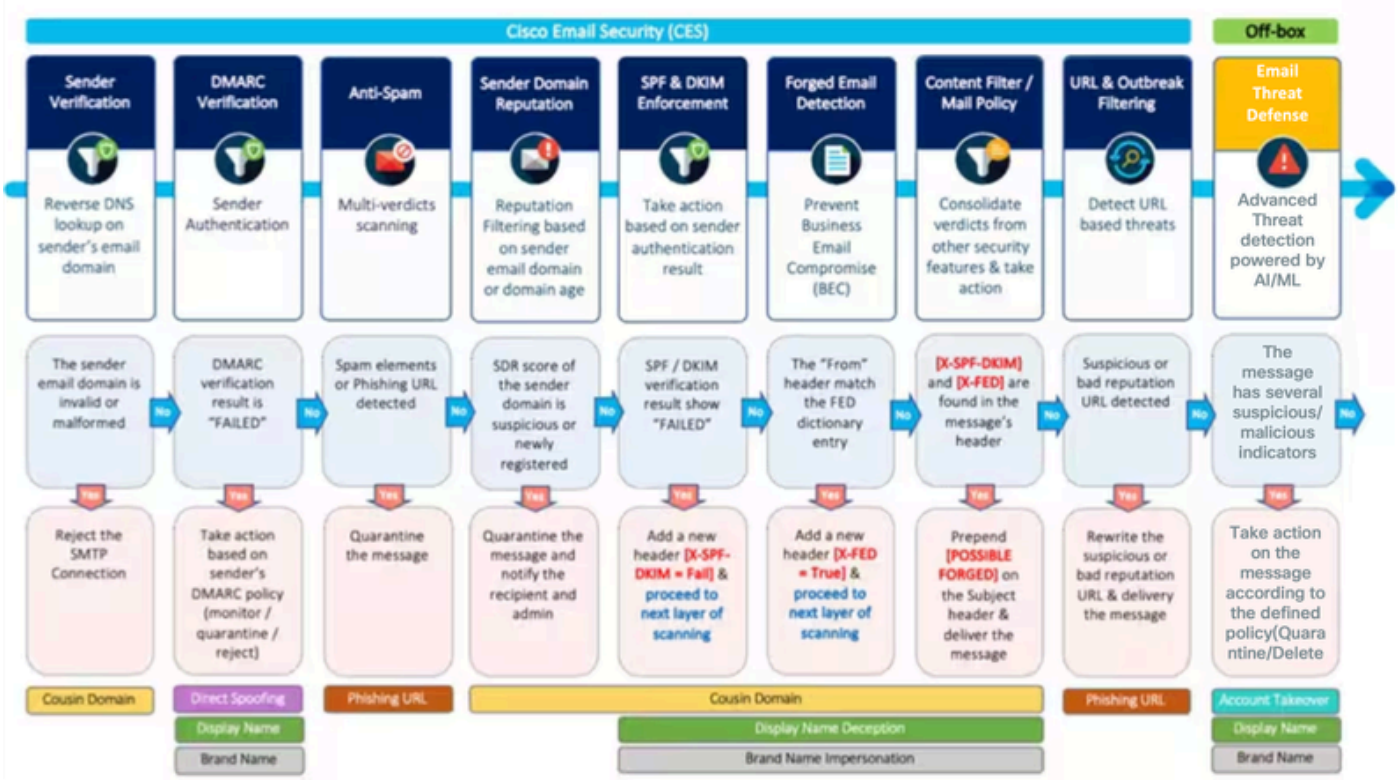
Die erste Kategorie bezieht sich auf den Missbrauch des Domain-Namens des Besitzers im Envelope From-Wert im Internet-Header einer E-Mail. Cisco Secure Email kann diesen Angriff mithilfe einer DNS-Verifizierung (Domain Name Server) des Absenders beheben, sodass nur legitime Absender zugelassen werden. Das gleiche Ergebnis kann global durch die DMARC-, DKIM- und SPF-Verifizierung erreicht werden.

Die anderen Kategorien verletzen jedoch nur teilweise den Domain-Teil der E-Mail-Adresse des Absenders. Daher ist es nicht einfach, sich abzuschrecken, wenn Sie nur DNS-Texteinträge oder die Absenderverifizierung verwenden. Im Idealfall empfiehlt es sich, einige Funktionen von Cisco Secure Email und Cisco Secure Email Threat Defense (ETD) zu kombinieren, um diese komplexen Bedrohungen abzuwehren. Wie Sie wissen, kann die Verwaltung und Konfiguration von Funktionen in Cisco Secure E-Mail von Organisation zu Organisation variieren, und unsachgemäße Anwendungen können zu einer hohen Anzahl von Fehlalarmen führen. Daher ist es wichtig, die geschäftlichen Anforderungen des Unternehmens zu verstehen und die Funktionen entsprechend anzupassen.

E-Mail-Spoofing-Abwehrworkflow

Das Diagramm zeigt die Sicherheitsfunktionen, die Best Practices für die Überwachung, Warnung und Durchsetzung gegen Spoofing-Angriffe darstellen (Abbildung 1). Die Details der einzelnen Funktionen werden in diesem Dokument bereitgestellt. Die Best Practice besteht in einem tief greifenden Abwehransatz zur Erkennung von E-Mail-Spoofing. Angreifer können ihre Methoden in einer Organisation im Laufe der Zeit ändern, sodass ein Administrator alle Änderungen überwachen und die entsprechenden Warnungen und Durchsetzungsmaßnahmen überprüfen muss.

Bild 1. Cisco Secure Email Spoof Defense-Pipeline

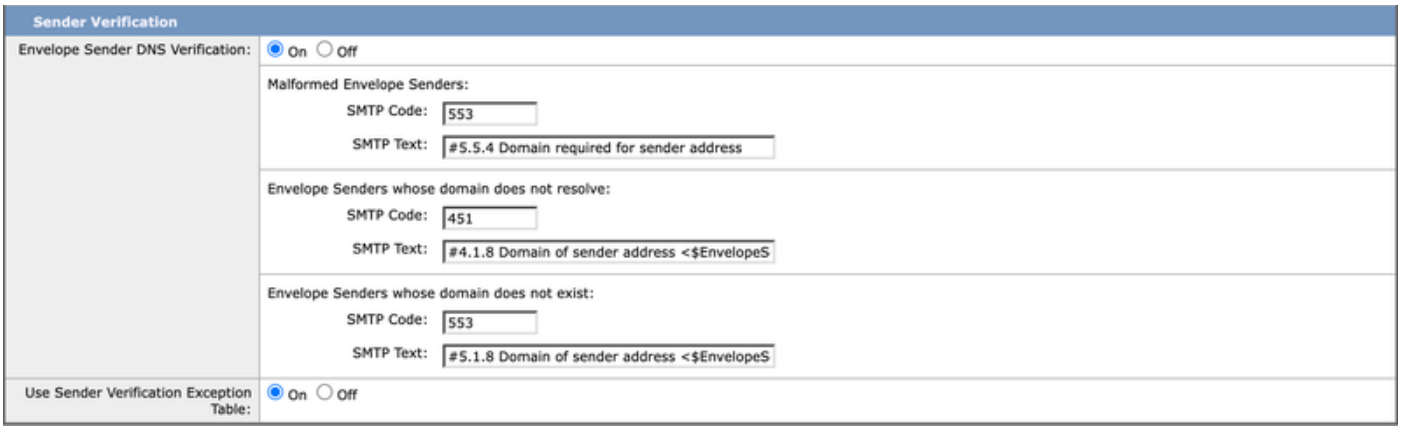


Layer 1: Gültigkeitsprüfung der Domäne des Absenders

Die Absenderverifizierung ist eine einfachere Methode, um E-Mails zu verhindern, die von einer gefälschten E-Mail-Domäne gesendet werden, wie etwa Cousin-Domain-Spoofing (c1sc0.com ist beispielsweise der Betrüger von cisco.com). Cisco Secure Email führt eine MX-Datensatzabfrage für die Domäne der E-Mail-Adresse des Absenders durch und führt während des SMTP-Gesprächs eine A-Datensatzsuche für den MX-Datensatz durch. Wenn die DNS-Abfrage NXDOMAIN zurückgibt, kann die Domäne als nicht vorhanden behandelt werden. Es ist eine gängige Methode für Angreifer, die Informationen des Umschlagabsenders zu fälschen, sodass die E-Mail eines nicht verifizierten Absenders akzeptiert und weiter verarbeitet wird. Cisco Secure Email kann alle eingehenden Nachrichten, die nicht verifiziert werden konnten und diese Funktion verwenden, zurückweisen, es sei denn, die Domäne oder IP-Adresse des Absenders wurde zuvor in der Ausnahmetabelle hinzugefügt.

