Beveiligde e-mailgateway configureren om Microsoft Quarantine en Microsoft Quarantine Notification te gebruiken

Inhoud

Inleiding

In dit document worden de configuratiestappen beschreven die nodig zijn om Cisco Secure Email (CES) te integreren met Microsoft 365-quarantaine.

Overzicht

In moderne e-mailinfrastructuren worden vaak meerdere beveiligingslagen geïmplementeerd, waardoor e-mails in quarantaine worden geplaatst door verschillende systemen. Om de gebruikerservaring te stroomlijnen en de consistentie van meldingen te verbeteren, is het nuttig om het quarantainebeheer in één platform te centraliseren. In deze handleiding wordt uitgelegd hoe u ongewenste berichten, zoals spam en graymail, die door Cisco CES zijn geïdentificeerd, kunt omleiden naar de Microsoft 365-gebruikersquarantaine.

Voorwaarden

Om deze configuratie te voltooien, moet u ervoor zorgen dat u het volgende hebt:

1. Een actieve tenant in Cisco Secure Email Gateway
2. Een actieve tenant in Microsoft Exchange online.
3. Toegang tot Microsoft 365 (O365) services
4. Een Microsoft 365 Defender-licentie (vereist om quarantainebeleid en -meldingen te configureren)

Microsoft 365 (O365) configureren

Begin met het instellen van Microsoft 365 om in quarantaine geplaatste berichten te ontvangen en te beheren.

Quarantainemeldingen inschakelen in Microsoft Exchange online

U kunt naar de officiële Microsoft-documentatie verwijzen om gebruikersmeldingen voor in quarantaine geplaatste berichten te configureren:
Microsoft Quarantine Notification-configuratie

Een e-mailstroomregel maken

Wanneer meldingen actief zijn, configureert u een regel die berichten die zijn gemarkeerd door Cisco Secure Email Gateway doorstuurt naar de gehoste quarantaine van Microsoft.

1. Open het Microsoft Exchange Admin Center.
2. Ga in het linkermenu naar Mail Flow → Regels.
3. Klik op Regel toevoegen en selecteer Een nieuwe regel maken.
4. Stel de naam van de regel in op: CSE Quarantaine Rule.
5. Selecteer onder Deze regel toepassen als, De berichtkoptekst selecteren, en kies overeenkomende tekstpatronen.
6. Voer in de naam van de koptekst: X-CSE-Quarantaine in en stel de waarde in op overeenkomend met: true.
7. Onder Doe het volgende, kies Omleiden van het bericht naar, en selecteer Gehoste quarantaine.
8. Sla de configuratie op.
9. Controleer na het opslaan of de regel is ingeschakeld.

Op de foto zie je hoe de regel eruit ziet.

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

Microsoft-regel

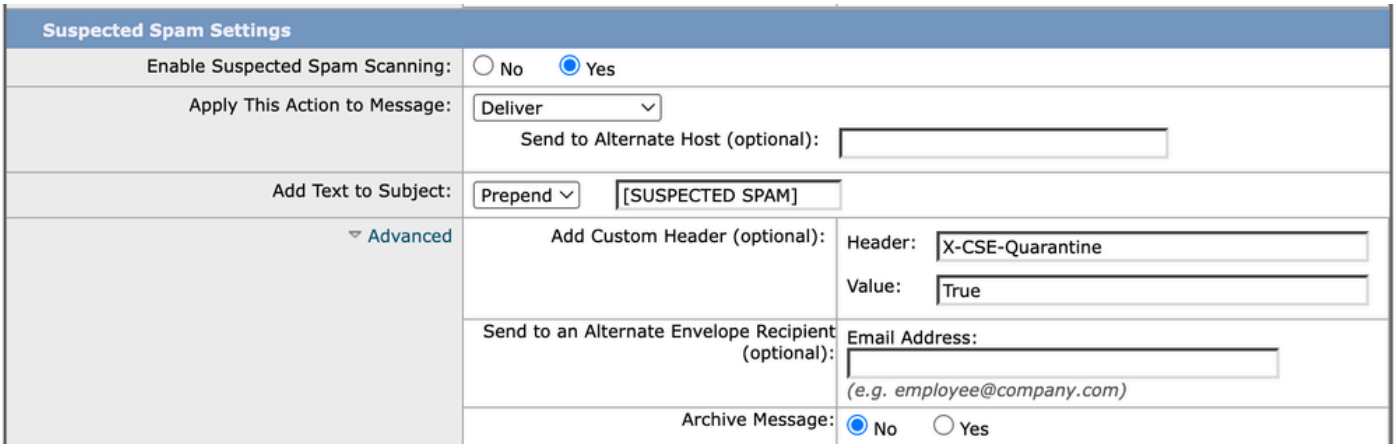
Cisco Secure Email configureren

In Cisco CES kunt u een aangepaste header (X-CSE-Quarantine: true) toevoegen aan elk bericht dat we naar Microsoft's quarantaine willen doorverwijzen.

Deze berichten kunnen worden gemarkeerd door elk inhoudsfilter of elke engine in CES. In dit voorbeeld configureren we het voor berichten met verdachte spam.

