Rilevamento e prevenzione dello spoofing della posta elettronica

Sommario

Introduzione

Questo documento descrive come rilevare e impedire lo spoofing delle e-mail quando si usa Cisco Secure Email.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.

- Cisco Secure Email

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Informazioni sul documento

Questo documento è destinato ai clienti Cisco, ai partner di canale Cisco e ai tecnici Cisco che implementano Cisco Secure Email. Il presente documento riguarda:

- Che cos'è lo spoofing della posta elettronica?
- Flusso di lavoro difesa spoofing e-mail
- Cosa si può fare di più con la prevenzione dello spoofing?

Che cos'è lo spoofing della posta elettronica

Lo spoofing delle e-mail è una falsificazione dell'intestazione dell'e-mail in cui il messaggio sembra provenire da una persona o da un luogo diverso dall'origine effettiva. Lo spoofing delle e-mail viene utilizzato nelle campagne di phishing e spam perché è probabile che le persone aprano un'e-mail quando ritengono che sia stata inviata da una fonte attendibile e legittima. Per ulteriori informazioni sullo spoofing, vedere Che cos'è lo spoofing delle e-mail e come rilevarlo.

Lo spoofing delle e-mail rientra nelle seguenti categorie:

Categoria	Descrizione	Destinazione principale
Spoofing diretto dei domini	Rappresenta un dominio simile nella busta Da come dominio del destinatario.	Dipendenti
Nome visualizzato inganno	Nell'intestazione Da viene visualizzato un mittente legittimo con il nome esecutivo di un'organizzazione. Sono anche noti come BEC (Business Email Compromise).	Dipendenti
Rappresentazione del nome del marchio	L'intestazione Da mostra un mittente legittimo con il nome del marchio di un'organizzazione nota.	Clienti/partner
Attacco phishing basato su URL	Un messaggio di posta elettronica con un URL che tenta di rubare dati sensibili o di accedere alle informazioni dalla vittima. Un esempio di attacco basato su URL di phishing è un'e-mail falsa inviata da una banca che richiede di fare clic su un collegamento e verificare i dettagli dell'account.	Dipendenti/Partner

Attacco a un cugino o a un dominio simile	Il valore dell'intestazione Busta da o Da mostra un indirizzo mittente simile che rappresenta un indirizzo reale per ignorare le ispezioni Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) e Domain-based Message Authentication, Reporting and Conformance (DMARC).	Dipendenti/Partner
Presa in conto / Conto compromesso	Ottenere l'accesso non autorizzato a un account di posta elettronica reale che appartiene a qualcuno, quindi inviare e-mail ad altre vittime come legittimo proprietario dell'account di posta elettronica.	Tutti

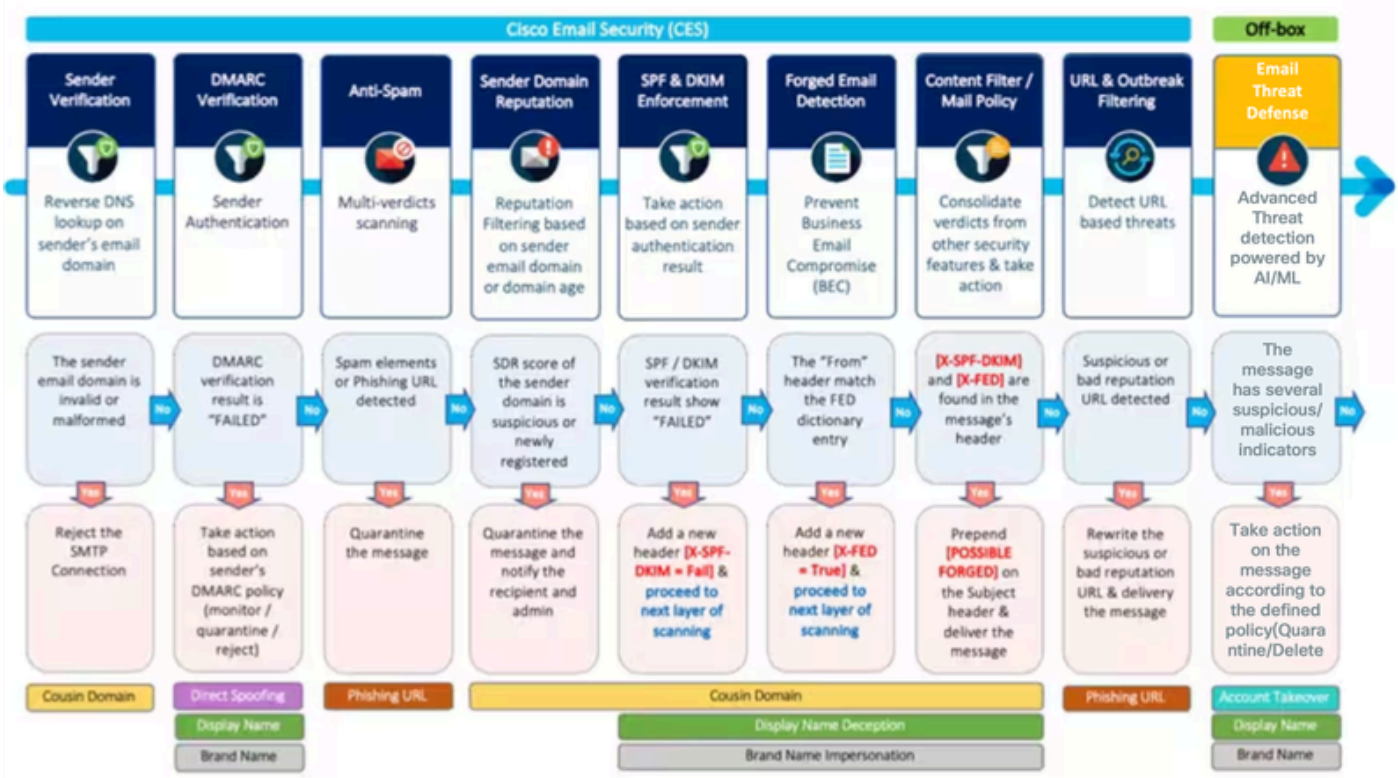
La prima categoria riguarda abusi del nome di dominio del proprietario nel valore Busta da nell'intestazione Internet di un messaggio e-mail. Cisco Secure Email può porre rimedio a questo attacco utilizzando la verifica DNS (Domain Name Server) del mittente per consentire solo i mittenti legittimi. Lo stesso risultato può essere ottenuto a livello globale utilizzando la verifica DMARC, DKIM e SPF.

Tuttavia, le altre categorie violano solo parzialmente la parte del dominio dell'indirizzo e-mail del mittente. Non è quindi facile essere scoraggiati quando si utilizzano solo record di testo DNS o la verifica del mittente. In teoria, sarebbe meglio combinare alcune funzionalità di Cisco Secure Email e Cisco Secure Email Threat Defense (ETD) per combattere queste minacce avanzate. Come è noto, l'amministrazione e la configurazione di Cisco Secure Email possono variare da un'organizzazione all'altra e un'applicazione scorretta può portare a un'elevata incidenza di falsi positivi. È quindi essenziale comprendere le esigenze aziendali dell'organizzazione e personalizzarne le caratteristiche.

Flusso di lavoro difesa spoofing e-mail

Nel diagramma sono illustrate le funzioni di sicurezza che consentono di adottare le procedure ottimali per monitorare, avvisare e impedire attacchi di tipo spoofing (immagine 1). In questo documento vengono forniti i dettagli di ciascuna funzionalità. La procedura ottimale è un approccio di difesa approfondita per rilevare lo spoofing delle e-mail. Gli aggressori possono modificare i propri metodi nei confronti di un'organizzazione nel corso del tempo, pertanto un amministratore deve monitorare qualsiasi modifica e controllare gli avvisi e l'applicazione appropriati.

