Detección y prevención de la suplantación de correo electrónico

Contenido

Introducción

Este documento describe cómo detectar y prevenir la suplantación de correo electrónico cuando se utiliza Cisco Secure Email.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- Cisco Secure Email

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

Acerca de este documento

Este documento está dirigido a clientes de Cisco, partners de canal de Cisco e ingenieros de Cisco que implementan Cisco Secure Email. Este documento abarca:

- ¿Qué es la suplantación de correo electrónico?
- Flujo de trabajo de defensa de correo electrónico falso
- ¿Qué más se puede hacer con la prevención de la suplantación?

Qué es la suplantación de correo electrónico

La suplantación de correo electrónico es una falsificación del encabezado de correo electrónico en la que el mensaje parece haber tenido su origen en alguien o en algún lugar distinto del origen real. La suplantación de correo electrónico se utiliza en las campañas de phishing y spam porque es más probable que las personas abran un correo electrónico cuando creen que una fuente legítima y de confianza lo ha enviado. Para obtener más información sobre la suplantación, consulte Qué es la suplantación de correo electrónico y Cómo detectarla.

La suplantación de correo electrónico se clasifica en las siguientes categorías:

Categoría	Descripción	Objetivo principal
Suplantación de dominio directa	Suplantar un dominio similar en el remitente del sobre como dominio del destinatario.	Empleados
Decepción de nombre de visualización	El encabezado De muestra un remitente legítimo con el nombre ejecutivo de una organización. También se les conoce como Business Email Compromise (BEC).	Empleados
Suplantación de marca	El encabezado De muestra un remitente legítimo con el nombre comercial de una organización conocida.	Clientes/partners
Ataque basado en URL de phishing	Un correo electrónico con una URL que intenta robar datos confidenciales o iniciar sesión en la información de la víctima. Un correo electrónico falso de un banco que le pide que haga clic en un enlace y verifique los detalles de su cuenta es un ejemplo de un ataque basado en una URL de suplantación de identidad.	Empleados/partners
Primo o ataque de	El valor del encabezado De o De del sobre muestra una	Empleados/partners

dominio parecido	dirección de remitente similar que se hace pasar por una real para omitir las inspecciones de Marco de políticas de remitente (SPF), Correo identificado por DomainKeys (DKIM) y Autenticación de mensajes basada en dominio, informes y conformidad (DMARC).	
Adquisición de cuenta/Cuenta comprometida	Obtenga acceso no autorizado a una cuenta de correo electrónico real que pertenezca a alguien y, a continuación, envíe mensajes de correo electrónico a otras víctimas como propietario legítimo de la cuenta de correo electrónico.	Todos

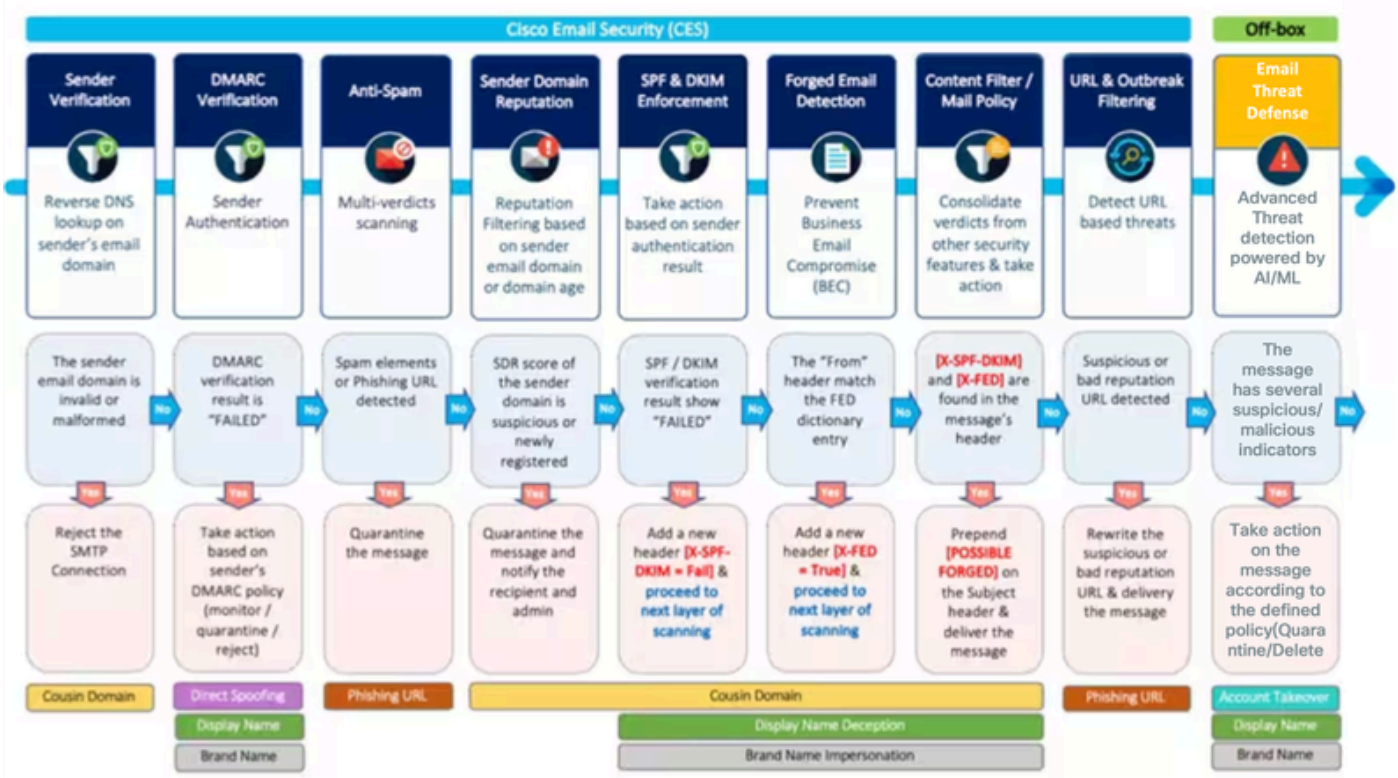
La primera categoría se refiere a abusos del nombre de dominio del propietario en el valor Envelope From (De sobre) del encabezado de Internet de un correo electrónico. Cisco Secure Email puede remediar este ataque mediante la verificación del servidor de nombres de dominio (DNS) del remitente para permitir solo remitentes legítimos. El mismo resultado se puede lograr globalmente mediante la verificación de DMARC, DKIM y SPF.