Best Practice: Konfigurieren Sie Cisco Secure Email, um die SMTP-Konversation abzulehnen, wenn die E-Mail-Domäne des Umschlagabsenderfelds ungültig ist. Zulassen legitimer Absender durch Konfigurieren der Mail Flow-Richtlinie, der Absenderverifizierung und der Ausnahmetabelle (optional). Weitere Informationen finden Sie unter Schutz vor Spoof mithilfe der Absenderverifizierung.

Bild 2. Abschnitt "Absenderverifizierung" in der Standard-E-Mail-Fluss-Richtlinie



Layer 2: Überprüfen des Headers "From" mit DMARC

Die DMARC-Verifizierung ist eine viel leistungsfähigere Funktion zur Bekämpfung von Direct Domain Spoofing und umfasst auch Display Name- und Brand Impersonation-Angriffe. DMARC verknüpft mit SPF authentifizierte Informationen oder DKIM (sendende Domänenquelle oder Signatur) mit dem, was dem Endempfänger im Von-Header angezeigt wird, und stellt sicher, dass SPF- und DKIM-Bezeichner mit dem FROM-Header-Bezeichner übereinstimmen.

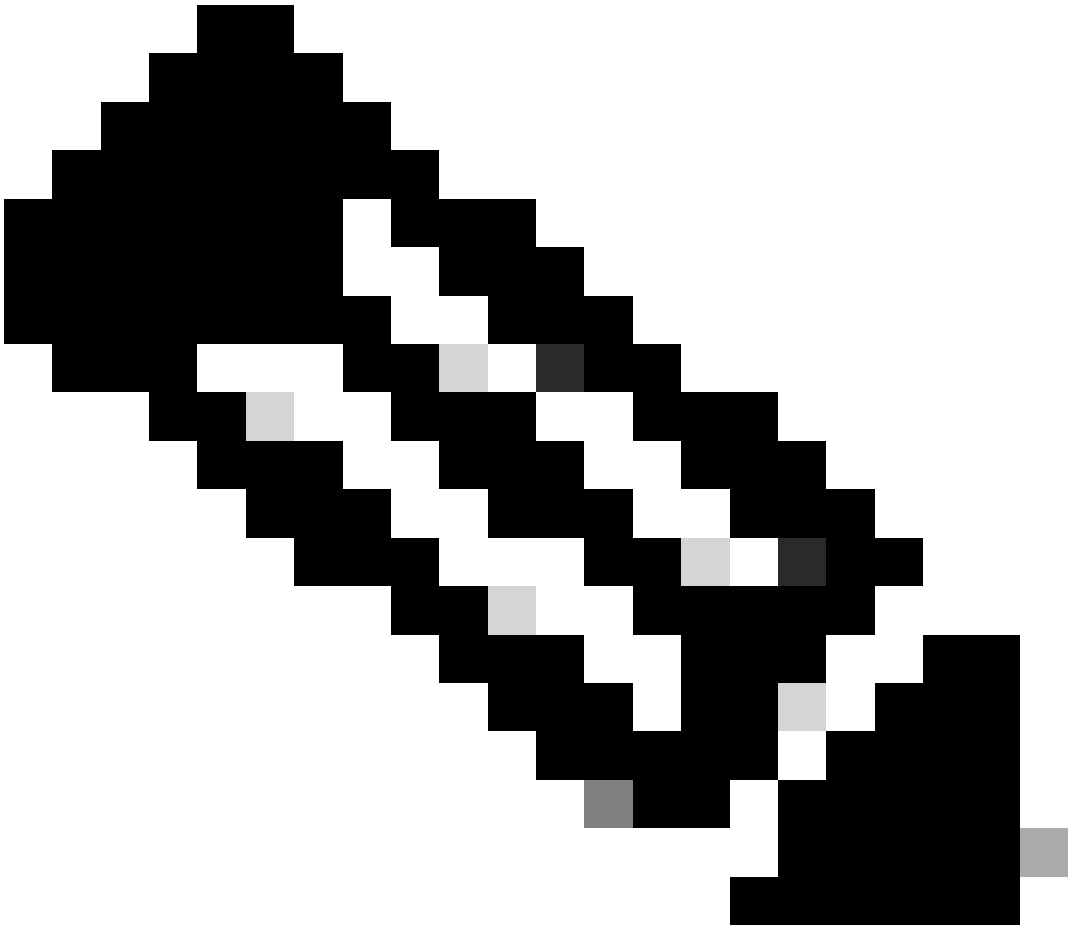
Um die DMARC-Verifizierung zu bestehen, muss eine eingehende E-Mail mindestens einen dieser Authentifizierungsmechanismen übergeben. Darüber hinaus kann der Administrator mit Cisco Secure Email ein DMARC-Verifizierungsprofil definieren, das die DMARC-Richtlinien des Domäneninhabers außer Kraft setzt und aggregierte (RUA) und fehlerhaft/forensische (RUF) Berichte an die Domäneninhaber sendet. Dies trägt dazu bei, die Authentifizierungsbereitstellungen im Gegenzug zu stärken.

Best Practice: Bearbeiten Sie das standardmäßige DMARC-Profil, das die vom Absender empfohlenen DMARC-Richtlinienaktionen verwendet. Darüber hinaus müssen die globalen Einstellungen der DMARC-Verifizierung bearbeitet werden, um eine korrekte Berichterstellung zu ermöglichen. Sobald das Profil entsprechend konfiguriert wurde, muss der DMARC-Überprüfungsdienst in der Standardrichtlinie für Mail Flow Policies aktiviert werden.

Bild 3. DMARC-Verifizierungsprofil

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.



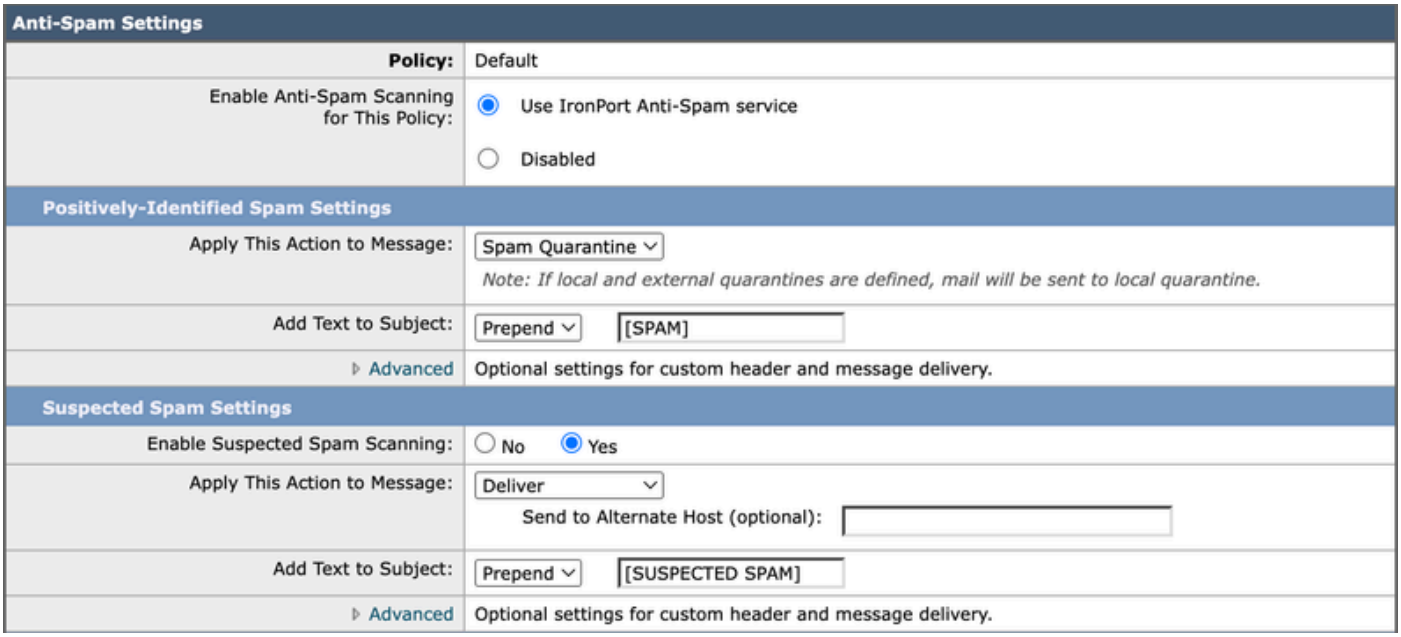
Hinweis: DMARC muss implementiert werden, indem der Eigentümer der Domäne in Verbindung mit einem Domänenüberwachungstool, wie Cisco Domain Protection, gesendet wird. Bei entsprechender Implementierung trägt die DMARC-Durchsetzung in Cisco Secure Email zum Schutz vor Phishing-E-Mails bei, die an Mitarbeiter von nicht autorisierten Absendern oder Domänen gesendet werden. Weitere Informationen zu Cisco Domain Protection finden Sie unter: Cisco Secure Email Domain Protection - Informationen auf einen Blick.

