Configurar o Secure Email Gateway para usar a Quarentena da Microsoft e a Notificação de Quarentena da Microsoft

Contents

Introdução

Este documento descreve as etapas de configuração necessárias para integrar o Cisco Secure Email (CES) à quarentena do Microsoft 365.

Overview

Em infraestruturas de e-mail modernas, várias camadas de segurança são frequentemente implementadas, resultando em e-mails em quarentena por diferentes sistemas. Para simplificar a experiência do usuário e melhorar a consistência da notificação, é vantajoso centralizar o gerenciamento de quarentena em uma única plataforma. Este guia explica como redirecionar mensagens indesejadas, como spam e mensagens em cinza, identificadas pelo Cisco CES na quarentena de usuário do Microsoft 365.

Pré-requisitos

Para concluir essa configuração, verifique se você tem o seguinte:

1. Um locatário ativo no Cisco Secure Email Gateway
2. Um locatário ativo no Microsoft Exchange online.
3. Acesso aos serviços do Microsoft 365 (O365).
4. Uma licença do Microsoft 365 Defender (necessária para configurar políticas e notificações de quarentena)

Configurar o Microsoft 365 (O365)

Comece configurando o Microsoft 365 para receber e gerenciar mensagens em quarentena.

Habilitar notificações de quarentena no Microsoft Exchange online

Você pode consultar a documentação oficial da Microsoft para configurar notificações de usuário para mensagens em quarentena:
Configuração de Notificação de Quarentena da Microsoft

Criar uma regra de fluxo de e-mails

Quando as notificações estiverem ativas, configure uma regra que redirecione as mensagens marcadas pelo Cisco Secure Email Gateway para a quarentena hospedada da Microsoft.

1. Abra o Centro de Administração do Microsoft Exchange.
2. No menu à esquerda, vá para Regras de → de fluxo de e-mail.
3. Clique em Adicionar uma regra e selecione Criar uma nova regra.
4. Defina o nome da regra como: Regra de quarentena CSE.
5. Em Aplicar esta regra se, selecione O cabeçalho da mensagem e escolha corresponde aos padrões de texto.
6. No nome do cabeçalho, insira: X-CSE-Quarantine e defina o valor para corresponder: verdadeiro.
7. Em Faça o seguinte, escolha Redirecionar a mensagem para e selecione Quarentena hospedada.
8. Salve a configuração.
9. Após salvar, verifique se a regra está ativada.

Na figura, você pode ver como a regra se parece.

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

Regra da Microsoft

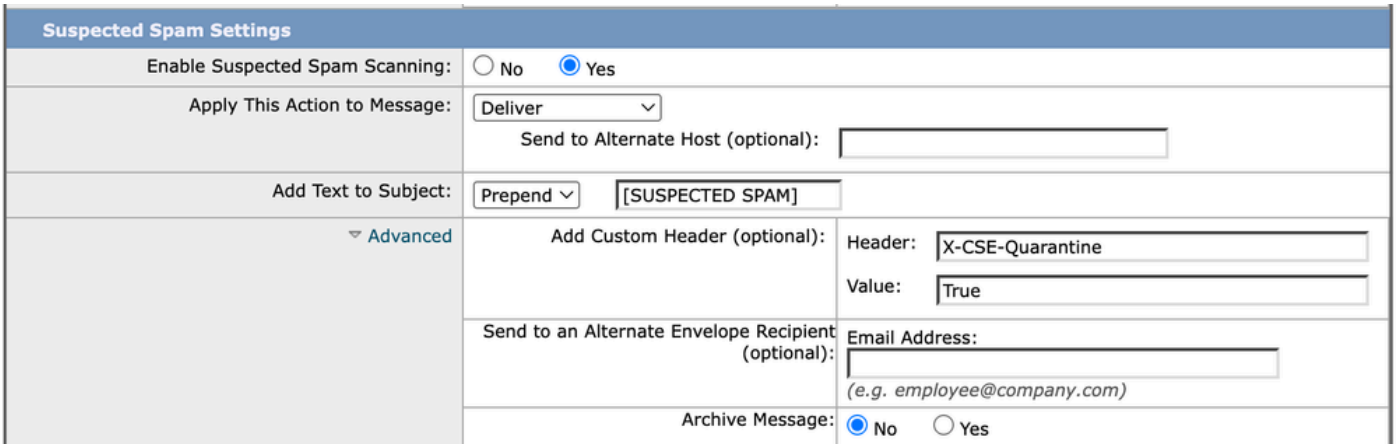
Configurar o Cisco Secure Email

No Cisco CES, você pode adicionar um cabeçalho personalizado (X-CSE-Quarantine: true) a qualquer mensagem que desejamos redirecionar para a quarentena da Microsoft.

Essas mensagens podem ser sinalizadas por qualquer filtro de conteúdo ou mecanismo no CES. Neste exemplo, ele é configurado para mensagens de spam suspeito.