Sin embargo, las otras categorías solo infringen parcialmente la parte del dominio de la dirección de correo electrónico del remitente. Por lo tanto, no es fácil disuadirse cuando se utilizan registros de texto DNS o verificación de remitente solo. Idealmente, sería mejor combinar algunas funciones de Cisco Secure Email y Cisco Secure Email Threat Defence (ETD) para combatir estas amenazas avanzadas. Como sabe, la administración y configuración de las funciones de Cisco Secure Email puede variar de una organización a otra, y una aplicación incorrecta puede provocar una alta incidencia de falsos positivos. Por lo tanto, es esencial comprender las necesidades empresariales de la organización y adaptar las funciones.

Flujo de trabajo de defensa de correo electrónico falso

En el diagrama (Imagen 1) se muestran las funciones de seguridad que se ocupan de las prácticas recomendadas para supervisar, advertir y aplicar los ataques de suplantación. Los detalles de cada función se proporcionan en este documento. La mejor práctica es un enfoque de defensa en profundidad para detectar la suplantación de correo electrónico. Los atacantes pueden cambiar sus métodos con respecto a una organización con el tiempo, por lo que un administrador debe supervisar cualquier cambio y comprobar las advertencias y la aplicación adecuadas.

Imagen 1. Canal de defensa contra la suplantación de Cisco Secure Email

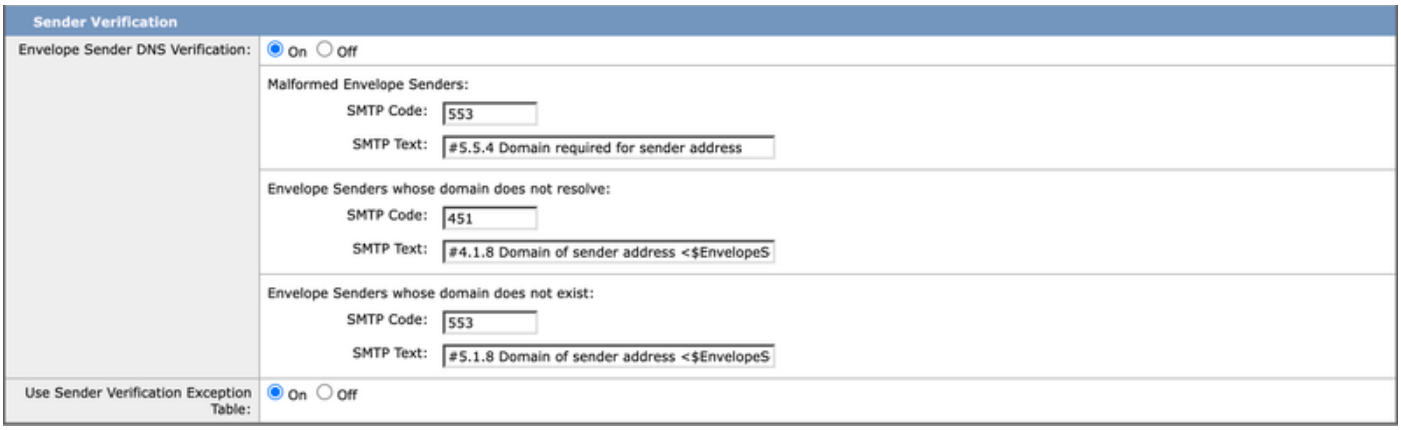


Capa 1: Verificación de validez en el dominio del remitente

La verificación de remitente es una forma más sencilla de evitar los correos electrónicos enviados desde un dominio de correo electrónico falso, como la suplantación del dominio de primos (por ejemplo, c1sc0.com es el impostor de cisco.com). Cisco Secure Email realiza una consulta de registro MX para el dominio de la dirección de correo electrónico del remitente y realiza una búsqueda de registro A en el registro MX durante la conversación SMTP. Si la consulta DNS devuelve NXDOMAIN, puede tratar el dominio como inexistente. Es una técnica habitual que los atacantes falsifiquen la información del remitente del sobre, de modo que el correo electrónico de un remitente no verificado se acepte y se procese posteriormente. Cisco Secure Email puede rechazar todos los mensajes entrantes que no pasen la comprobación de verificación que utiliza esta función, a menos que el dominio o la dirección IP del remitente se haya agregado previamente en la tabla de excepciones.