Layer 3: Verhindern, dass Spammer gefälschte E-Mails versenden

Spoofing-Angriffe können eine weitere häufige Form einer Spam-Kampagne sein. Um betrügerische E-Mails mit Spam-/Phishing-Elementen wirksam zu identifizieren und wirksam zu blockieren, ist ein wirksamer Schutz vor Spam erforderlich. Anti-Spam bietet in Verbindung mit anderen Best-Practice-Maßnahmen, die in diesem Dokument ausführlich beschrieben werden, die besten Ergebnisse, ohne den Verlust legitimer E-Mails.

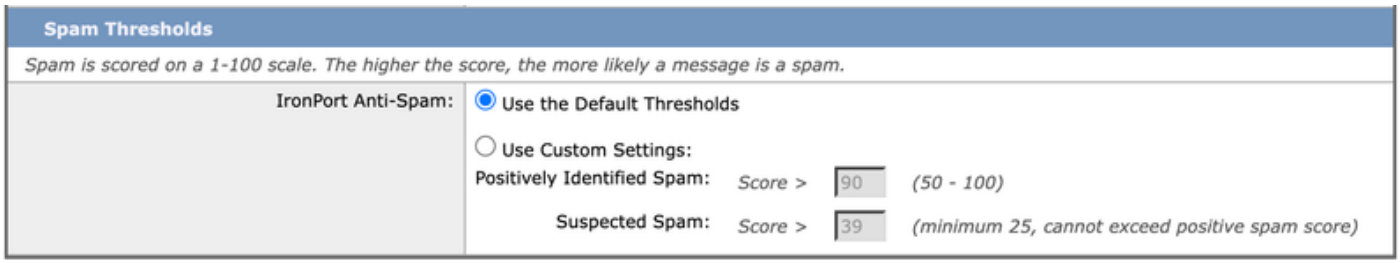
Best Practice: Aktivieren Sie den Anti-Spam-Scan in der Standard-E-Mail-Richtlinie, und legen Sie die Quarantäne-Aktion fest, um Spam-Einstellungen positiv zu identifizieren. Erhöhen Sie die Mindestgröße für das Scannen von Spam-Nachrichten auf mindestens 2 Mio. weltweit.

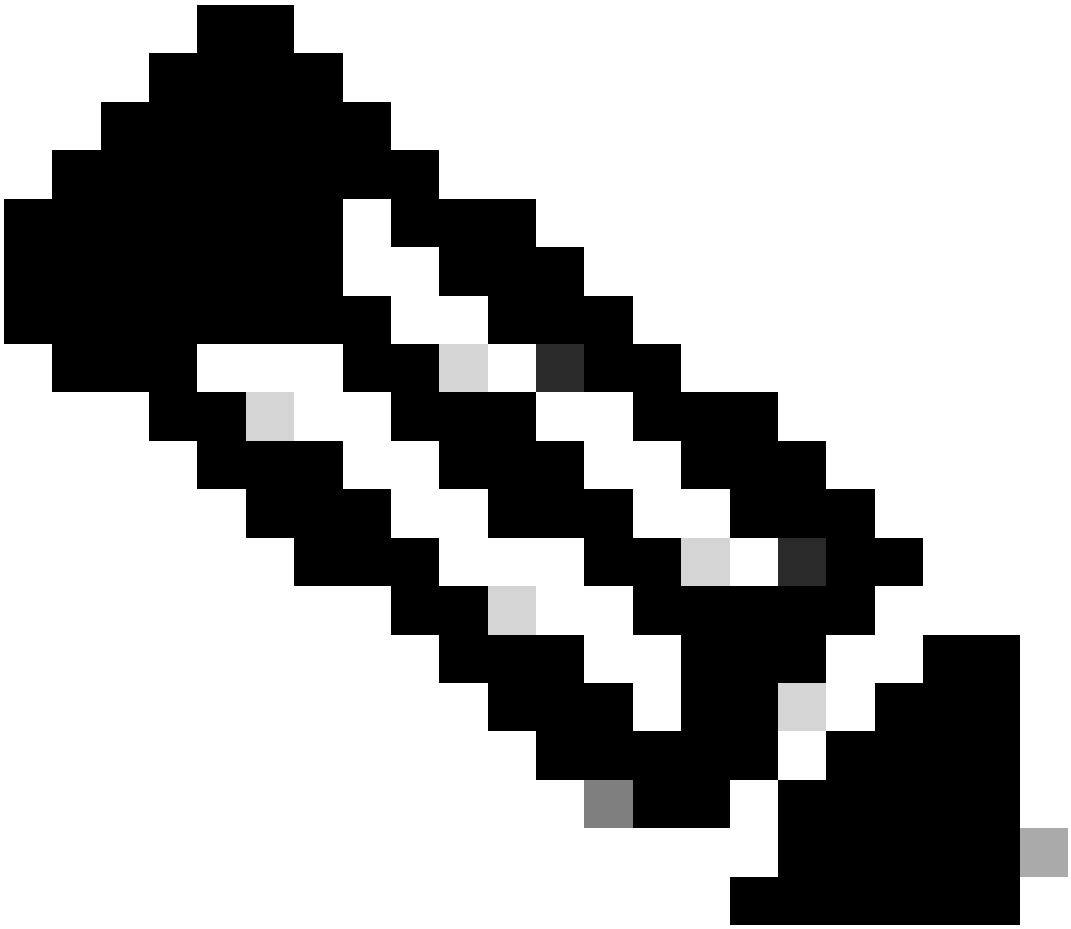
Abbildung 4: Anti-Spam-Einstellung in Standard-Mail-Richtlinie



Der Spam-Schwellenwert kann für positiven und vermuteten Spam angepasst werden, um die Empfindlichkeit zu erhöhen oder zu verringern (Abbildung 5). Cisco rät dem Administrator jedoch davon ab, dies zu tun, und verwendet nur die Standardschwellenwerte als Ausgangspunkt, sofern Cisco nichts anderes bestimmt.

Bild 5. Anti-Spam-Schwellenwerte in Standard-Mail-Richtlinie festlegen





> Hinweis: Cisco Secure Email bietet eine zusätzliche intelligente Multi-Scan (IMS)-Engine, die verschiedene Kombinationen von der Anti-Spam-Engine bietet, um die Spam-Abfangrate (die aggressivste Abfangrate) zu erhöhen.