Immagine 1. Cisco Secure Email Spoof Defense Pipeline

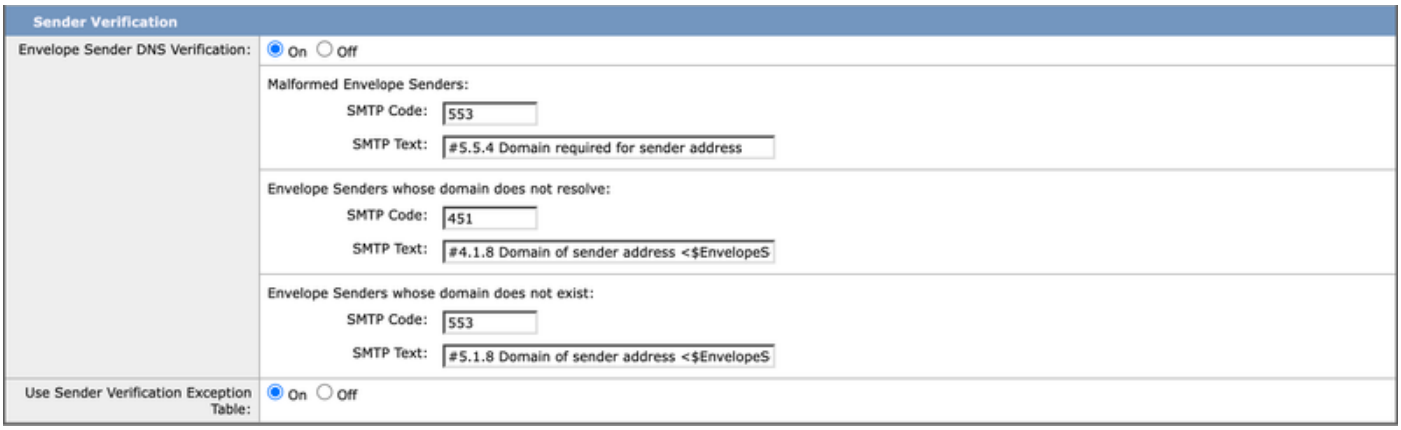


Livello 1: controllo di validità nel dominio del mittente

La verifica del mittente è un modo più semplice per impedire l'invio di e-mail da un dominio falso, come lo spoofing del dominio del cugino (ad esempio, c1sc0.com è l'impostore di cisco.com). Cisco Secure Email esegue una query sui record MX per il dominio dell'indirizzo e-mail del mittente ed esegue una ricerca dei record A sul record MX durante la conversazione SMTP. Se la query DNS restituisce NXDOMAIN, il dominio può essere considerato inesistente. È una tecnica comune per gli aggressori falsificare le informazioni del mittente della busta in modo che l'e-mail da un mittente non verificato venga accettata ed elaborata ulteriormente. Cisco Secure Email può rifiutare tutti i messaggi in arrivo che non superano il controllo di verifica che utilizza questa funzione, a meno che il dominio o l'indirizzo IP del mittente non sia stato preaggiunto nella tabella delle eccezioni.

Procedura consigliata: Configurare Cisco Secure Email per rifiutare la conversazione SMTP se il dominio di posta elettronica del campo del mittente della busta non è valido. Consenti solo mittenti legittimi configurando il criterio del flusso di posta, la verifica del mittente e la tabella delle eccezioni (facoltativo). Per ulteriori informazioni, visita la pagina relativa alla protezione da spoof mediante la verifica del mittente.

Immagine 2. Sezione verifica mittente nel criterio Flusso di posta predefinito



Livello 2: verifica dell'intestazione From mediante DMARC

La verifica DMARC è una funzione molto più potente per combattere lo spoofing diretto dei domini e include anche attacchi di visualizzazione del nome e di rappresentazione del marchio. DMARC associa le informazioni autenticate con SPF o DKIM (origine o firma del dominio di invio) a quelle presentate al destinatario finale nell'intestazione From e verifica che gli identificatori SPF e DKIM siano allineati con l'identificatore dell'intestazione FROM.

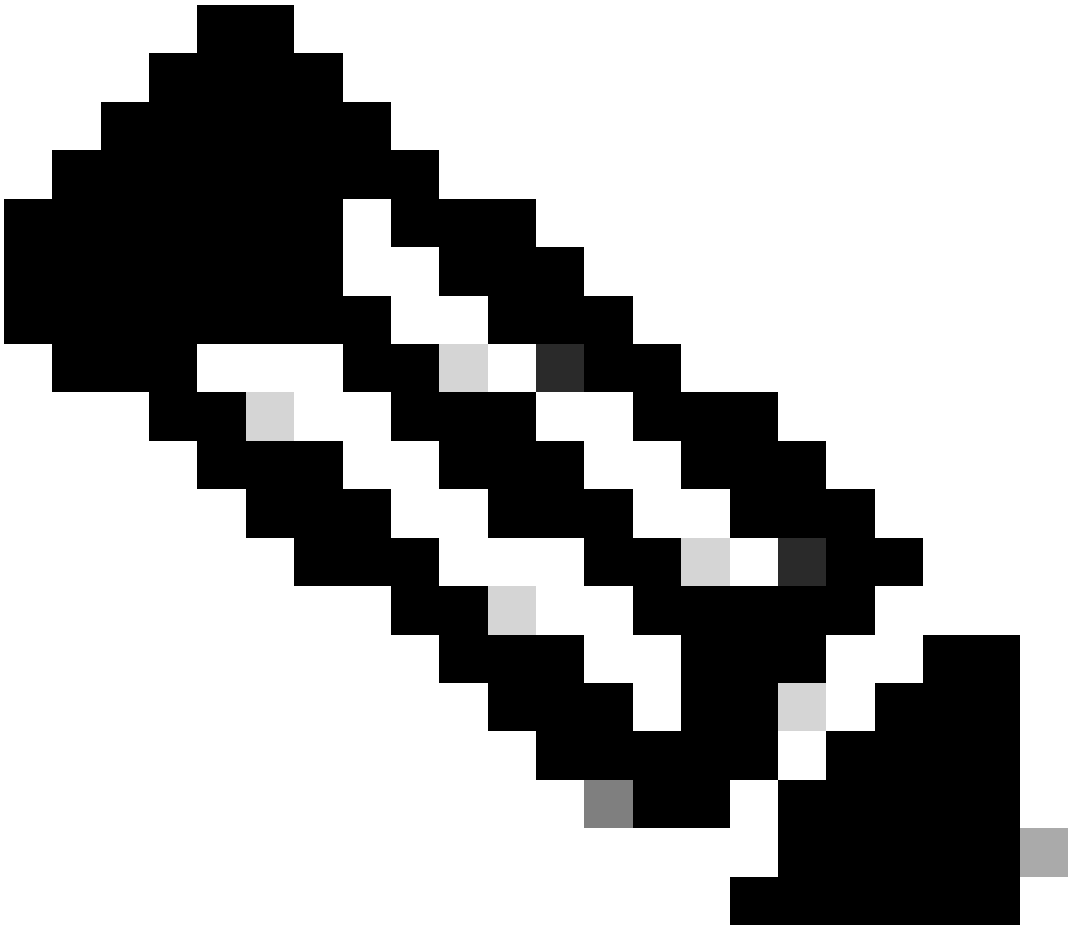
Per superare la verifica DMARC, un messaggio e-mail in arrivo deve superare almeno uno di questi meccanismi di autenticazione. Inoltre, Cisco Secure Email consente all'amministratore di definire un profilo di verifica DMARC per ignorare i criteri DMARC del proprietario del dominio e inviare rapporti di aggregazione (RUA) e di errore/indagine legale (RUF) ai proprietari del dominio. In questo modo è possibile rafforzare le distribuzioni di autenticazione in cambio.

Procedura consigliata: modificare il profilo DMARC predefinito che utilizza le azioni dei criteri DMARC consigliate dal mittente. È inoltre necessario modificare le impostazioni globali della verifica DMARC per consentire la generazione corretta del report. Dopo aver configurato il profilo in modo appropriato, è necessario abilitare il servizio di verifica DMARC nel criterio predefinito Criteri di flusso di posta.

Immagine 3. Profilo di verifica DMARC

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.