Práctica recomendada: configure Cisco Secure Email para que rechace la conversación SMTP si el dominio de correo electrónico del campo remitente del sobre no es válido. Permitir sólo remitentes legítimos mediante la configuración de la directiva de flujo de correo, la verificación de remitentes y la tabla de excepciones (opcional). Para obtener más información, visite Protección contra falsificación mediante la verificación de remitente.

Imagen 2. Sección Verificación de Remitente en Política de Flujo de Correo Predeterminada



Capa 2: verificación del encabezado De mediante DMARC

La verificación de DMARC es una función mucho más potente para luchar contra la suplantación de dominio directa, y también incluye los ataques de suplantación de marca y nombre de visualización. DMARC vincula la información autenticada con SPF o DKIM (origen o firma del dominio de envío) con lo que se presenta al destinatario final en el encabezado From y comprueba que los identificadores SPF y DKIM están alineados con el identificador del encabezado FROM.

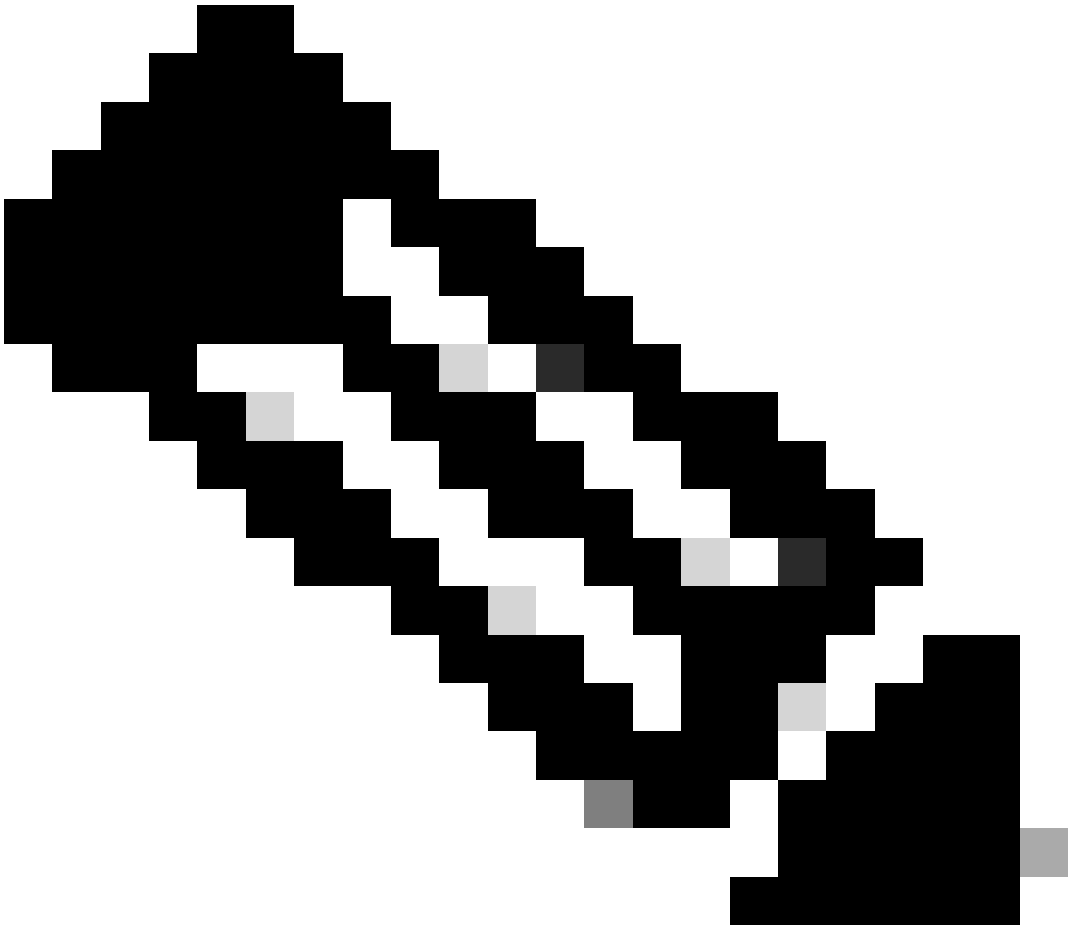
Para superar la verificación de DMARC, un correo electrónico entrante debe superar al menos uno de estos mecanismos de autenticación. Además, Cisco Secure Email también permite al administrador definir un perfil de verificación de DMARC para anular las políticas de DMARC del propietario del dominio y enviar informes de agregación (RUA) y de fallos/diagnóstico (RUF) a los propietarios del dominio. Esto ayuda a fortalecer sus implementaciones de autenticación a cambio.

Práctica recomendada: edite el perfil predeterminado de DMARC que utiliza las acciones de política de DMARC que aconseja el remitente. Además, la configuración global de la verificación de DMARC debe editarse para permitir la generación correcta de informes. Una vez que el perfil esté configurado correctamente, el servicio de verificación de DMARC debe estar habilitado en la política predeterminada de políticas de flujo de correo.