Layer 4: Ermittlung schädlicher Absender über E-Mail-Domäne

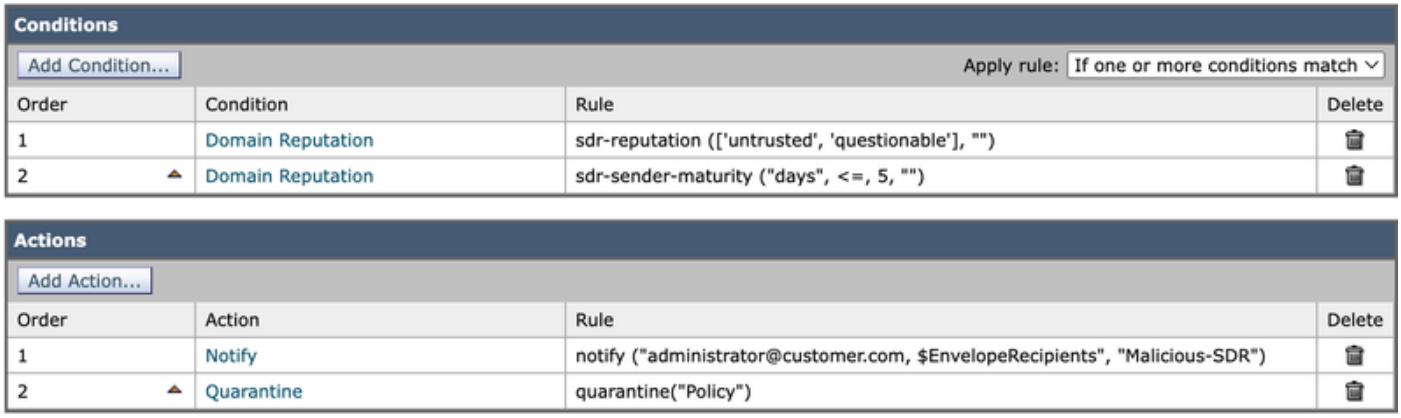
Cisco Talos Sender Domain Reputation (SDR) ist ein Cloud-Service, der anhand der Domänen im E-Mail-Umschlag und -Header die Reputation von E-Mail-Nachrichten beurteilt. Die domänenbasierte Reputationsanalyse ermöglicht eine höhere Spam-Abfangrate, da sie über die Reputation von gemeinsam genutzten IP-Adressen, Hosting-Diensten oder Infrastrukturanbietern

hinausgeht. Stattdessen werden Urteile abgeleitet, die auf Funktionen basieren, die mit vollqualifizierten Domänennamen (Fully Qualified Domain Names, FQDNs) und anderen Absenderinformationen in der SMTP-Konversation (Simple Mail Transfer Protocol) und Nachrichtenheadern verknüpft sind.

Die Absenderreife ist eine wichtige Funktion, um die Reputation des Absenders festzustellen. Die Absenderreife wird automatisch für die Spam-Klassifizierung auf der Grundlage mehrerer Informationsquellen generiert und kann sich vom Whois-basierten Domänenalter unterscheiden. Die Reife des Absenders ist auf 30 Tage begrenzt. Darüber hinaus gilt eine Domäne als reif für den E-Mail-Absender, und es werden keine weiteren Details angegeben.

Best Practice: Erstellen Sie einen eingehenden Content-Filter, der die Sendedomäne erfasst, in der das SDR-Reputationsurteil entweder unter "Untrusted/Questionable" fällt, oder die Reife des Absenders beträgt höchstens 5 Tage. Die empfohlene Aktion besteht darin, die Nachricht unter Quarantäne zu stellen und den E-Mail-Sicherheitsadministrator und den ursprünglichen Empfänger zu benachrichtigen. Weitere Informationen zur SDR-Konfiguration finden Sie im Cisco Video unter Cisco Email Security Update (Version 12.0): Sender Domain Reputation (SDR).

Bild 6. Content-Filter für SDR-Reputation und Domain-Alter mit Benachrichtigungs- und Quarantäneaktionen.



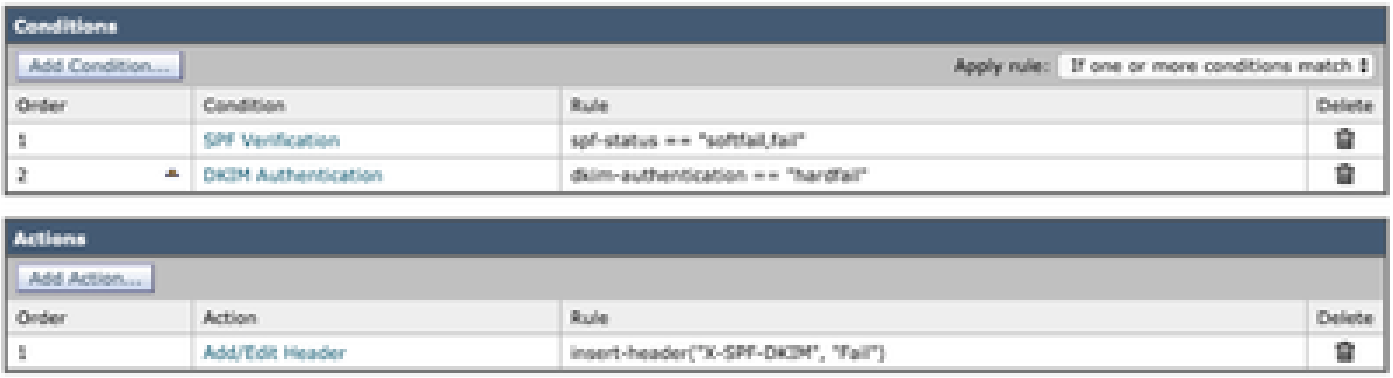
Layer 5: Reduzierung von Fehlalarmen mit SPF- oder DKIM-Verifizierungsergebnissen

Es ist zwingend erforderlich, die SPF- oder DKIM-Verifizierung (beide oder eine) durchzusetzen, um für die meisten Angriffstypen eine mehrschichtige Spoof-E-Mail-Erkennung zu ermöglichen. Anstatt eine abschließende Aktion (z. B. Löschen oder Quarantäne) durchzuführen, empfiehlt Cisco, der Nachricht, die die SPF- oder DKIM-Verifizierung nicht besteht, einen neuen Header wie [X-SPF-DKIM] hinzuzufügen und das Ergebnis mit der später behandelten Funktion für die Erkennung gefälschter E-Mails (FED) zu kombinieren. Dies trägt zu einer verbesserten Abfangrate von Spoofing-E-Mails bei.

Best Practice: Erstellen Sie einen Content-Filter, der die SPF- oder DKIM-Verifizierungsergebnisse jeder eingehenden Nachricht überprüft, die frühere Prüfungen bestanden hat. Fügen Sie einen neuen X-Header (z. B. X-SPF-DKIM=Fail) für die Nachricht hinzu, die die SPF- oder DKIM-Verifizierung nicht besteht und an die nächste Scan-Ebene weitergeleitet wird -

die Erkennung gefälschter E-Mails (FED).

