Configurare Secure Email Gateway per l'utilizzo di Microsoft Quarantine Notification e Quarantine di Microsoft

Sommario

Introduzione

In questo documento viene descritta la procedura di configurazione necessaria per integrare Cisco Secure Email (CES) con la quarantena Microsoft 365.

Panoramica

Nelle moderne infrastrutture di posta elettronica vengono spesso implementati più livelli di sicurezza, con il risultato che i messaggi di posta elettronica vengono messi in quarantena da diversi sistemi. Per semplificare l'esperienza degli utenti e migliorare la coerenza delle notifiche, è utile centralizzare la gestione della quarantena in un'unica piattaforma. Questa guida spiega come reindirizzare i messaggi indesiderati, come spam e posta grigia, identificati da Cisco CES nella quarantena per gli utenti di Microsoft 365.

Prerequisiti

Per completare la configurazione, verificare di avere a disposizione quanto segue:

1. Un tenant attivo in Cisco Secure Email Gateway
2. Un tenant attivo in Microsoft Exchange online.
3. Accesso ai servizi Microsoft 365 (O365)
4. Una licenza di Microsoft 365 Defender (necessaria per configurare i criteri e le notifiche di quarantena)

Configurazione di Microsoft 365 (O365)

Configurare innanzitutto Microsoft 365 per la ricezione e la gestione dei messaggi in quarantena.

Abilita notifiche di quarantena in Microsoft Exchange online

È possibile fare riferimento alla documentazione ufficiale di Microsoft per configurare le notifiche utente per i messaggi in quarantena:
Configurazione notifica quarantena Microsoft

Regola Crea un flusso di posta

Una volta attivate le notifiche, configurare una regola che reindirizzi i messaggi contrassegnati da Cisco Secure Email Gateway alla quarantena ospitata da Microsoft.

1. Aprire l'interfaccia di amministrazione di Microsoft Exchange.
2. Dal menu a sinistra, andare a Flusso di posta → Regole.
3. Fare clic su Aggiungi regola e quindi selezionare Crea nuova regola.
4. Impostare il nome della regola su: Regola di quarantena CSE.
5. In Applica questa regola se, selezionare L'intestazione del messaggio, quindi scegliere corrispondenze pattern di testo.
6. Nel nome dell'intestazione, immettere: X-CSE-Quarantine e impostare il valore in modo che corrisponda a: vero.
7. In Eseguire le operazioni seguenti, scegliere Reindirizza il messaggio a e selezionare Quarantena ospitata.
8. Salvare la configurazione.
9. Dopo il salvataggio, verificare che la regola sia abilitata.

Nell'immagine potete vedere come appare la regola.

CSE Quarantine

Edit rule conditions Edit rule settings

Status: Disabled

Enable or disable rule

Enabled

Updating the rule status, please wait...

Rule settings

Rule name
CSE Quarantine

Mode
Enforce

Severity
Not specified

Set date range
Specific date range is not set

Senders address
Matching Header

Priority
1

For rule processing errors
Ignore

Rule description

Apply this rule if

'X-CSE-Quarantine' header matches the following patterns: 'true'

Do the following

Deliver the message to the hosted quarantine.

Rule comments

Regola Microsoft

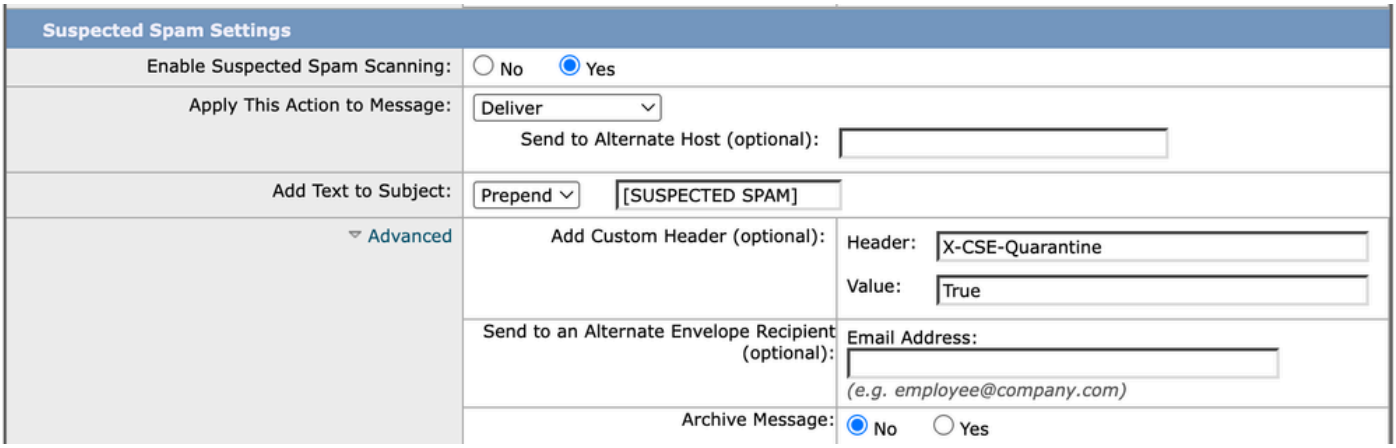
Configurazione di Cisco Secure Email

In Cisco CES, è possibile aggiungere un'intestazione personalizzata (X-CSE-Quarantine: true) a qualsiasi messaggio che si desidera reindirizzare alla quarantena di Microsoft.