Imagen 3. Perfil de verificación de 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.



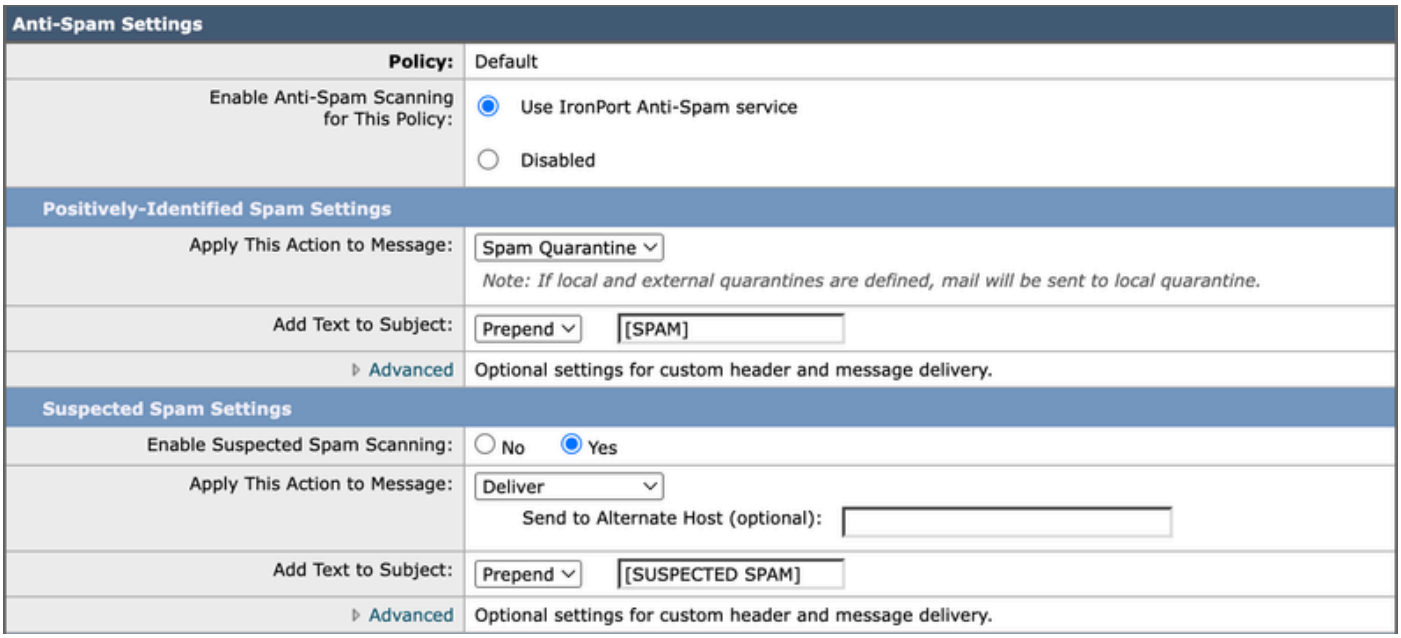
Nota: DMARC debe implementarse enviando al propietario del dominio junto con una herramienta de supervisión de dominios, como Cisco Domain Protection. Cuando se implementa de forma adecuada, la aplicación de DMARC en Cisco Secure Email ayuda a proteger frente a los correos electrónicos de suplantación de identidad enviados a los empleados desde remitentes o dominios no autorizados. Para obtener más información sobre Cisco Domain Protection, visite este enlace: Guía rápida de Cisco Secure Email Domain Protection.

Capa 3: evite que los spammers envíen correos electrónicos falsos

Los ataques de suplantación de identidad pueden ser otra forma habitual de una campaña de spam. Por lo tanto, es esencial habilitar la protección antispam para identificar de forma eficaz los correos electrónicos fraudulentos que contienen elementos de spam/phishing y bloquearlos positivamente. El antispam, combinado con otras acciones de prácticas recomendadas descritas en detalle en este documento, proporciona los mejores resultados sin perder correos electrónicos legítimos.

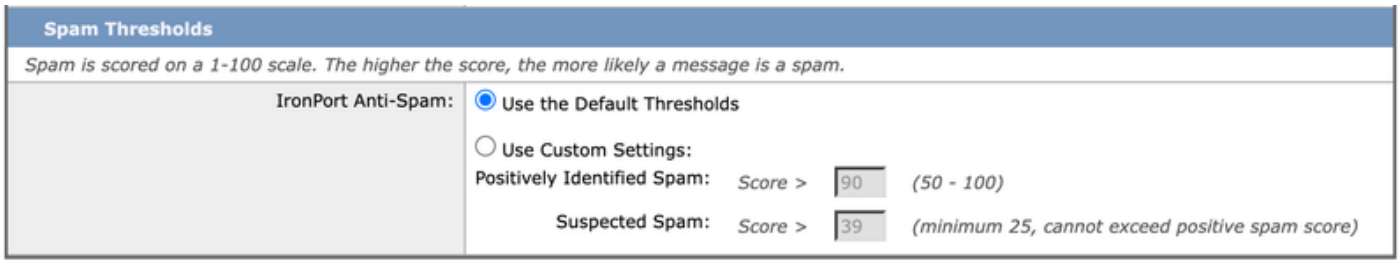
Práctica recomendada: active el análisis antispam en la política de correo predeterminada y establezca una acción de cuarentena para identificar positivamente la configuración de spam. Aumentar el tamaño mínimo de análisis de los mensajes de spam a al menos 2 millones globalmente.