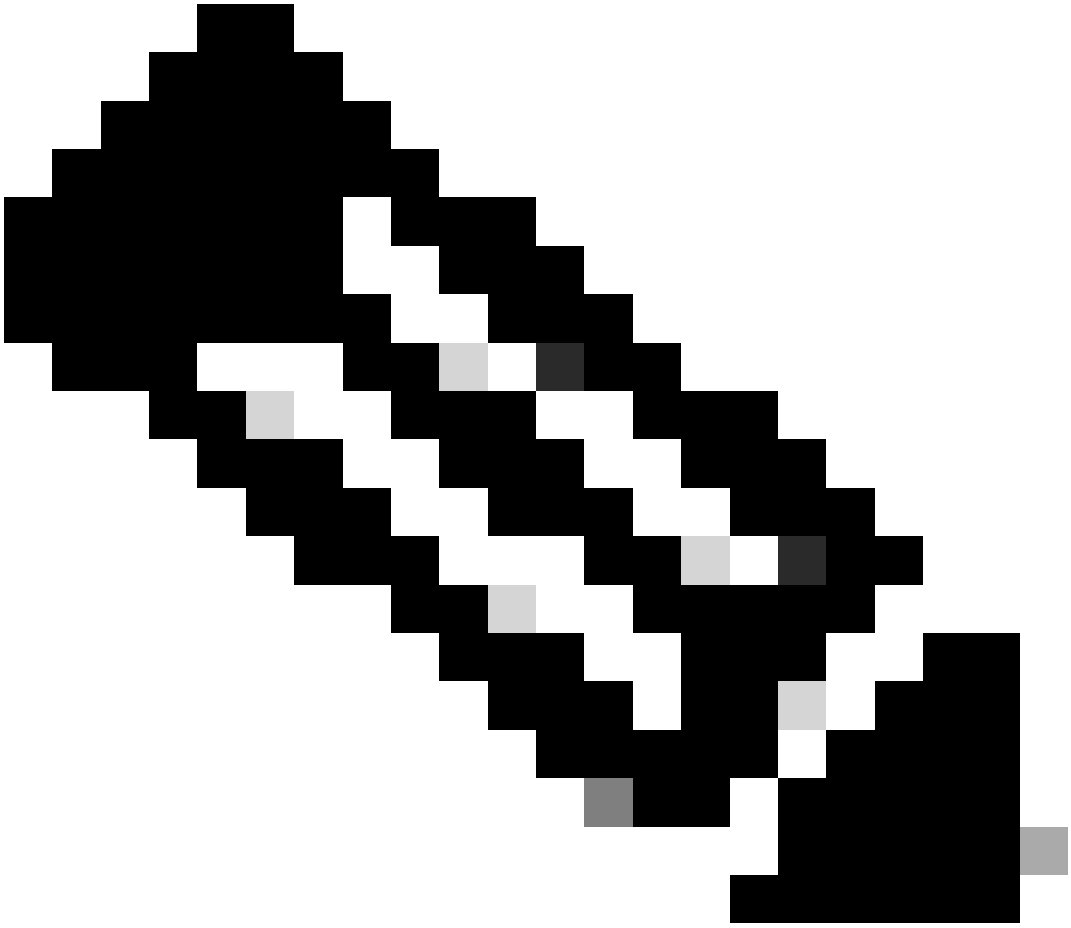
Bild 7. Content-Filter, der Nachrichten mit fehlgeschlagenen SPF- oder DKIM-Ergebnissen überprüft



Ebene 6: Nachrichten mit möglicherweise gefälschtem Absendernamen erkennen

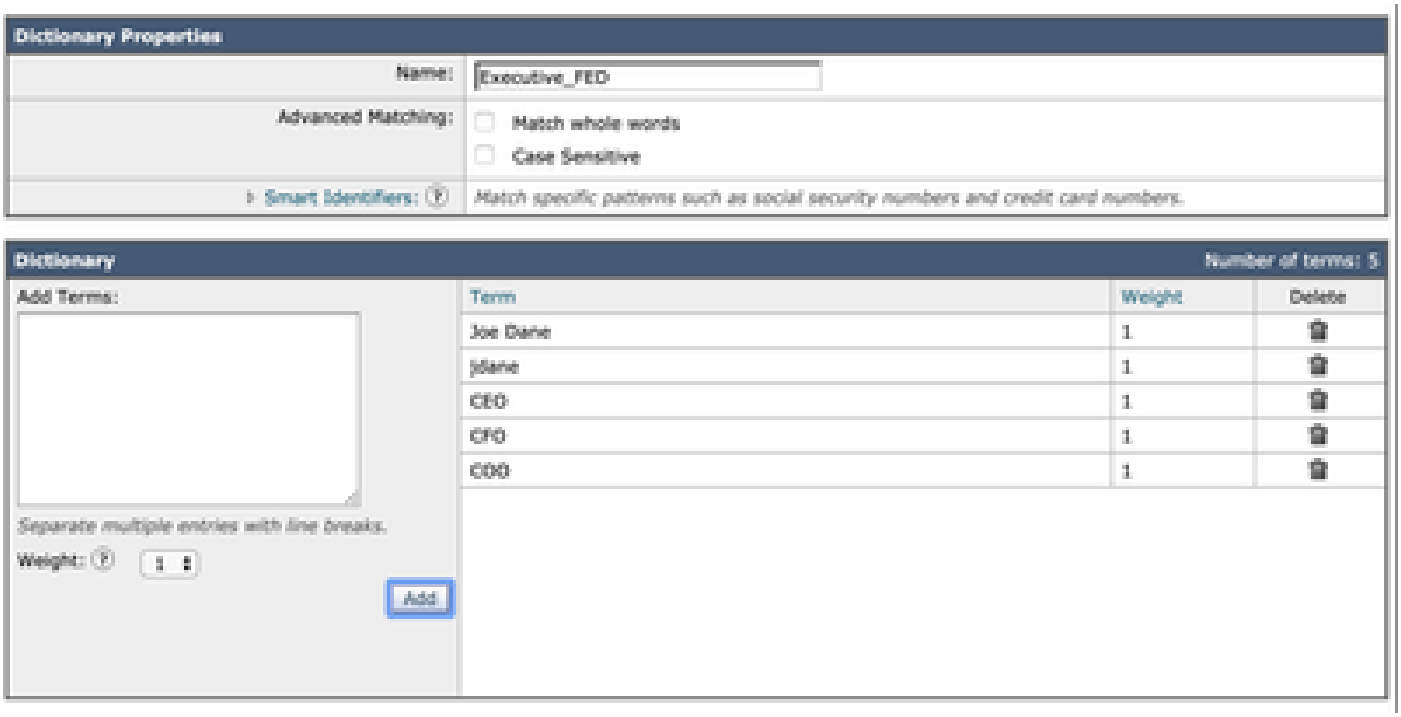
Ergänzend zu SPF-, DKIM- und DMARC-Prüfungen ist die Erkennung gefälschter E-Mails (FED) eine weitere wichtige Verteidigungslinie gegen E-Mail-Spoofing. Die FED ist ideal für die Beseitigung von Spoofangriffen, die den From-Wert im Nachrichtentext missbrauchen. Da Sie die Namen von Führungskräften innerhalb der Organisation bereits kennen, können Sie ein Wörterbuch dieser Namen erstellen und dieses Wörterbuch dann mit der FED-Bedingung in Content-Filtern referenzieren. Darüber hinaus können Sie, abgesehen von den Namen von Führungskräften, ein Wörterbuch mit Cousins oder Domains mit ähnlichen Merkmalen erstellen, die auf Ihrer Domain basieren, indem Sie DNSTWIST (DNSTWIT) verwenden, um gegen Domainspoofing mit ähnlichen Merkmalen zu konkurrieren.

Best Practice: Identifizieren Sie die Benutzer in Ihrer Organisation, deren Nachrichten wahrscheinlich gefälscht sind. Erstellen Sie ein benutzerdefiniertes Wörterbuch, das Führungskräfte berücksichtigt. Für jeden Namen einer Führungskraft muss das Wörterbuch den Benutzernamen und alle möglichen Benutzernamen als Begriffe enthalten (Bild 8). Wenn das Wörterbuch fertig ist, können Sie im Content-Filter die Option "Gefälschte E-Mail-Erkennung" verwenden, um den Wert "Von" von eingehenden Nachrichten mit diesen Wörterbucheinträgen abzugleichen.



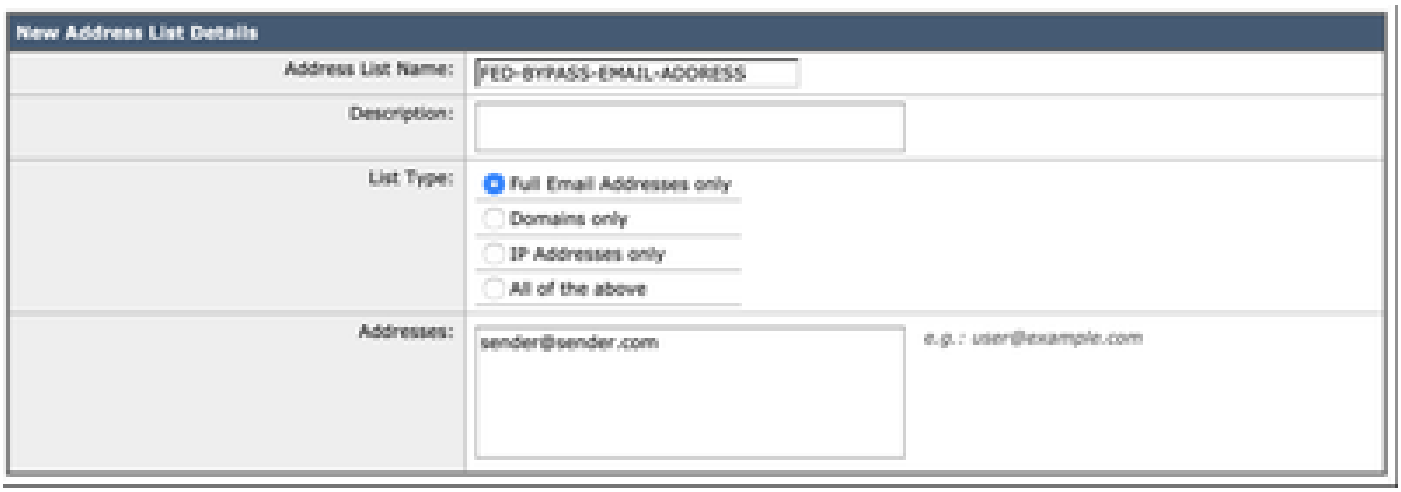
Hinweis: Da die meisten Domänen keine registrierten Permutationen sind, bietet die Überprüfung des DNS-Absenders Schutz vor diesen Domänen. Wenn Sie Wörterbucheinträge verwenden möchten, achten Sie nur auf die registrierten Domänen, und achten Sie darauf, dass 500-600 Einträge pro Wörterbuch nicht überschritten werden.