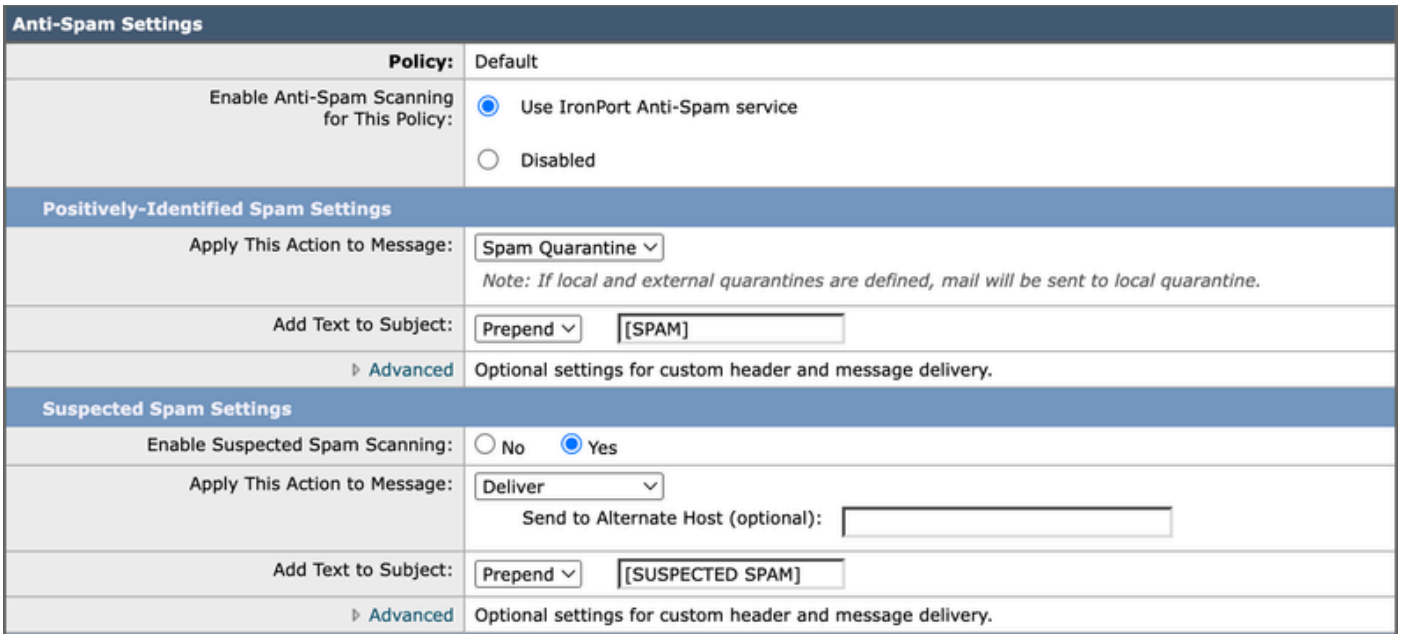
Nota: DMARC deve essere implementato inviando il proprietario del dominio insieme a uno strumento di monitoraggio del dominio, come Cisco Domain Protection. Se implementata correttamente, l'applicazione DMARC in Cisco Secure Email consente di proteggere i messaggi di phishing inviati ai dipendenti da mittenti o domini non autorizzati. Per ulteriori informazioni su Cisco Domain Protection, visitare il sito Web all'indirizzo: Cisco Secure Email Domain Protection-A-Glance.

Layer 3: Impedisci agli spammer di inviare e-mail falsificate

Gli attacchi di tipo spoofing possono costituire un'altra forma comune di campagna di posta indesiderata. Pertanto, abilitare la protezione dalla posta indesiderata è essenziale per identificare in modo efficace i messaggi di posta elettronica fraudolenti che contengono elementi di posta indesiderata/phishing e bloccarli in modo positivo. La protezione dalla posta indesiderata, combinata con altre azioni basate su procedure ottimali descritte in modo approfondito in questo documento, offre i migliori risultati senza perdere le e-mail legittime.

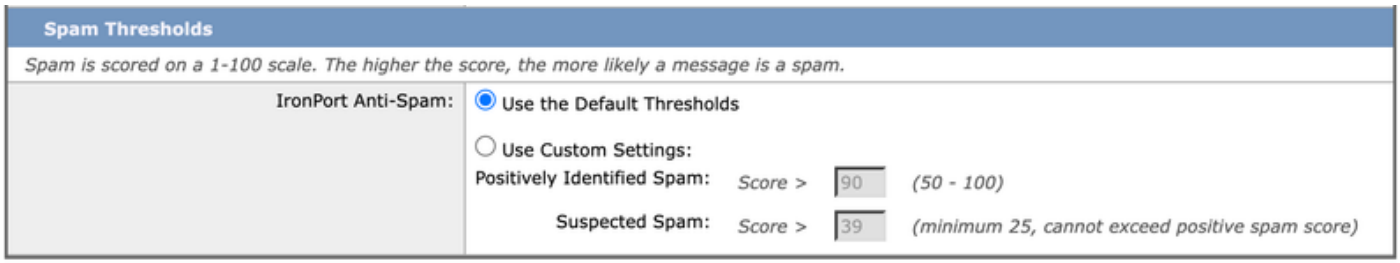
Procedura consigliata: Abilitare l'analisi della posta indesiderata nei criteri di posta predefiniti e impostare l'azione di quarantena per identificare le impostazioni della posta indesiderata in modo positivo. Aumentare le dimensioni minime di scansione per i messaggi di posta indesiderata ad almeno 2 milioni a livello globale.

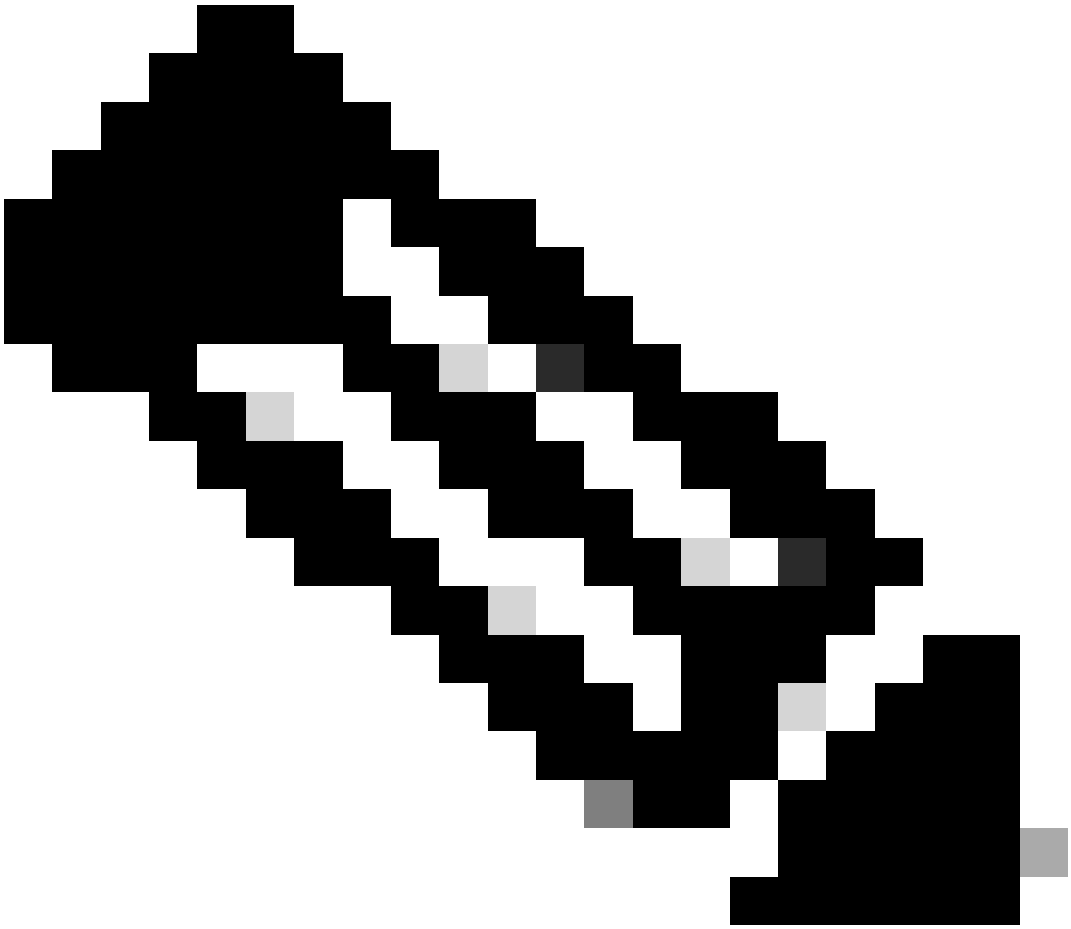
Immagine 4. Impostazione della protezione dalla posta indesiderata nei criteri di posta predefiniti



è possibile impostare la soglia per la posta indesiderata in modo da aumentare o ridurre la sensibilità della posta indesiderata (immagine 5); tuttavia, Cisco sconsiglia all'amministratore di effettuare questa operazione e di utilizzare solo le soglie predefinite come base, a meno che non venga specificato diversamente da Cisco.