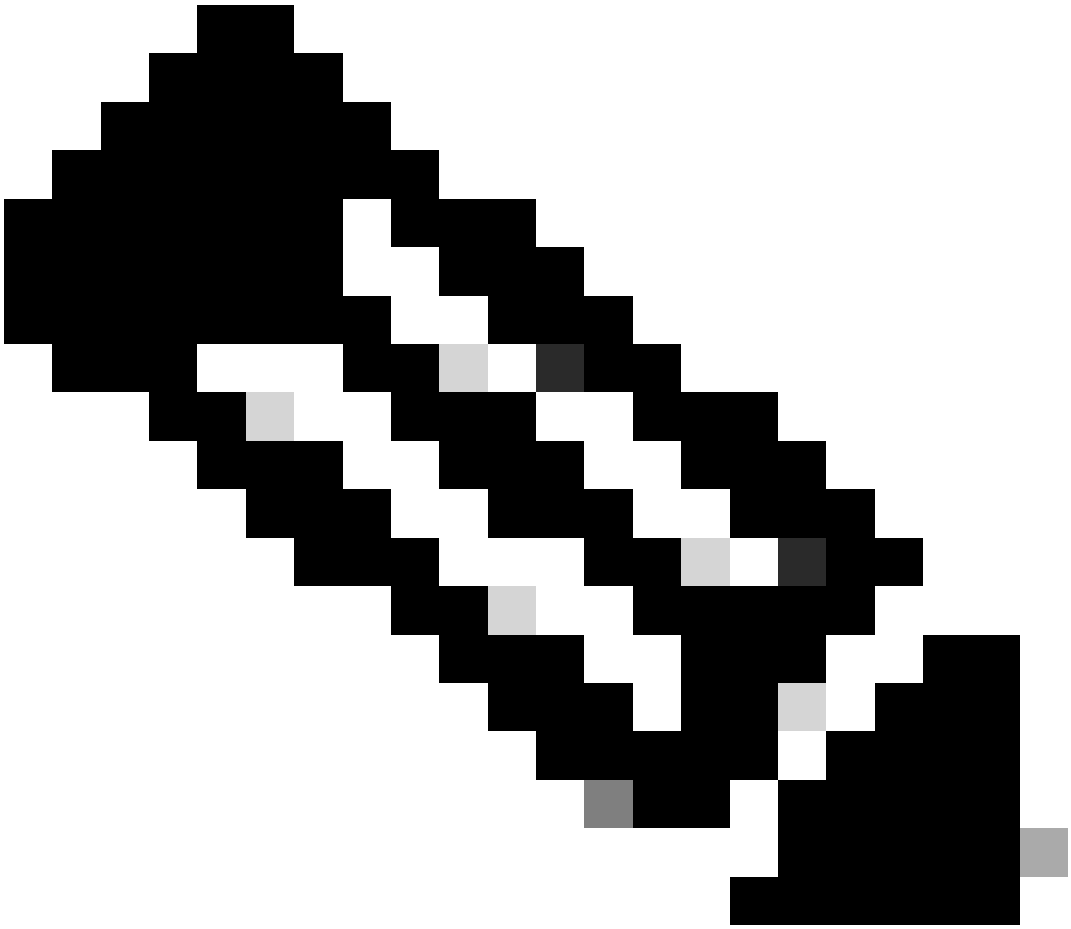
Imagen 4. Configuración Anti-Spam en Política de Correo Predeterminada



El umbral de spam se puede ajustar para que el spam positivo y sospechoso aumente o disminuya la sensibilidad (Imagen 5); sin embargo, Cisco desaconseja al administrador que lo haga y que utilice únicamente los umbrales predeterminados como línea de base, a menos que Cisco le indique lo contrario.

Imagen 5. Configuración de umbrales de antispam en la política de correo predeterminada





Nota: Cisco Secure Email ofrece un motor de análisis múltiple inteligente (IMS) complementario que proporciona diferentes combinaciones del motor antispam para aumentar los índices de detección de spam (el índice de detección más agresivo).

Capa 4: determinación de remitentes malintencionados mediante dominio de correo electrónico