Bild 8. Benutzerdefiniertes Verzeichnis zur Erkennung gefälschter E-Mails



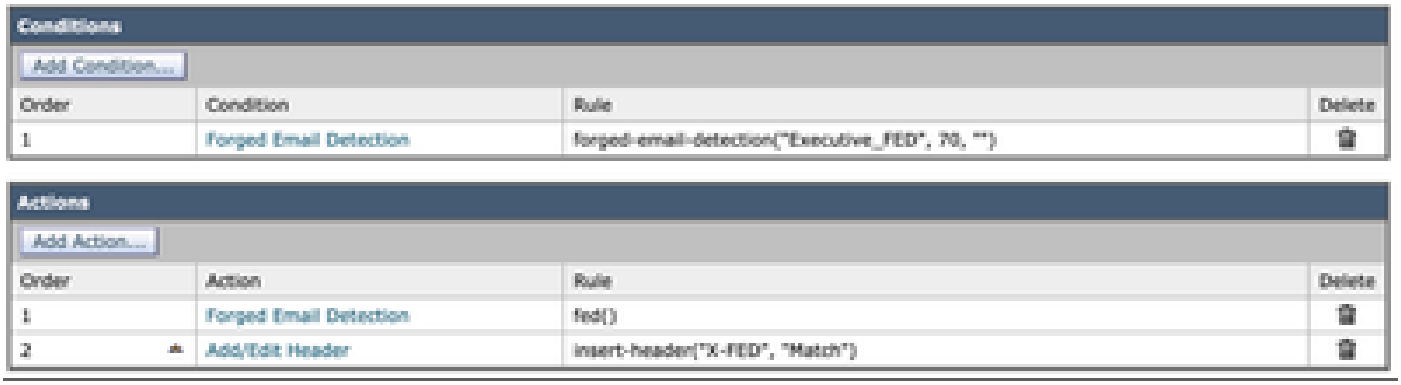
Es ist optional, eine Ausnahmebedingung für Ihre E-Mail-Domäne in Umschlag senden hinzuzufügen, um die FED-Prüfung zu umgehen. Alternativ kann eine benutzerdefinierte Adressliste erstellt werden, um die FED-Prüfung an eine Liste von E-Mail-Adressen zu übergeben, die im Formular-Header angezeigt werden (Abbildung 9).

Bild 9. Adressliste erstellen, um FED-Prüfung zu umgehen



Wenden Sie die proprietäre Aktion für die Erkennung gefälschter E-Mails an, um den Wert "Von" zu entfernen und die tatsächliche E-Mail-Adresse des Umschlagabsenders im Nachrichteneingang zu überprüfen. Fügen Sie dann einen neuen X-Header (z. B. X-FED=Match) für die Nachricht hinzu, die mit der Bedingung übereinstimmt, und senden Sie die Nachricht an die nächste Inspektionsschicht (Bild 10).

Bild 10. Empfohlene Content-Filter-Einstellung für FED

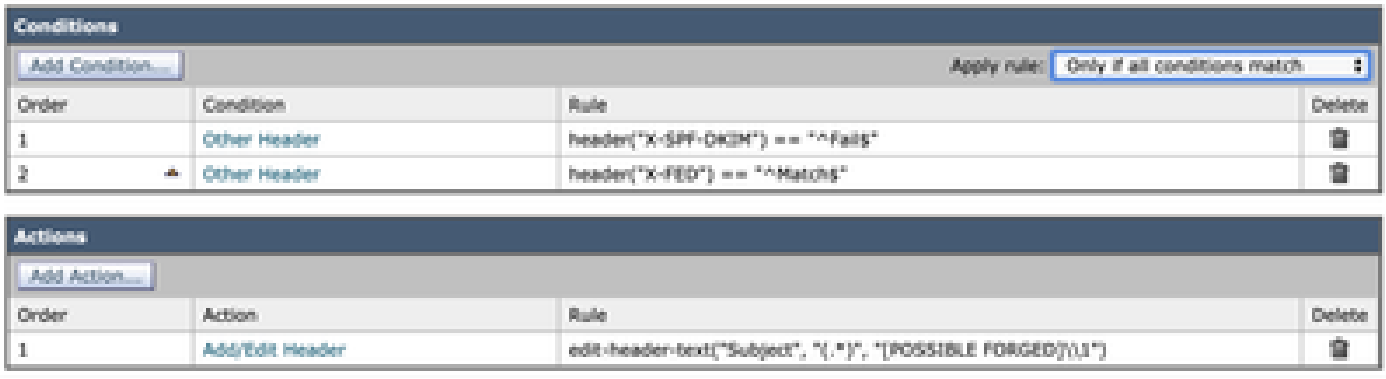


Layer 7: Positiv identifizierte Spoofing-E-Mail

Eine echte Spoofing-Kampagne zu identifizieren, ist effektiver, wenn man auf andere Urteile aus verschiedenen Sicherheitsmerkmalen in der Pipeline verweist, wie etwa die von SPF/DKIM Enforcement und FE produzierten X-Header-Informationen. Administratoren können beispielsweise einen Content-Filter erstellen, um Nachrichten zu identifizieren, die aufgrund von fehlgeschlagenen SPF/DKIM-Verifizierungsergebnissen (X-SPF-DKIM=Fail) mit den beiden neuen X-Headern hinzugefügt wurden und deren Header "From" mit den Einträgen des FED-Wörterbuchs übereinstimmt (X-FED=Match).

Die empfohlene Aktion kann darin bestehen, die Nachricht in Quarantäne zu setzen und den Empfänger zu benachrichtigen, oder die ursprüngliche Nachricht weiter zuzustellen, aber der Betreffzeile [MÖGLICHERWEISE GEFORMTE] Wörter als Warnung an den Empfänger vorzustellen, wie in Abbildung 11 dargestellt.

Bild 11. Alle X-Header in einer einzigen (endgültigen) Regel kombinieren



Layer 8: Schutz vor Phishing-URLs

Der Schutz vor Phishing-Links ist in die URL- und Outbreak-Filterung der Cisco Secure Email integriert. Kombinierte Bedrohungen kombinieren Spoofing- und Phishing-Nachrichten, um dem Ziel legitimer zu erscheinen. Die Aktivierung der Outbreak-Filterung ist entscheidend, um solche Bedrohungen in Echtzeit erkennen, analysieren und stoppen zu können. Es lohnt sich zu wissen, dass die URL-Reputation innerhalb der Anti-Spam-Engine bewertet wird und als Teil der Entscheidung für die Spam-Erkennung verwendet werden kann. Wenn die Anti-Spam-Engine die Nachricht nicht mit der URL als Spam stoppt, wird sie von der URL und der Outbreak-Filterung im

zweiten Teil der Sicherheits-Pipeline ausgewertet.

