Configuración de Secure Email Gateway para utilizar la cuarentena de Microsoft y la notificación de cuarentena de Microsoft

Contenido

Introducción

Overview

Prerequisites

Configuración de Microsoft 365 (O365)

- Habilitar notificaciones de cuarentena en Microsoft Exchange en línea
- Crear una regla de flujo de correo

Configuración de Cisco Secure Email

Verificación

Introducción

Este documento describe los pasos de configuración requeridos para integrar Cisco Secure Email (CES) con Microsoft 365 Quarantine.

Overview

En las infraestructuras de correo electrónico modernas, a menudo se implementan varias capas de seguridad, lo que hace que los distintos sistemas pongan en cuarentena los mensajes de correo electrónico. Para optimizar la experiencia del usuario y mejorar la coherencia de las notificaciones, resulta beneficioso centralizar la administración de la cuarentena en una única plataforma. Esta guía explica cómo redirigir los mensajes no deseados (como spam y graymail) identificados por Cisco CES a la cuarentena de usuario de Microsoft 365.

Prerequisites

Para completar esta configuración, asegúrese de que dispone de lo siguiente:

1. Un arrendatario activo en Cisco Secure Email Gateway
2. Arrendatario activo de Microsoft Exchange en línea.
3. Acceso a los servicios de Microsoft 365 (O365)
4. Una licencia de Microsoft 365 Defender (necesaria para configurar políticas y notificaciones de cuarentena)

Configuración de Microsoft 365 (O365)

Comience configurando Microsoft 365 para recibir y administrar mensajes en cuarentena.

Habilitar notificaciones de cuarentena en Microsoft Exchange en línea

Puede consultar la documentación oficial de Microsoft para configurar las notificaciones de usuario para los mensajes en cuarentena:
Configuración de Notificación de cuarentena de Microsoft

Crear una regla de flujo de correo

Una vez que las notificaciones estén activas, configure una regla que redirija los mensajes marcados por Cisco Secure Email Gateway a la cuarentena alojada de Microsoft.

1. Abra el Centro de administración de Microsoft Exchange.
2. En el menú de la izquierda, vaya a Reglas de flujo de correo →.
3. Haga clic en Agregar una regla y, a continuación, seleccione Crear una nueva regla.
4. Establezca el nombre de la regla en: Regla de cuarentena de CSE.
5. En Aplicar esta regla si, seleccione El encabezado del mensaje y, a continuación, elija Coincide con los patrones de texto.
6. En el nombre del encabezado, ingrese: X-CSE-Quarantine, y establezca el valor para que coincida: verdadero.
7. En Haga lo siguiente, elija Redirigir el mensaje a y seleccione Cuarentena alojada.
8. Guarde la configuración.
9. Después de guardar, asegúrese de que la regla está habilitada.

En la imagen puede ver el aspecto de la regla.

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

Regla de Microsoft

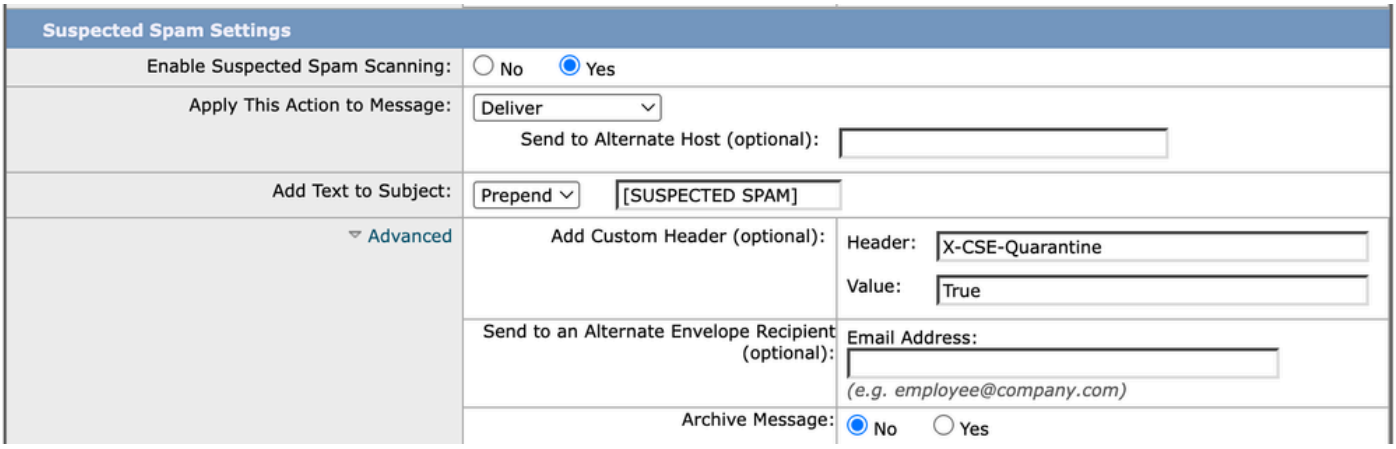
Configuración de Cisco Secure Email

En Cisco CES, puede agregar un encabezado personalizado (X-CSE-Quarantine: true) a cualquier mensaje que deseemos redirigir a la cuarentena de Microsoft.