Immagine 5. Impostazione delle soglie per la protezione dalla posta indesiderata nei criteri di posta elettronica predefiniti





Nota: Cisco Secure Email offre un motore IMS (Intelligent Multi-Scan) aggiuntivo che fornisce combinazioni diverse dal motore antispam per aumentare le velocità di recupero della posta indesiderata (velocità di recupero più aggressiva).

Livello 4: individuazione di mittenti dannosi tramite il dominio di posta elettronica

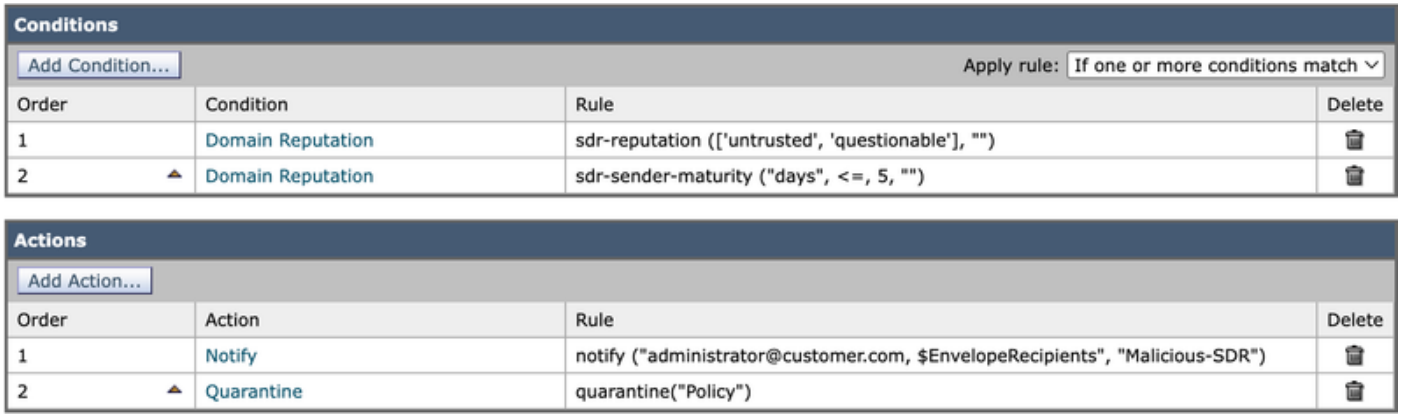
Cisco Talos Sender Domain Reputation (SDR) è un servizio cloud che fornisce un verdetto di reputazione per i messaggi e-mail basato sui domini nella busta e nell'intestazione dell'e-mail. L'analisi della reputazione basata su dominio consente una maggiore percentuale di messaggi indesiderati, guardando oltre la reputazione degli indirizzi IP condivisi, dell'hosting o dei provider

dell'infrastruttura. Al contrario, emette verdetti sulla base delle funzionalità associate ai nomi di dominio completi (FQDN) e di altre informazioni sul mittente nelle conversazioni e nelle intestazioni dei messaggi SMTP (Simple Mail Transfer Protocol).

La maturità del mittente è una caratteristica essenziale per stabilire la reputazione del mittente. La maturità del mittente viene generata automaticamente per la classificazione della posta indesiderata in base a più fonti di informazioni e può differire dall'età del dominio basato su Whois. La scadenza del mittente è impostata su un limite di 30 giorni e oltre questo limite, un dominio viene considerato maturo come mittente di posta elettronica e non vengono forniti ulteriori dettagli.

Procedura ottimale: creare un filtro dei contenuti in arrivo che acquisisca il dominio di invio in cui il verdetto sulla reputazione dell'SDR rientra in Non attendibile/Discutibile oppure la maturità del mittente è inferiore o uguale a 5 giorni. L'azione consigliata è quella di mettere in quarantena il messaggio e avvisare l'amministratore della sicurezza della posta elettronica e il destinatario originale. Per ulteriori informazioni su come configurare l'SDR, vedere il video di Cisco all'indirizzo Cisco Email Security Update (versione 12.0): Sender Domain Reputation (SDR) (informazioni in lingua inglese).

Immagine 6. Filtro dei contenuti per la reputazione dell'SDR e l'età del dominio con le azioni di notifica e quarantena.

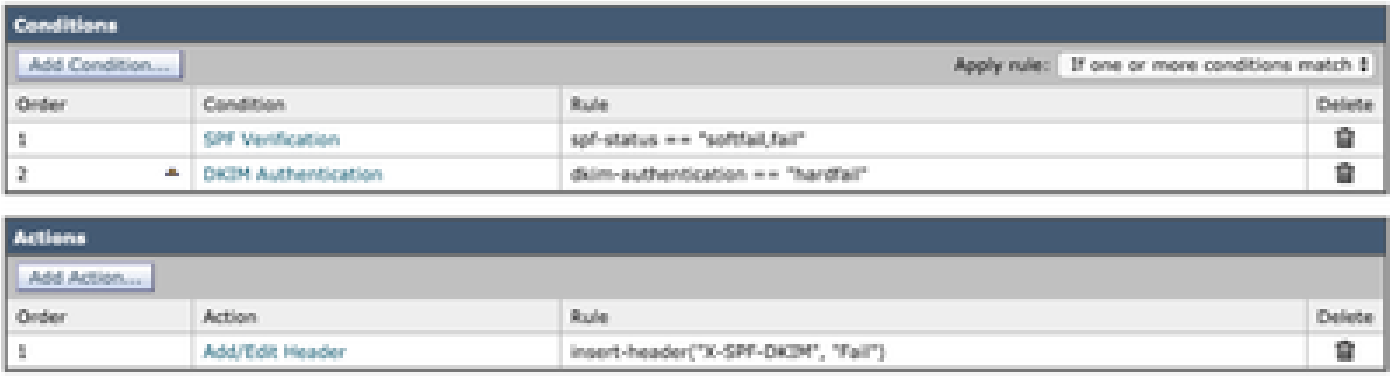


Layer 5: Riduzione dei falsi positivi con i risultati della verifica SPF o DKIM

È fondamentale applicare la verifica SPF o DKIM (entrambe o una delle due) per creare più livelli di rilevamento e-mail contraffatte per la maggior parte dei tipi di attacchi. Anziché adottare un'azione finale (come il rilascio o la quarantena), Cisco consiglia di aggiungere una nuova intestazione come [X-SPF-DKIM] sul messaggio che non supera la verifica SPF o DKIM e di collaborare con la funzione Forged Email Detection (FED), che viene trattata più avanti, in favore di una maggiore percentuale di messaggi di spoofing.

Procedura consigliata: creare un filtro contenuti che ispeziona i risultati della verifica SPF o DKIM di ogni messaggio in arrivo passato durante le ispezioni precedenti. Aggiungere una nuova X-header (ad esempio X-SPF-DKIM=Fail) sul messaggio che non supera la verifica SPF o DKIM e che passa al livello successivo di scansione - Forged Email Detection (FED).