Empfehlung: Erstellen Sie eine Content-Filter-Regel, die eine URL mit einer schädlichen Reputationsbewertung blockiert und die URL mit einer neutralen Reputationsbewertung an Cisco Security Proxy weiterleitet (Abbildung 12). Aktivieren Sie die Filter für Bedrohungs-Outbreaks, indem Sie Nachrichtenänderung aktivieren. Mit URL Rewrite (URL umschreiben) kann der Cisco Security Proxy verdächtige URLs analysieren (Bild 13). Weitere Informationen finden Sie unter: Konfigurieren der URL-Filterung für Secure Email Gateway und Cloud Gateway

Bild 12. Content-Filter für URL-Reputationen

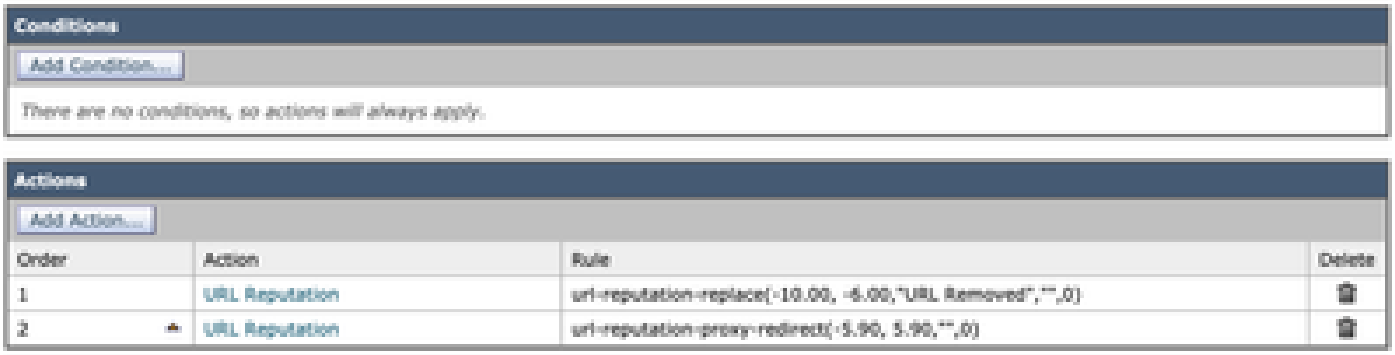
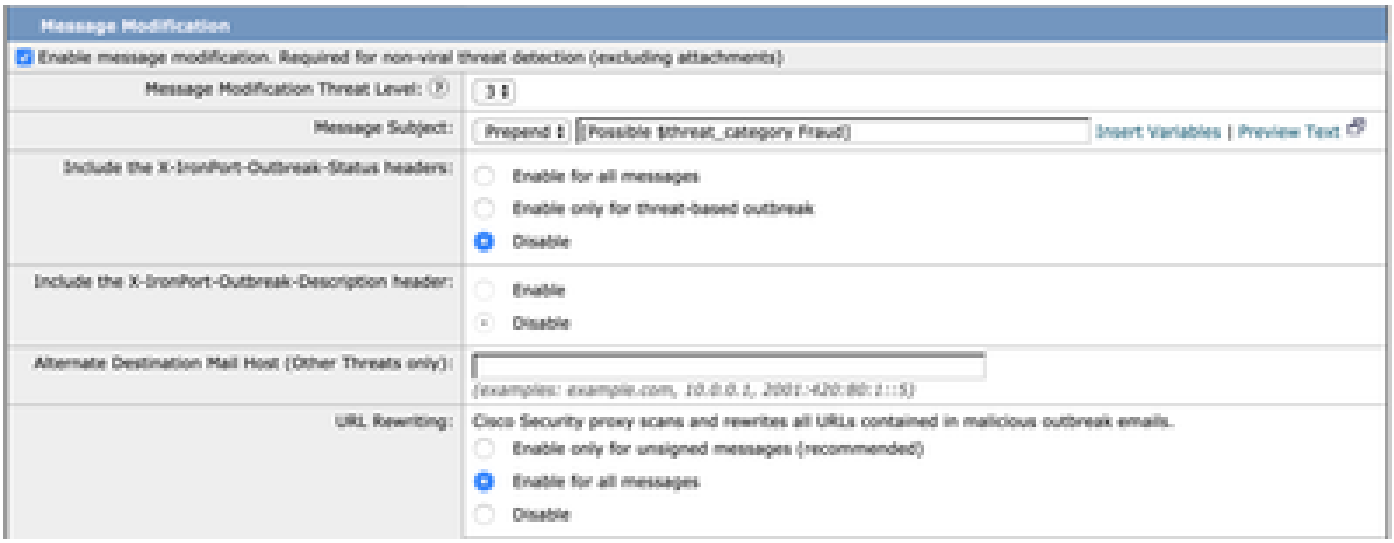


Bild 13. URL-Umschreiben bei Outbreak-Filterung aktivieren



Layer 9: Verbesserte Spoofing-Erkennung mit Cisco Secure Email Threat Defense (ETD)

Cisco bietet Email Threat Defense, eine Cloud-native Lösung, die herausragende Threat-Intelligence von Cisco Talos nutzt. Sie verfügt über eine API-fähige Architektur für schnellere Reaktionszeiten, vollständige E-Mail-Transparenz, einschließlich interner E-Mails, eine Gesprächsansicht für bessere Kontextinformationen und Tools zur automatischen oder manuellen Beseitigung von Bedrohungen, die in Microsoft 365-Mailboxen lauern. Weitere Informationen finden Sie im Datenblatt zu Cisco Secure Email Threat Defense.

Cisco Secure Email Threat Defense bekämpft Phishing mithilfe von Funktionen zur

Absenderauthentifizierung und BEC-Erkennung. Es integriert maschinelles Lernen und Engines für künstliche Intelligenz, die lokale Identitäts- und Beziehungsmodellierung mit Echtzeit-Verhaltensanalysen kombinieren, um Schutz vor auf Identitätstäuschung basierenden Bedrohungen zu bieten. Es modelliert vertrauenswürdiges E-Mail-Verhalten innerhalb von Organisationen und zwischen Einzelpersonen. Neben anderen wichtigen Funktionen bietet E-Mail Threat Defense folgende Vorteile:

- Erkennung von bekannten, neuen und zielgerichteten Bedrohungen mit erweiterten Funktionen zur Erkennung von Bedrohungen
- Identifizierung schädlicher Techniken und Kontexterfassung für spezifische Geschäftsrisiken.
- Schnelle Suche nach gefährlichen Bedrohungen und deren Behebung in Echtzeit
- Nutzen Sie durchsuchbare Bedrohungstelemetrie, um Bedrohungen zu kategorisieren und zu ermitteln, welche Bereiche Ihres Unternehmens für Angriffe am anfälligsten sind.

Abbildung 14: Cisco Secure Email Threat Defense bietet Informationen darüber, wie Ihr Unternehmen angegriffen wird.