1. Abra o Cisco Secure Email Management Console.
2. Vá para Políticas de e-mail → Políticas de recebimento de e-mail.
3. Edite as diretivas que deseja modificar (por exemplo, selecione a Diretiva Padrão).
4. Clique nas Configurações de spam da política selecionada.
5. Em Spam suspeito, altere a ação de Quarentena para Entregar.
6. Clique em Avançado e adicione um cabeçalho personalizado:
    - Nome do cabeçalho: X-CSE-Quarantine
    - Valor: verdadeiro (mesmo valor usado na regra da Microsoft)
7. Clique em Enviar e, em seguida, em Confirmar alterações para aplicar a configuração.

Na figura, você pode ver como é a configuração.

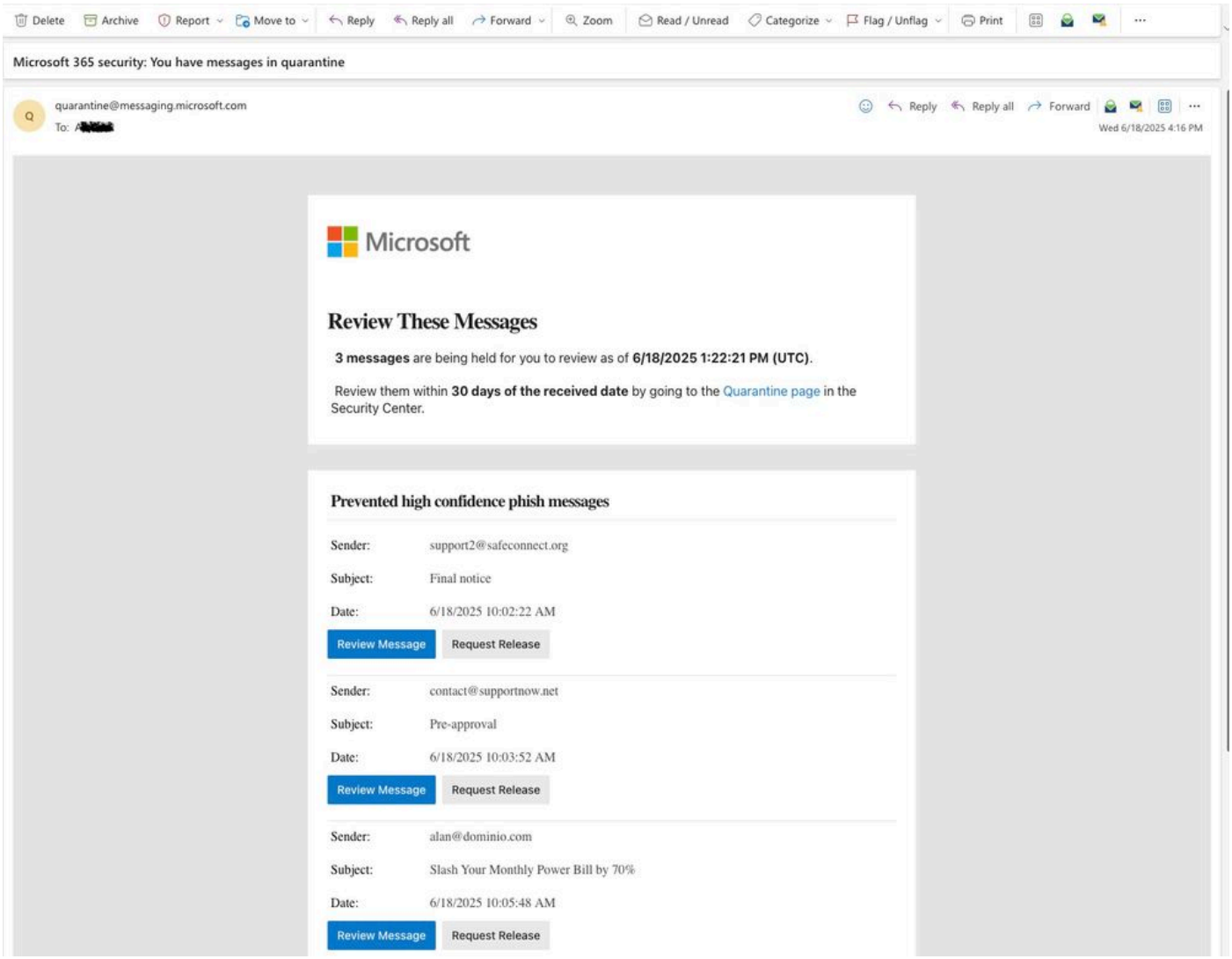


configuração de CES

Verificar

A partir desse ponto, os e-mails identificados pelo Cisco CES como spam em potencial serão marcados com o cabeçalho personalizado. O Microsoft 365 detecta essa marca e redireciona a mensagem para a quarentena do usuário.

Os usuários que receberão notificações de quarentena de acordo com a configuração do Microsoft 365.



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.