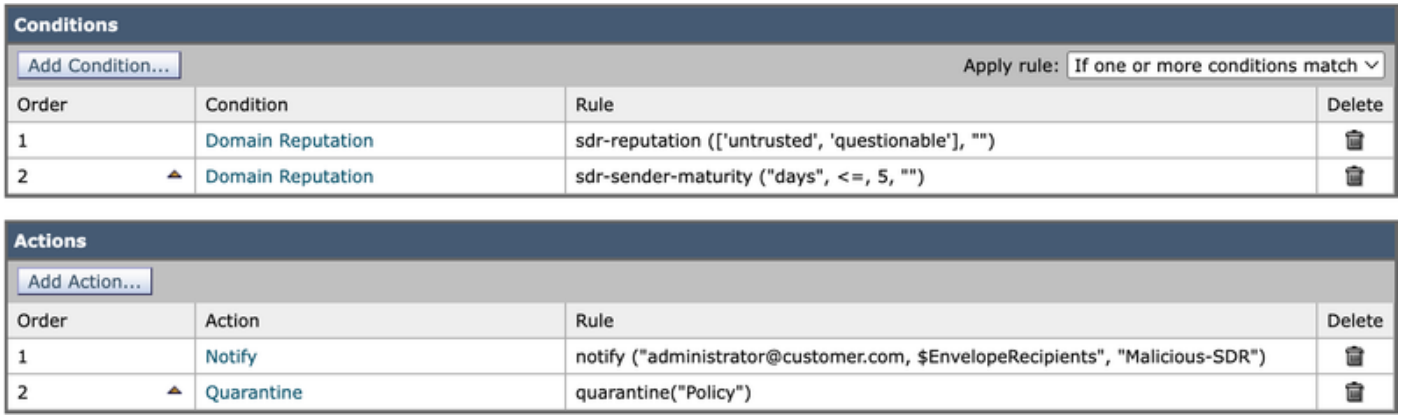
Cisco Talos Sender Domain Reputation (SDR) es un servicio en la nube que proporciona un veredicto de reputación para los mensajes de correo electrónico en función de los dominios del

sobre y el encabezado del correo electrónico. El análisis de reputación basado en dominios permite un mayor índice de detección de spam, ya que va más allá de la reputación de las direcciones IP compartidas, el alojamiento o los proveedores de infraestructura. En su lugar, deriva veredictos basados en las características asociadas con los nombres de dominio completos (FQDN) y otra información del remitente en la conversación SMTP (Protocolo simple de transferencia de correo) y los encabezados de los mensajes.

La madurez del remitente es una característica esencial para establecer la reputación del remitente. La madurez del remitente se genera automáticamente para la clasificación de spam en función de varias fuentes de información y puede diferir de la antigüedad del dominio basada en Whois. La madurez del remitente se establece en un límite de 30 días y, más allá de este límite, un dominio se considera maduro como remitente de correo electrónico y no se proporcionan más detalles.

Práctica recomendada: cree un filtro de contenido entrante que capture el dominio de envío en el que el veredicto de reputación de SDR se incluye en No fiable/Cuestionable o la madurez del remitente es inferior o igual a 5 días. La acción recomendada es poner el mensaje en cuarentena y notificarlo al administrador de seguridad de correo electrónico y al destinatario original. Para obtener más información sobre cómo configurar SDR, vea el vídeo de Cisco en Cisco Email Security Update (Versión 12.0): Sender Domain Reputation (SDR)

Imagen 6. Filtro de contenido para reputación de SDR y antigüedad del dominio con acciones de notificación y cuarentena.



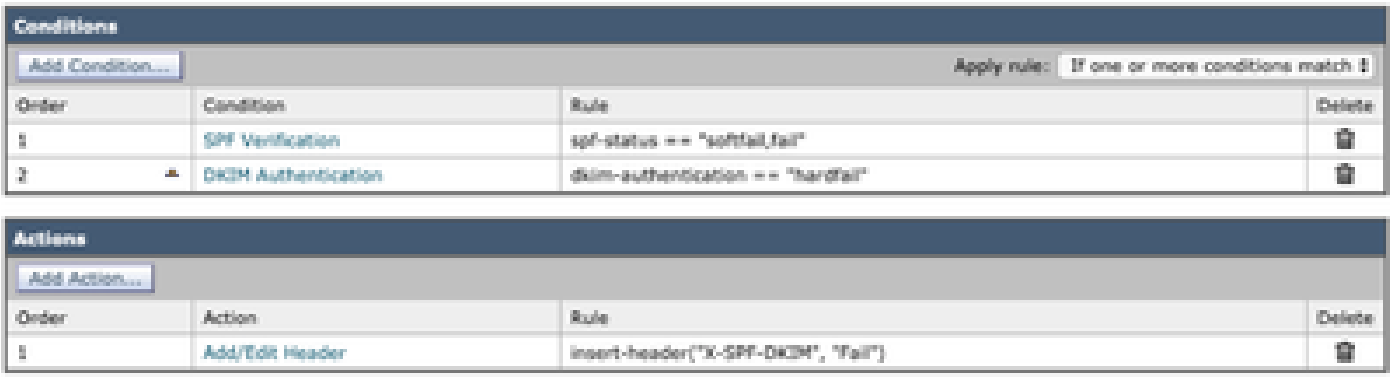
Capa 5: reducción de falsos positivos con resultados de verificación SPF o DKIM

Es imprescindible aplicar la verificación SPF o DKIM (ambas o una de ellas) para crear varias capas de detección de correo electrónico de suplantación para la mayoría de los tipos de ataques. En lugar de realizar una acción final (como descartar o poner en cuarentena), Cisco recomienda agregar un nuevo encabezado como [X-SPF-DKIM] en el mensaje que no supere la verificación SPF o DKIM y cooperar con el resultado mediante la función de detección de correo electrónico falsificado (FED), que se tratará más adelante, a favor de una tasa de captura mejorada de correos electrónicos de suplantación.

Práctica recomendada: cree un filtro de contenido que inspeccione los resultados de verificación SPF o DKIM de cada mensaje entrante que haya pasado por inspecciones anteriores. Agregue un nuevo encabezado X (por ejemplo, X-SPF-DKIM=Fail) en el mensaje que no supere la verificación

SPF o DKIM y se envíe a la siguiente capa de análisis: detección de correo electrónico falsificado (FED).