1. Open de Cisco Secure Email Management Console.
2. Ga naar E-mailbeleid → Beleid voor inkomende e-mail.
3. Bewerk het beleid dat u wilt wijzigen (selecteer bijvoorbeeld het standaardbeleid).
4. Klik op de spaminstellingen voor het geselecteerde beleid.
5. Onder Verdachte spam, wijzigt u de actie van Quarantaine naar Leveren.
6. Klik op Geavanceerd en voeg een aangepaste koptekst toe:
    - Naam koptekst: X-CSE-Quarantaine
    - Waarde: true (zelfde waarde als in de Microsoft-regel)
7. Klik op Indienen en Wijzigingen vastleggen om de configuratie toe te passen.

Op de foto zie je hoe de configuratie eruit ziet.

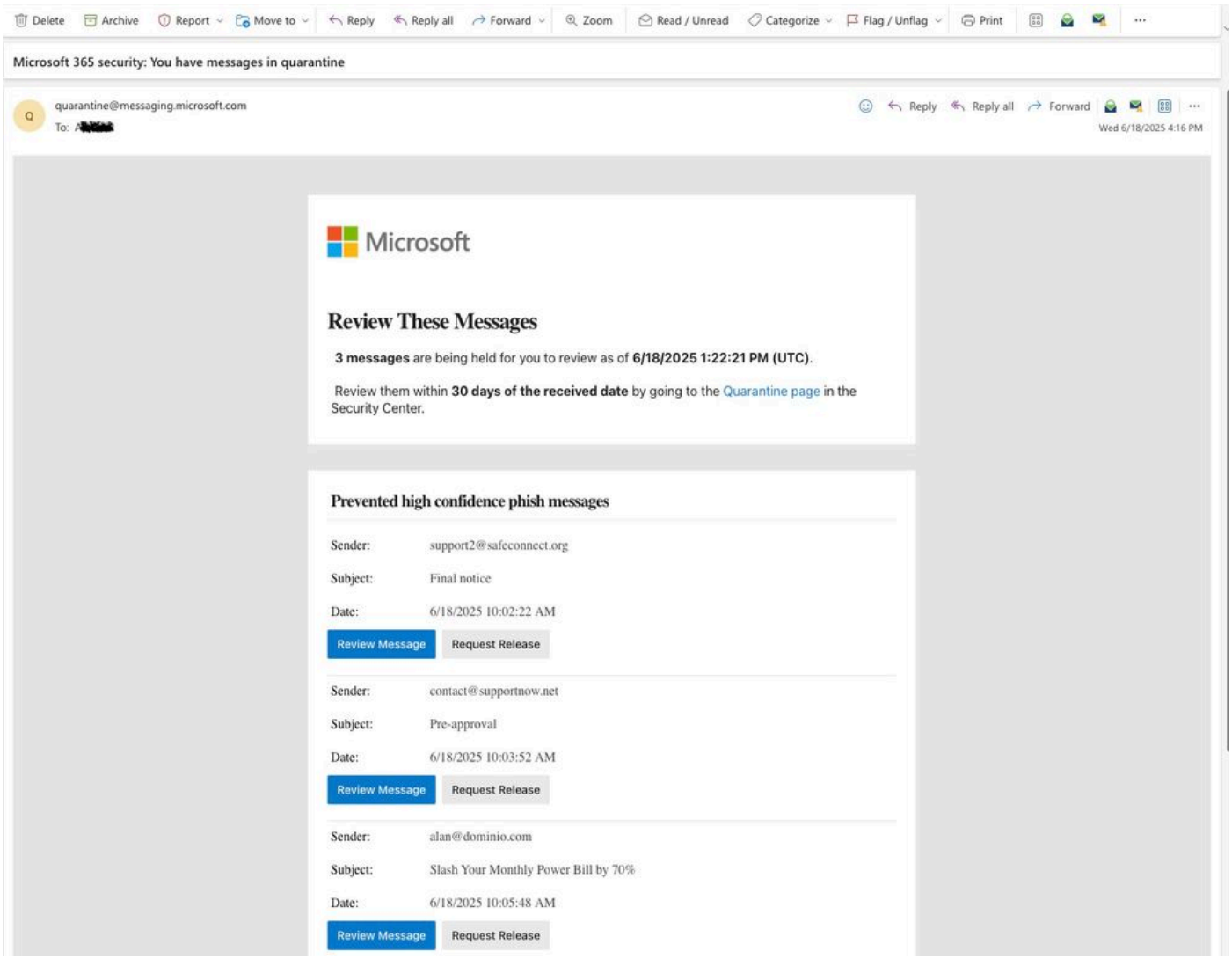


CES-configuratie

Verifiëren

Vanaf dit punt worden e-mails die door Cisco CES zijn geïdentificeerd als potentiële spam, gelabeld met de aangepaste header. Microsoft 365 detecteert deze tag en stuurt het bericht door naar de gebruikersquarantaine.

Gebruikers w0gaan quarantaine meldingen ontvangen volgens de Microsoft 365-configuratie.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.