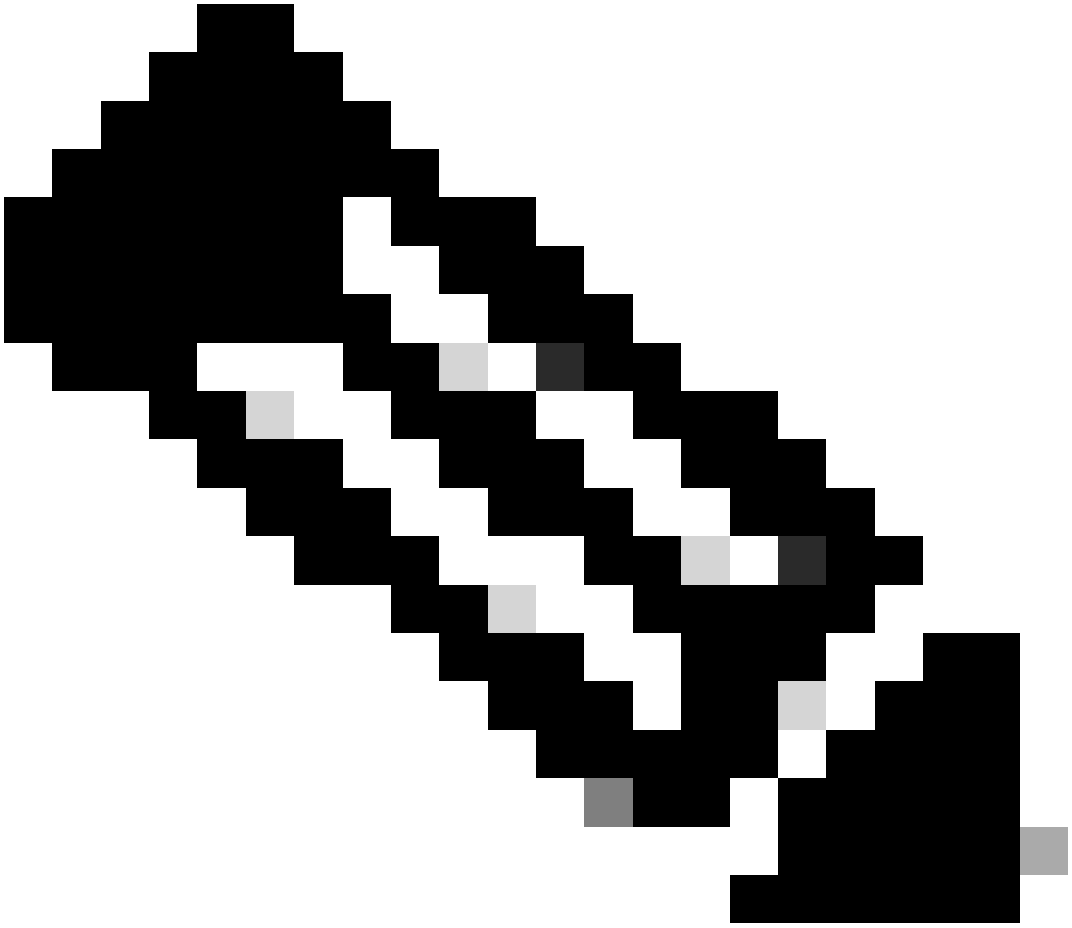
Immagine 7. Filtro contenuti che controlla i messaggi con risultati SPF o DKIM non riusciti



Livello 6: rilevamento messaggi con nome mittente probabilmente falsificato

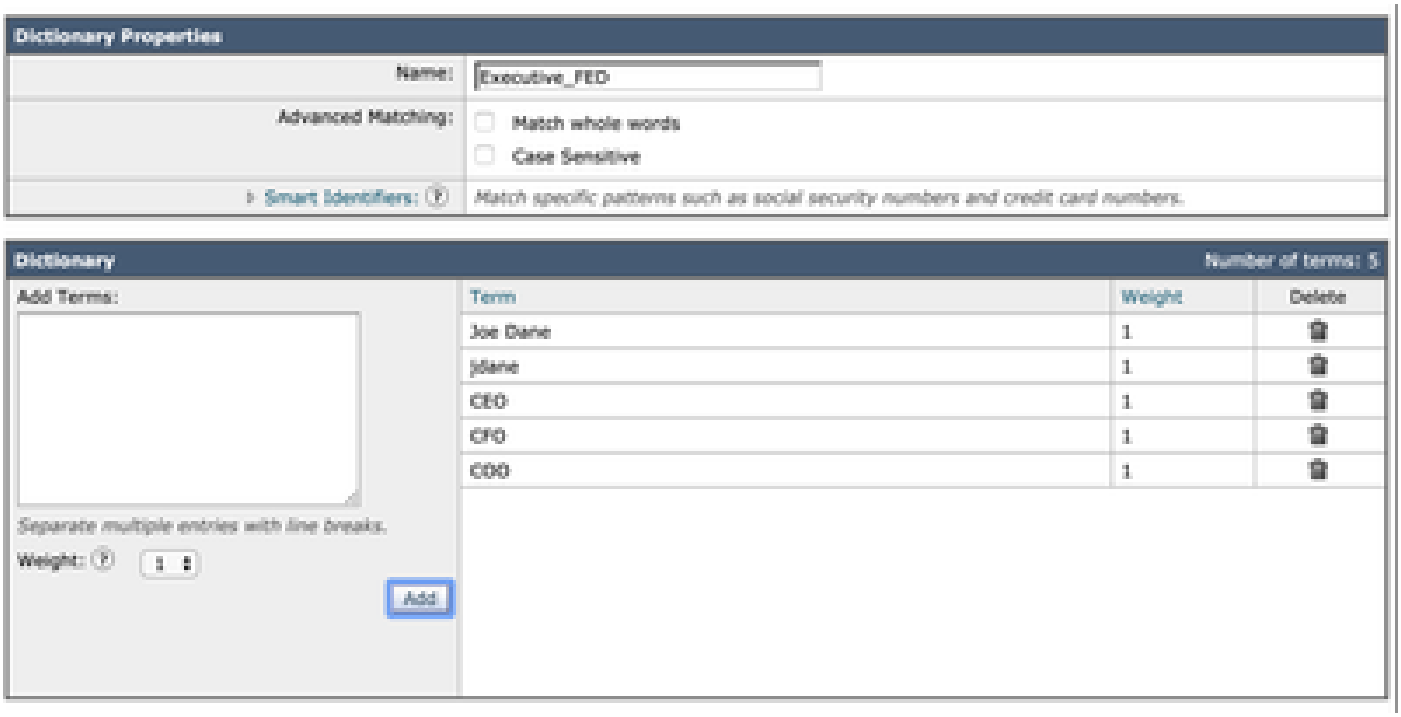
A complemento delle verifiche SPF, DKIM e DMARC, Forged Email Detection (FED) è un'altra linea di difesa cruciale contro lo spoofing della posta elettronica. La FED è ideale per porre rimedio agli attacchi spoof che abusano del valore From nel corpo del messaggio. Poiché si conoscono già i nomi dei dirigenti all'interno dell'organizzazione, è possibile creare un dizionario di tali nomi e quindi fare riferimento a tale dizionario con la condizione FED nei filtri dei contenuti. Inoltre, oltre ai nomi esecutivi, è possibile creare un dizionario di domini cugini o simili basato sul proprio dominio utilizzando DNSTWIST (DNSTWIT) per confrontarsi con lo spoofing dei domini simili.

Procedura ottimale: Identificare gli utenti dell'organizzazione i cui messaggi possono essere falsificati. Creare un dizionario personalizzato per i dirigenti. Per ogni nome esecutivo, il dizionario deve includere il nome utente e tutti i possibili nomi utente come termini (Immagine 8). Quando il dizionario è completo, usare Forged Email Detection nel filtro contenuti per far corrispondere il valore From dei messaggi in arrivo con queste voci del dizionario.