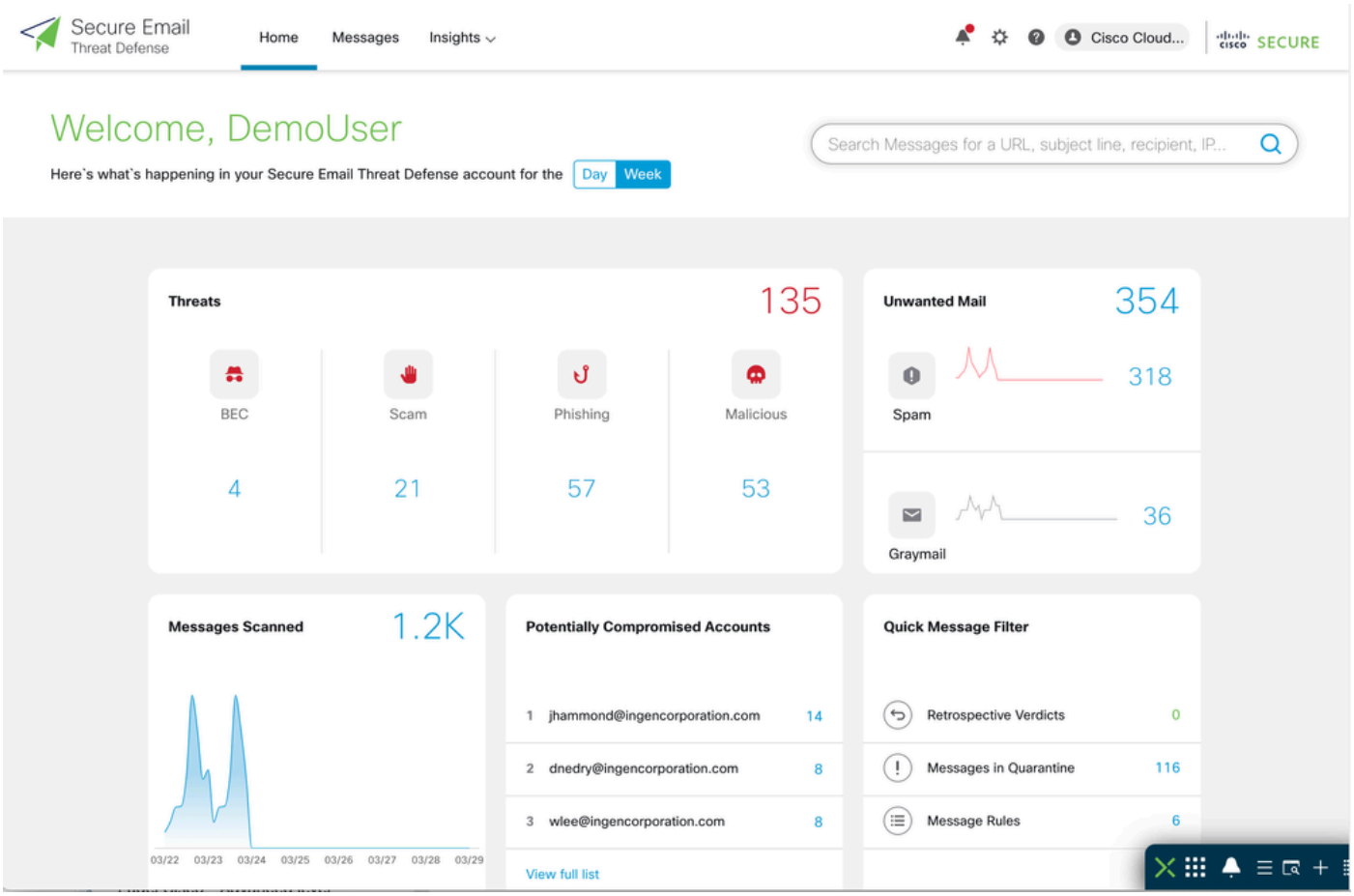
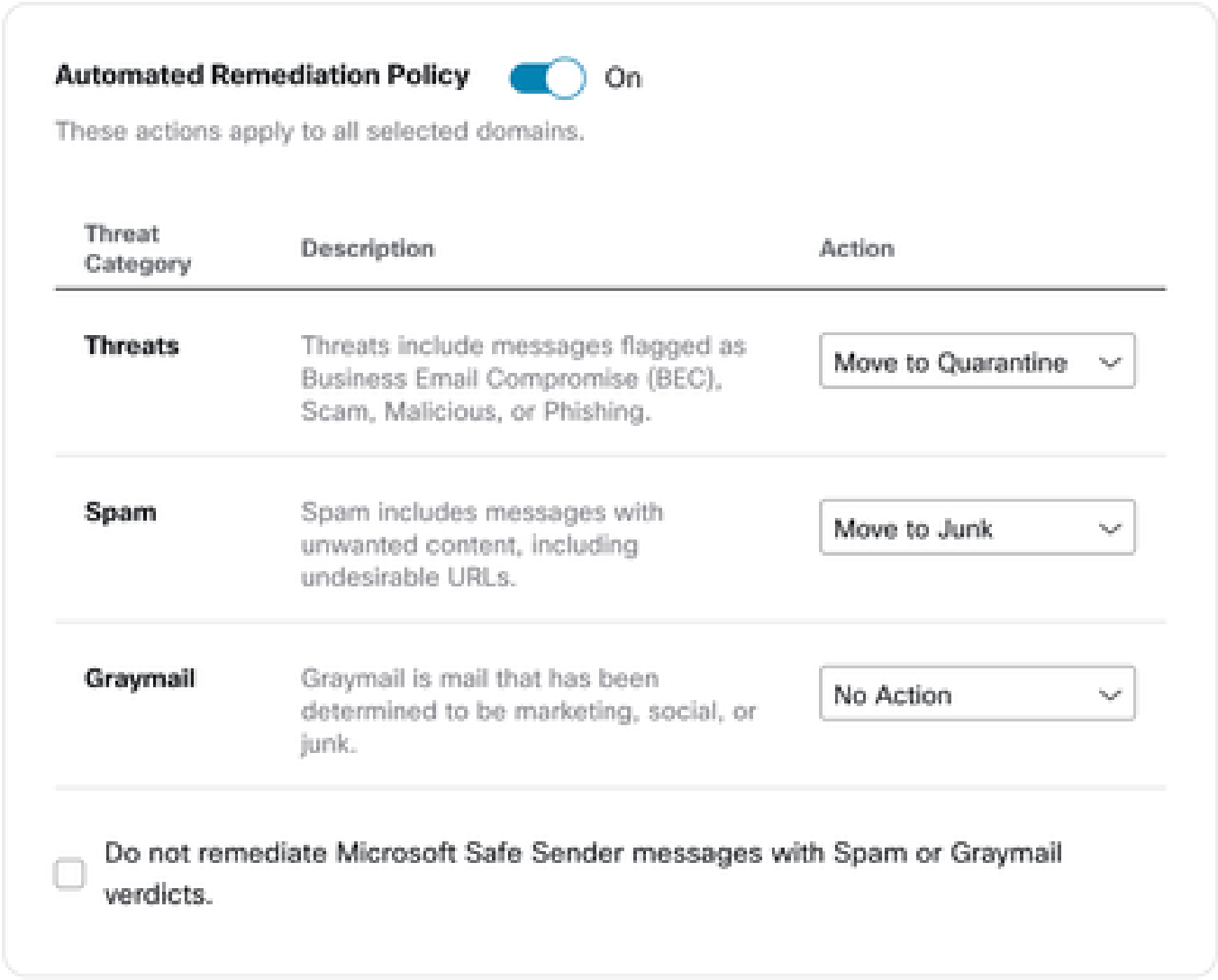


Bild 15. Die Cisco E-Mail Threat Defense-Richtlinieneinstellung bestimmt automatisch, ob die Nachricht mit der ausgewählten Bedrohungskategorie übereinstimmt.



Was können Sie noch mit Spoofing-Prävention tun?

Viele Spoofs können mit einigen einfachen Vorsichtsmaßnahmen beseitigt werden, die u. a. Folgendes umfassen:

- Einschränkung der in der Host Access Table (HAT) aufgeführten Domänen auf sehr wenige Hauptgeschäftspartner
- Sie können Mitglieder in der Absendergruppe SPOOF_ALLOW kontinuierlich nachverfolgen und aktualisieren, wenn Sie eine erstellt haben, und die Anweisungen unter dem Link "Best Practices" verwenden.
- Aktivieren Sie die Graupostenerkennung, und platzieren Sie sie auch in der Spam-Quarantäne.

Am wichtigsten ist jedoch, dass Sie SPF, DKIM und DMARC aktivieren und diese entsprechend implementieren. Die Hinweise zur Veröffentlichung von SPF-, DKIM- und DMARC-Datensätzen werden in diesem Dokument jedoch nicht behandelt. Weitere Informationen finden Sie in diesem Whitepaper: Best Practices zur E-Mail-Authentifizierung: Die optimalen Möglichkeiten zur Bereitstellung von SPF, DKIM und DMARC.

Beheben Sie E-Mail-Angriffe wie die hier vorgestellten Spoofing-Kampagnen. Wenn Sie Fragen zur Implementierung dieser Best Practices haben, wenden Sie sich an den technischen Support von Cisco, und eröffnen Sie ein Ticket. Alternativ können Sie sich auch an Ihr Cisco Account Team wenden, um eine Lösung und einen Design-Leitfaden zu erhalten. Weitere Informationen zu Cisco Secure Email finden Sie auf der Cisco Secure Email-Website.

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.