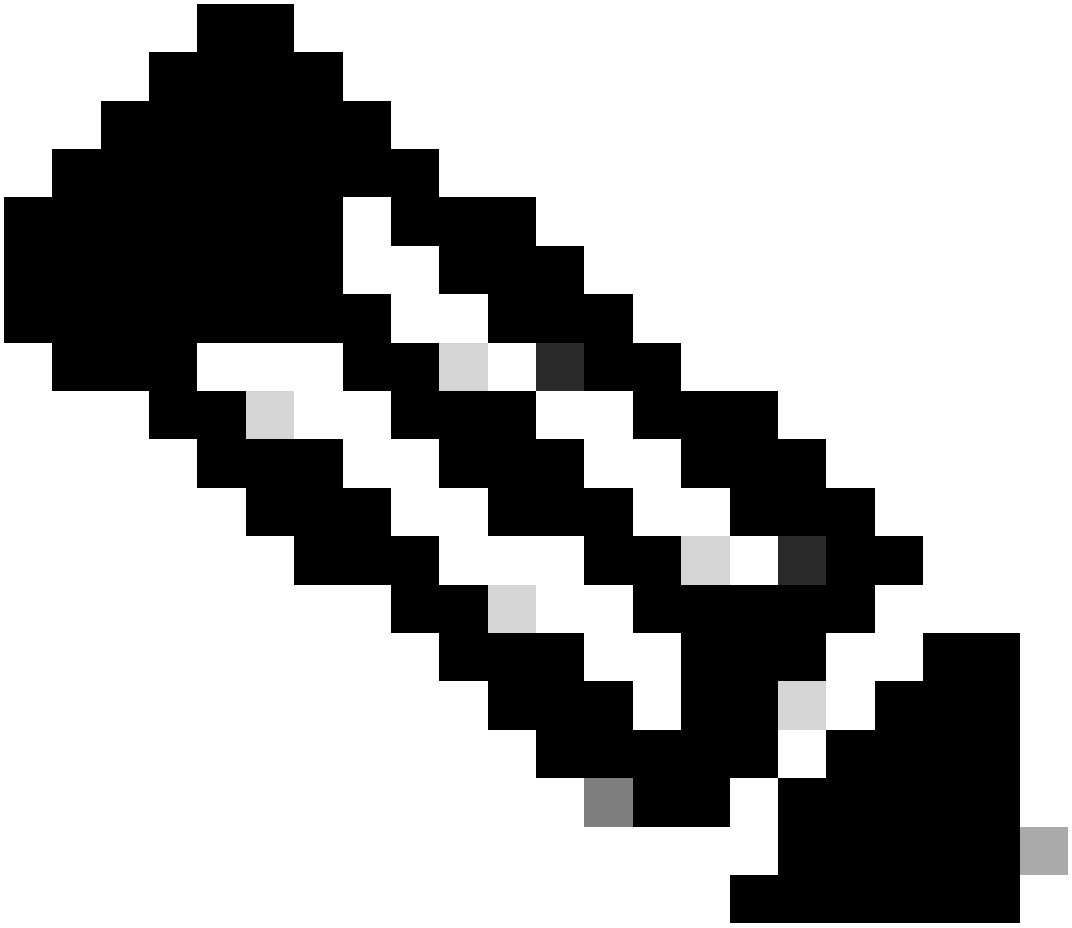
Imagen 7. Filtro de contenido que inspecciona los mensajes con resultados SPF o DKIM erróneos