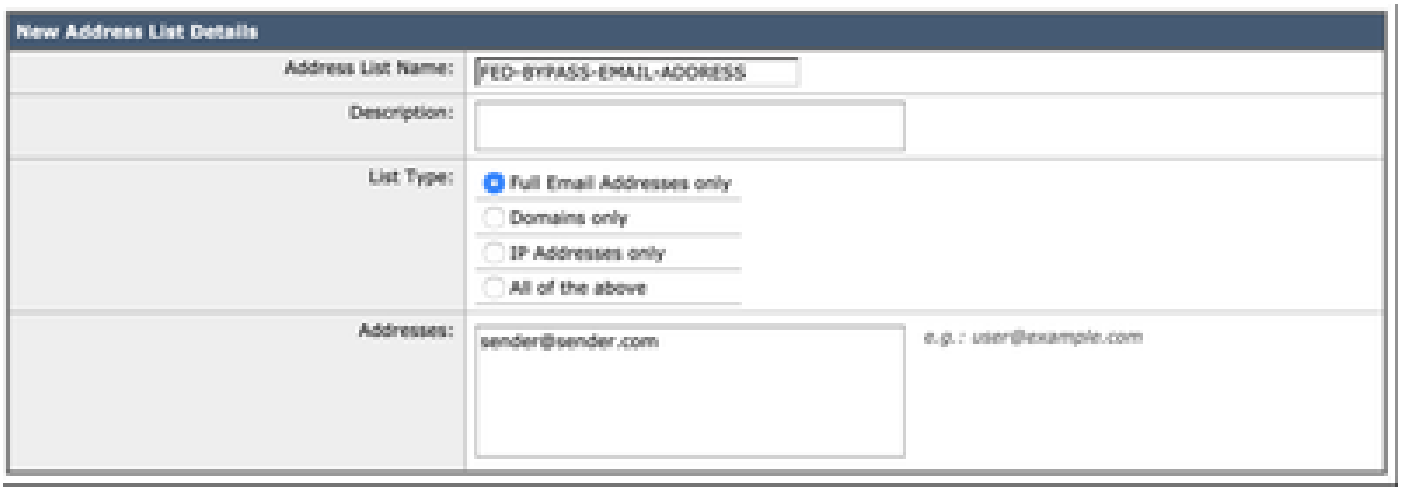
Nota: poiché la maggior parte dei domini non sono permutazioni registrate, la verifica del mittente DNS li protegge. Se si sceglie di utilizzare le voci del dizionario, prestare attenzione solo ai domini registrati e assicurarsi di non superare le 500-600 voci per dizionario.

Immagine 8. Directory personalizzata per rilevamento messaggi e-mail contraffatti



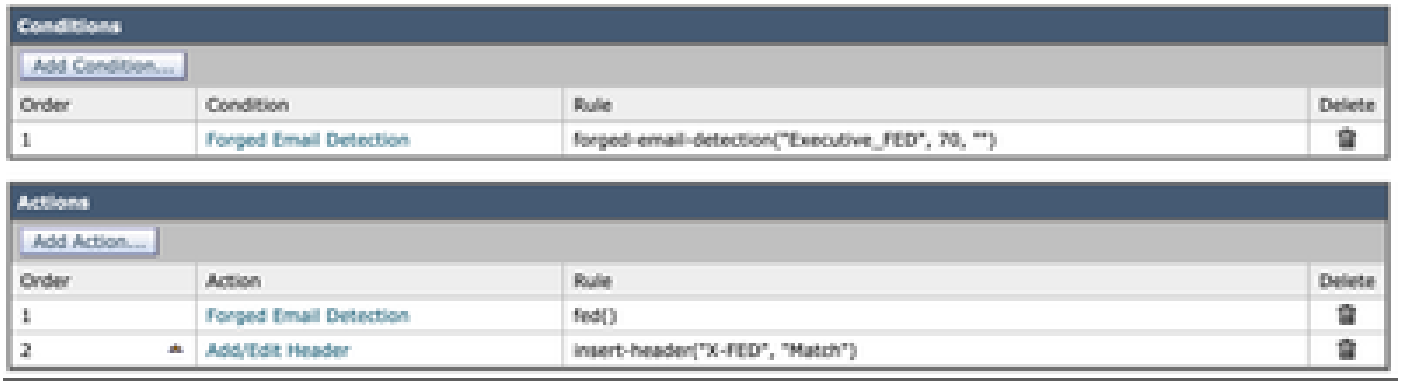
È facoltativo aggiungere una condizione di eccezione per il dominio e-mail nella busta Invia per ignorare l'ispezione FED. In alternativa, è possibile creare un elenco indirizzi personalizzato per ignorare l'ispezione FED e visualizzare un elenco di indirizzi e-mail nell'intestazione del modulo (immagine 9).

Immagine 9. Creazione di un elenco indirizzi per ignorare l'ispezione FED



Applicare l'azione proprietaria Forged Email Detection per rimuovere il valore From ed esaminare l'indirizzo e-mail del mittente effettivo della busta nella Posta in arrivo del messaggio. Quindi, invece di applicare un'azione finale, aggiungere una nuova intestazione X (ad esempio, X-FED=Match) sul messaggio che soddisfa la condizione e continuare a consegnare il messaggio al livello successivo di ispezione (Immagine 10).

Immagine 10. Impostazione filtro contenuto consigliata per FED

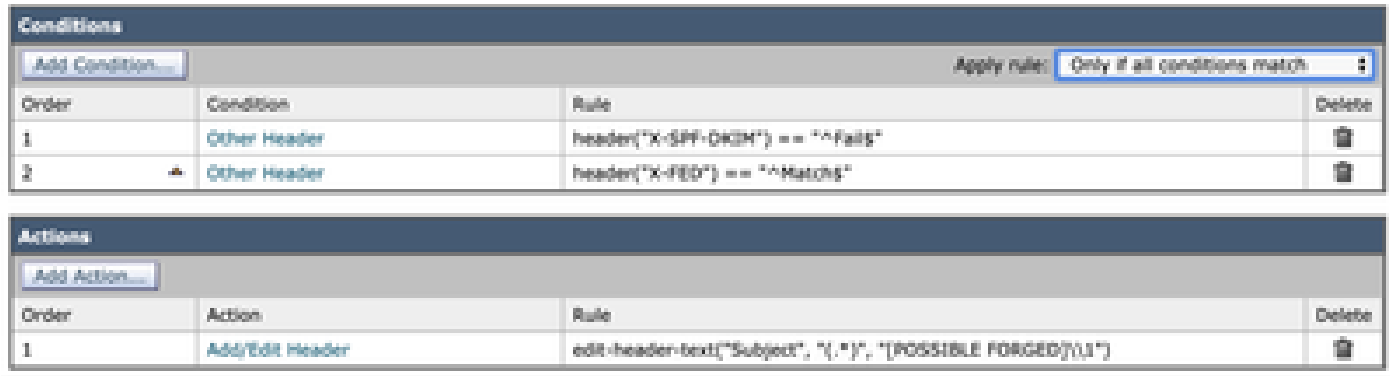


Layer 7: messaggio di posta elettronica con spoofing identificato positivamente

Identificare una vera e propria campagna di spoofing è più efficace facendo riferimento ad altri verdetti emessi da varie funzionalità di sicurezza in fase di elaborazione, come le informazioni di X-header prodotte da SPF/ DKIM Enforcemen e FE. Ad esempio, gli amministratori possono creare un filtro contenuti per identificare i messaggi aggiunti con entrambe le nuove intestazioni X a causa di errori nei risultati della verifica SPF/DKIM (X-SPF-DKIM=Fail) e quali voci dell'intestazione From corrispondono alle voci del dizionario FED (X-FED=Match).

L'azione consigliata può essere quella di mettere in quarantena il messaggio e di avvisare il destinatario oppure di continuare a recapitare il messaggio originale ma anteporre [POSSIBILI FALSIFICAZIONI] alla riga Oggetto come avviso al destinatario, come illustrato (Immagine 11).

Immagine 11. Combina tutte le intestazioni X in una singola regola (finale)



Layer 8: protezione dagli URL di phishing

Il filtro URL ed epidemie presente nel Cisco Secure Email offre una protezione contro i link di phishing. Le minacce miste combinano messaggi di spoofing e phishing per apparire più legittimi per l'obiettivo. Abilitare il filtro epidemie è fondamentale per aiutare a rilevare, analizzare e arrestare tali minacce in tempo reale. È importante sapere che la reputazione dell'URL viene valutata all'interno del motore antispam e che può essere usata come parte della decisione per il rilevamento della posta indesiderata. Se il motore della protezione dalla posta indesiderata non interrompe il messaggio con l'URL impostato come posta indesiderata, il messaggio viene valutato dal filtro URL ed epidemie nell'ultima parte della pipeline di sicurezza.