Estos mensajes se pueden marcar con cualquier filtro de contenido o motor en CES. En este ejemplo, lo configuramos para los mensajes de Spam Sospechoso.

1. Abra Cisco Secure Email Management Console.
2. Vaya a Políticas de correo → Políticas de correo entrante.
3. Edite las directivas que desee modificar (por ejemplo, seleccione la directiva predeterminada).
4. Haga clic en la configuración de spam para la política seleccionada.
5. En Spam sospechoso, cambie la acción de Cuarentena a Entregar.
6. Haga clic en Advanced y agregue un encabezado personalizado:
    - Nombre del encabezado: X-CSE-Quarantine
    - Valor: true (mismo valor utilizado en la regla de Microsoft)
7. Haga clic en Submit y luego en Commit Changes para aplicar la configuración.

En la imagen puede ver el aspecto de la configuración.

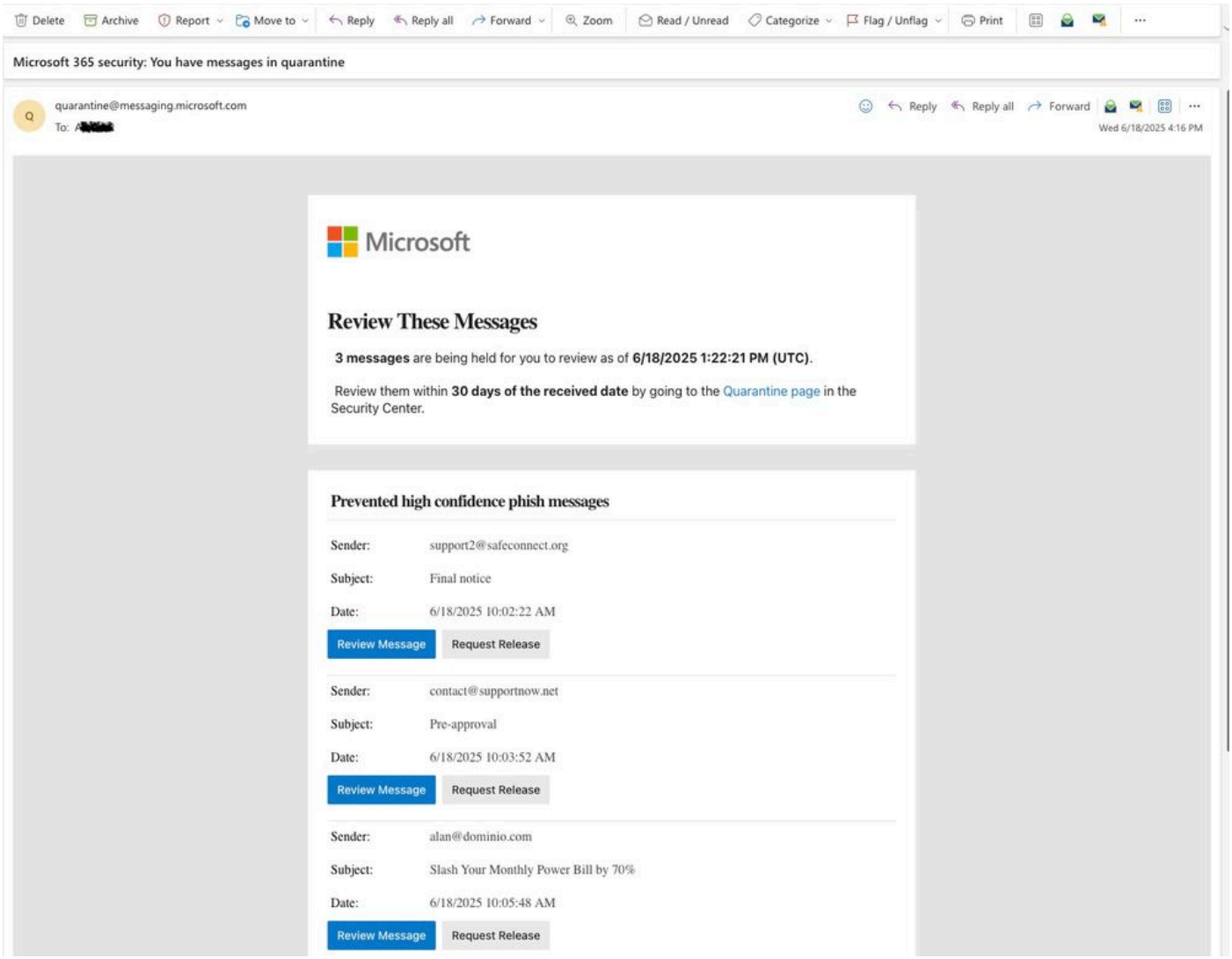


configuración de CES

Verificación

A partir de este momento, los correos electrónicos identificados por Cisco CES como spam potencial se etiquetarán con el encabezado personalizado. Microsoft 365 detecta esta etiqueta y redirige el mensaje a la cuarentena de usuario.

Los usuarios que vayan a recibir notificaciones de cuarentena según la configuración de Microsoft 365.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).