Questi messaggi possono essere contrassegnati da qualsiasi filtro o motore di contenuti in CES. Nell'esempio, viene configurata per i messaggi con posta indesiderata.

1. Aprire Cisco Secure Email Management Console.
2. Andare a Mail Policies → Incoming Mail Policies.
3. Modificare i criteri desiderati (ad esempio, selezionare il criterio predefinito).
4. Fare clic sulle impostazioni della posta indesiderata per il criterio selezionato.
5. In Sospetto posta indesiderata modificare l'azione da Quarantena a Consegna.
6. Fare clic su Advanced (Avanzate) e aggiungere un'intestazione custom:
    - Nome intestazione: X-CSE-Quarantine
    - Valore: true (stesso valore utilizzato nella regola di Microsoft)
7. Fare clic su Submit, quindi su Commit delle modifiche per applicare la configurazione.

Nell'immagine è possibile vedere l'aspetto della configurazione.

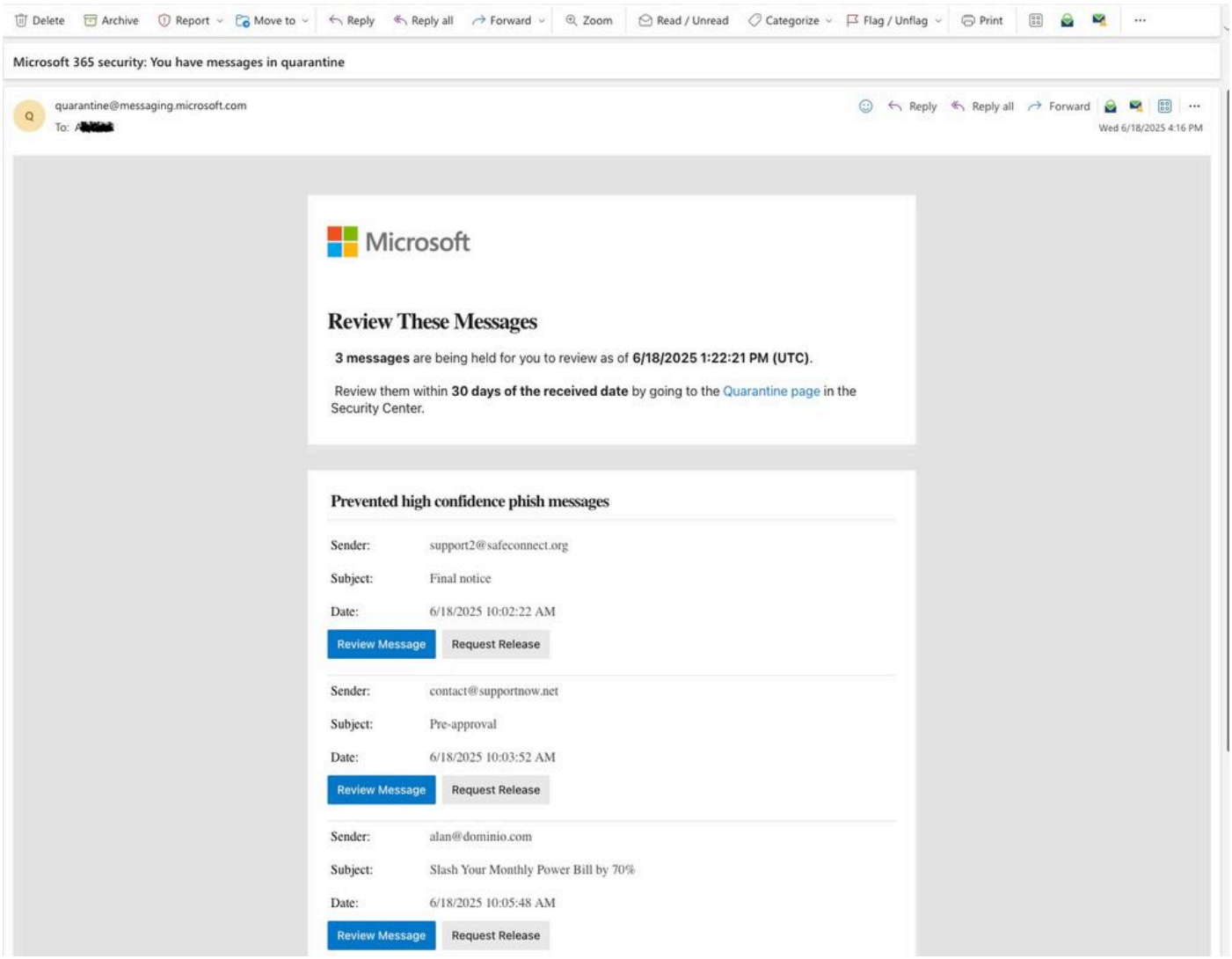


Configurazione CES

Verifica

Da questo momento in poi, le e-mail identificate da Cisco CES come potenziali spam verranno contrassegnate con l'intestazione personalizzata. Microsoft 365 rileva questo tag e reindirizza il messaggio alla quarantena utente.

Gli utenti che stanno per ricevere notifiche di quarantena in base alla configurazione di Microsoft 365.



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).