Consiglio: creare una regola di filtro dei contenuti che blocchi un URL con un punteggio di

reputazione dannoso e reindirizzi l'URL con un punteggio di reputazione neutro al proxy di sicurezza Cisco (immagine 12). Abilitare i filtri epidemie di minaccia abilitando la modifica dei messaggi. La riscrittura degli URL consente di analizzare gli URL sospetti tramite Cisco Security Proxy (immagine 13). Per ulteriori informazioni, visitare: [Configure URL Filtering for Secure Email Gateway and Cloud Gateway]

Immagine 12. Filtro contenuti per la reputazione degli URL

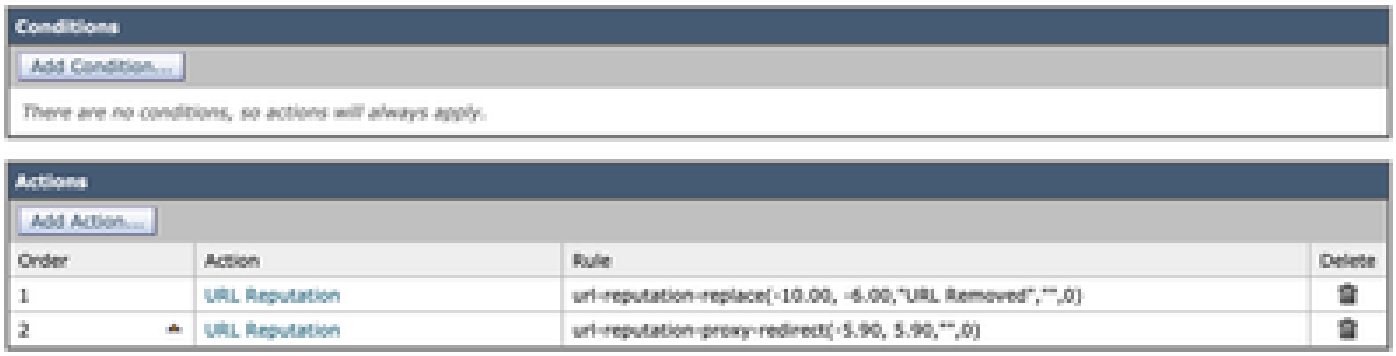
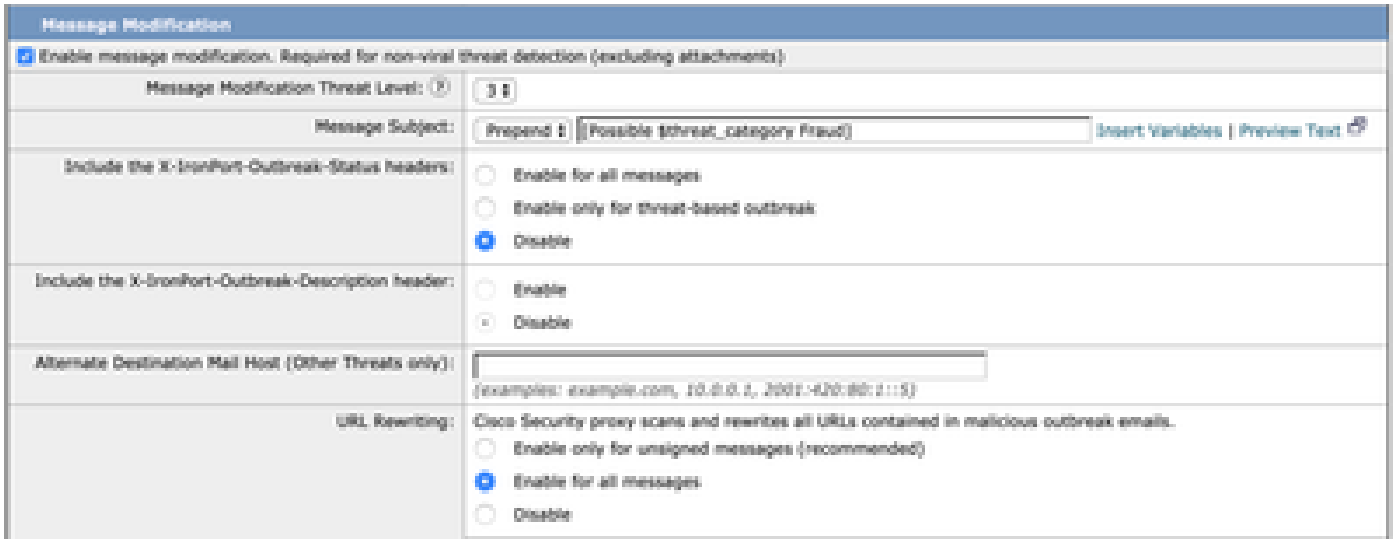


Immagine 13. Abilitazione della riscrittura degli URL nel filtro epidemie



Layer 9: funzionalità di rilevamento spoofing degli aumenti con Cisco Secure Email Threat Defense (ETD)

Cisco offre Email Threat Defense, una soluzione nativa del cloud che sfrutta le funzionalità avanzate di Cisco Talos per la gestione delle minacce. Dispone di un'architettura API per tempi di risposta più rapidi, visibilità completa dell'e-mail, messaggi interni inclusi, visualizzazione delle conversazioni per informazioni contestuali migliori e strumenti per il ripristino automatico o manuale delle minacce che si celano nelle caselle di posta Microsoft 365. Per ulteriori informazioni, vedere il [foglio dati Cisco Secure Email Threat Defense].

Cisco Secure Email Threat Defense combatte il phishing utilizzando l'autenticazione del mittente e le funzionalità di rilevamento BEC. Integra motori di apprendimento automatico e di intelligenza artificiale che combinano la modellazione di identità e relazioni locali con l'analisi del comportamento in tempo reale per proteggere contro minacce basate sull'inganno di identità.

Modella il comportamento affidabile dell'e-mail all'interno delle organizzazioni e tra i singoli utenti. Tra le altre caratteristiche principali, Email Threat Defense offre i seguenti vantaggi:

- Scoprite le minacce conosciute, emergenti e mirate con funzionalità avanzate di rilevamento delle minacce.
- Identificare le tecniche dannose e ottenere il contesto per i rischi aziendali specifici.
- Ricerca rapida di minacce pericolose e relativa risoluzione in tempo reale.
- Utilizzare la telemetria delle minacce per classificare le minacce e capire quali parti dell'organizzazione sono più vulnerabili agli attacchi.

Figura 14. Cisco Secure Email Threat Defense fornisce informazioni su come viene indirizzata l'organizzazione.

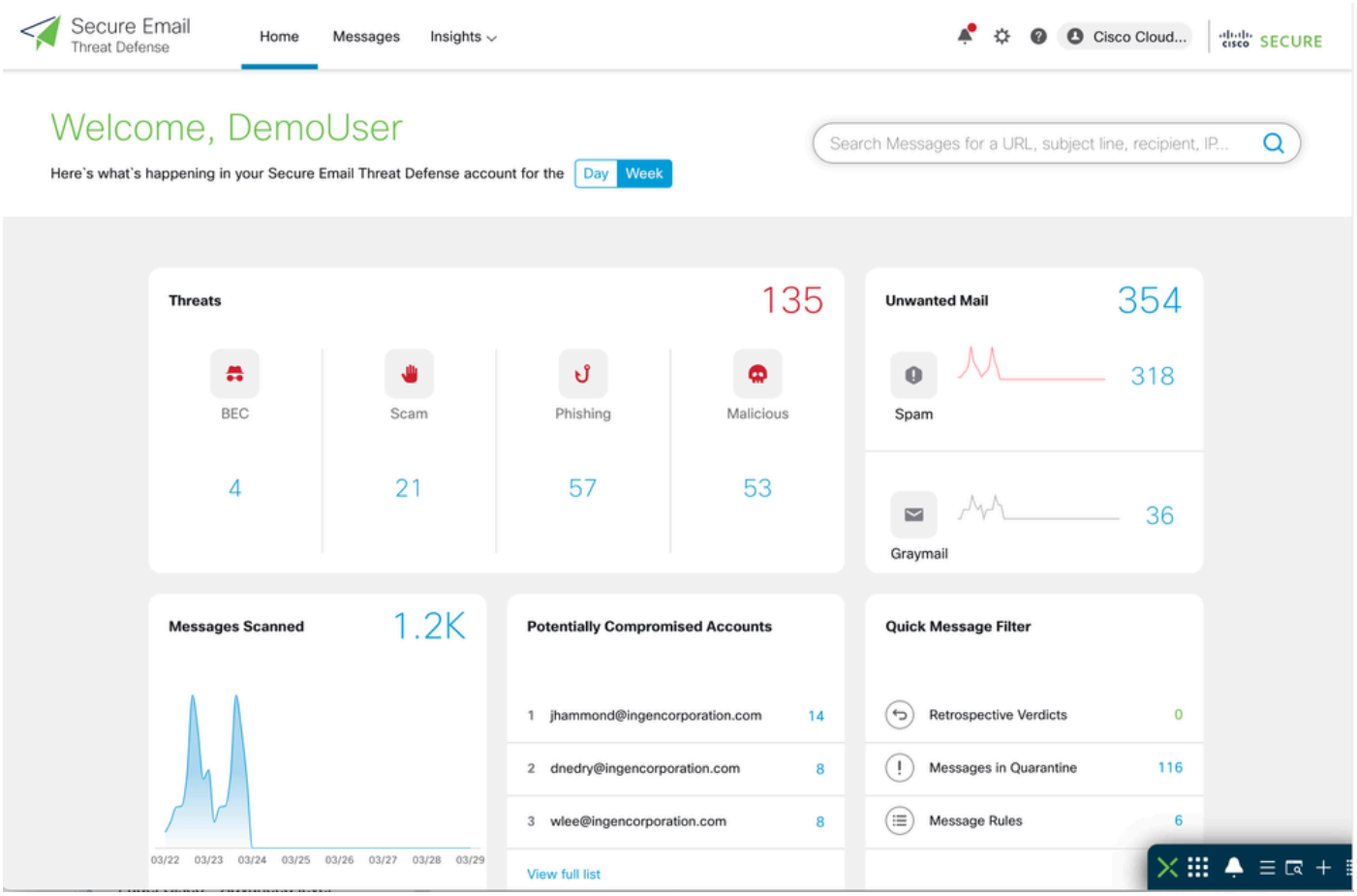
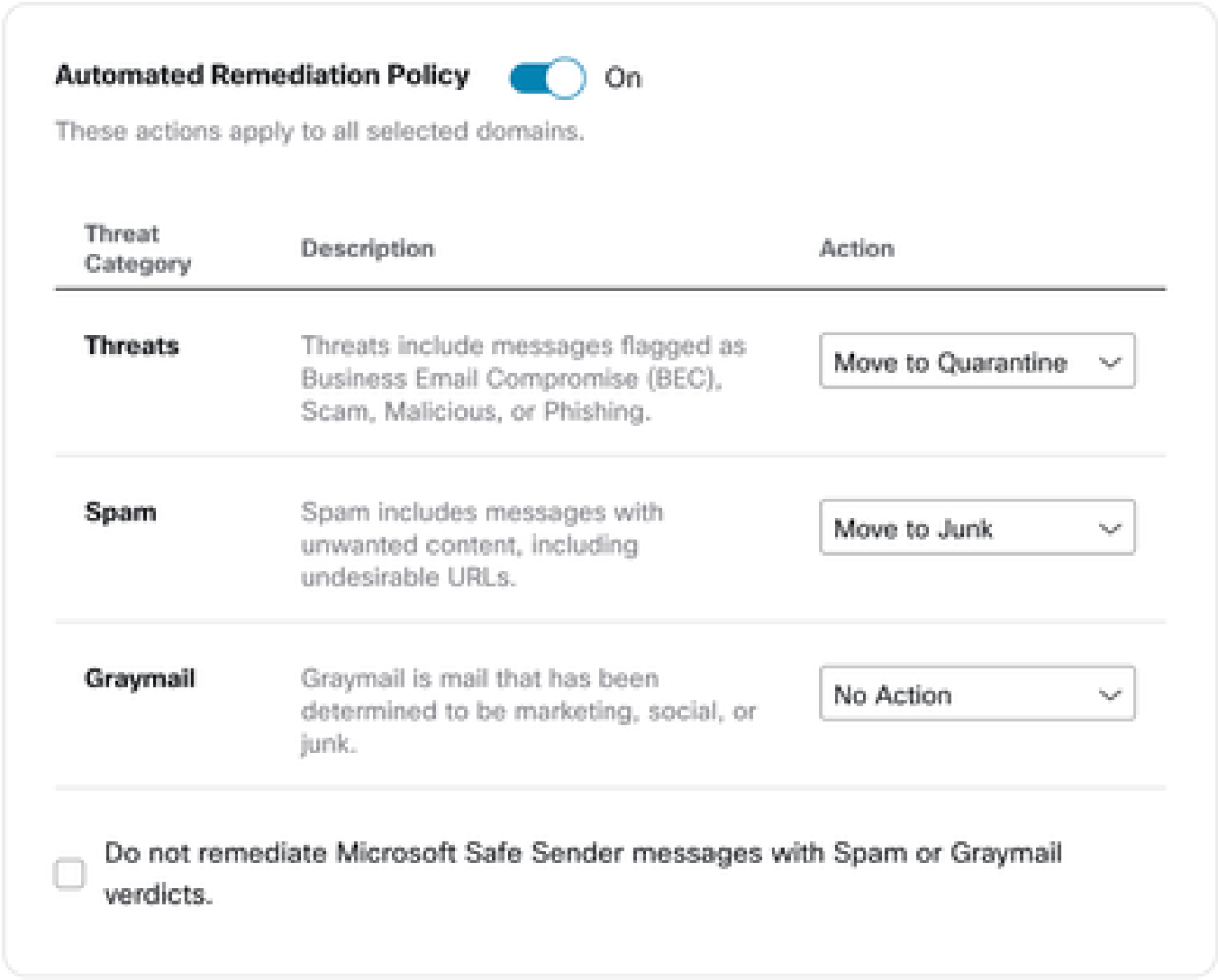


Immagine 15. L'impostazione dei criteri di Cisco Email Threat Defense determina automaticamente se il messaggio corrisponde alla categoria di minaccia selezionata



Ulteriori operazioni possibili con la prevenzione delle falsificazioni

Molte spoofs possono essere risolte con alcune semplici precauzioni che includono, ma non si limitano a queste:

- Limitare i domini elencati nella tabella Host Access Table (HAT) a un numero limitato di partner aziendali principali.
- Tenere traccia e aggiornare continuamente i membri nel gruppo mittente SPOOF_ALLOW se ne è stato creato uno e utilizzare le istruzioni fornite nel collegamento delle procedure consigliate.
- Abilitare il rilevamento della posta indesiderata e metterli anche in quarantena.

Ma, cosa più importante di tutte, abilitare SPF, DKIM e DMARC e implementarli in modo appropriato. Tuttavia, le linee guida sulla pubblicazione dei record SPF, DKIM e DMARC esulano dall'ambito di questo documento. A tale scopo, fare riferimento al seguente white paper: Email Authentication Best Practices: The Optimal Ways To Deploy SPF, DKIM, and DMARC (Procedure ottimali per l'autenticazione e-mail: i modi ottimali per distribuire SPF, DKIM e DMARC).

Comprendere la sfida di porre rimedio agli attacchi tramite e-mail come le campagne di spoofing

discusse qui. Per domande sull'implementazione di queste best practice, contattare il supporto tecnico Cisco e aprire una richiesta. In alternativa, contattare l'Account Team Cisco per una soluzione e una guida alla progettazione. Per ulteriori informazioni su Cisco Secure Email, visitare il sito Web Cisco Secure Email.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).