Capa 6: Detecte mensajes con un nombre de remitente posiblemente falsificado

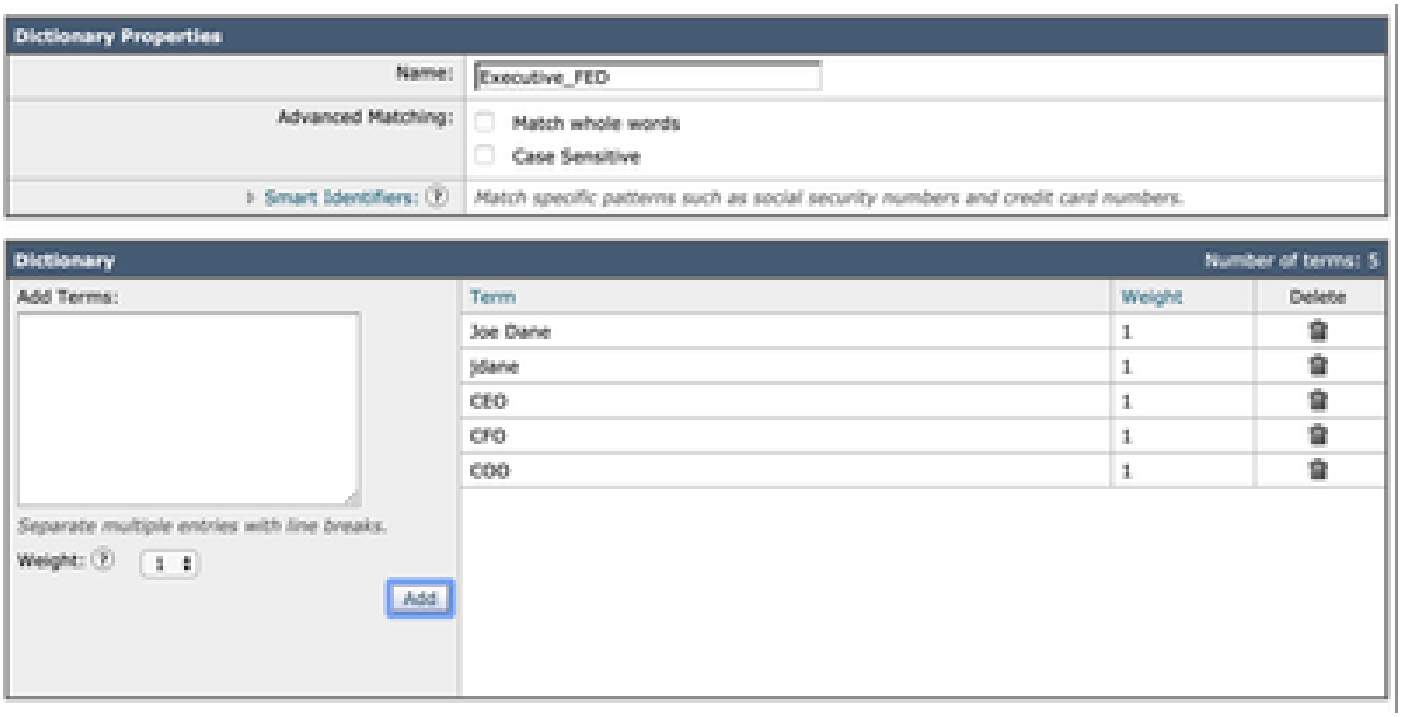
La detección de correo electrónico falsificado (FED), que complementa las verificaciones SPF, DKIM y DMARC, es otra línea de defensa fundamental contra la suplantación de correo electrónico. La FED es ideal para remediar los ataques de simulación que abusan del valor From en el cuerpo del mensaje. Dado que ya conoce los nombres de los ejecutivos dentro de la organización, puede crear un diccionario con estos nombres y, a continuación, hacer referencia a ese diccionario con la condición FED en los filtros de contenido. Además, aparte de los nombres de ejecutivos, puede crear un diccionario de dominios primos o parecidos basado en su dominio mediante el uso de DNSTWIST (DNSTWIT) para comparar con la suplantación de dominios parecidos.

Práctica recomendada: identifique a los usuarios de su organización cuyos mensajes puedan haber sido falsificados. Cree un diccionario personalizado que contabilice a los ejecutivos. Para cada nombre de ejecutivo, el diccionario debe incluir el nombre de usuario y todos los nombres de usuario posibles como términos (Imagen 8). Cuando el diccionario esté completo, utilice la detección de correo electrónico falsificado en el filtro de contenido para hacer coincidir el valor De de los mensajes entrantes con estas entradas del diccionario.



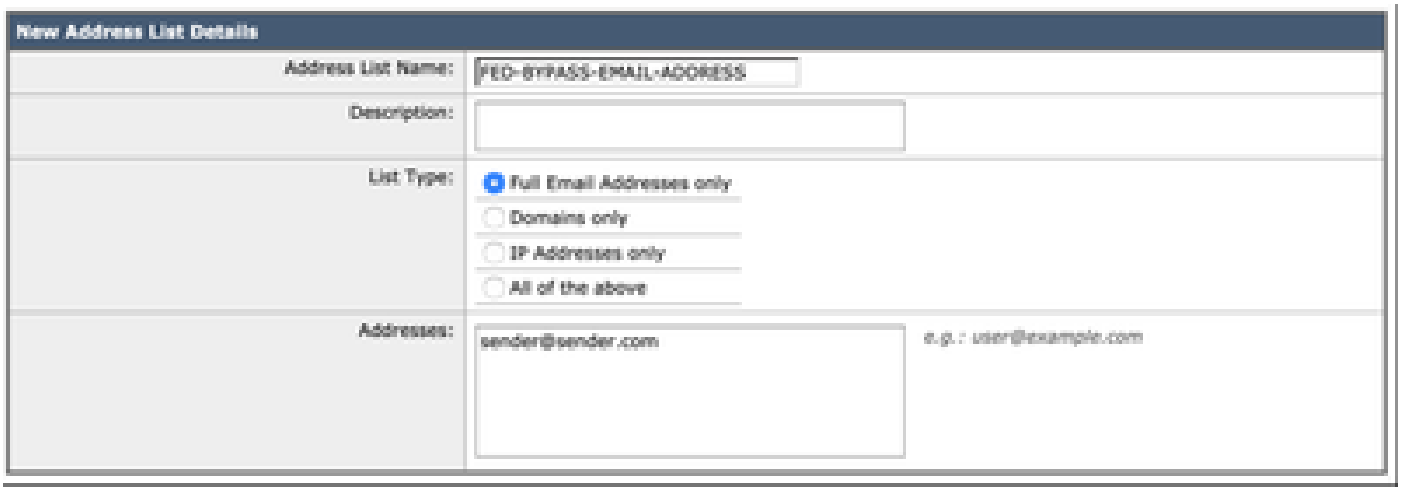
Nota: si se tiene en cuenta que la mayoría de los dominios no son permutaciones registradas, la verificación del remitente DNS protege frente a ellas. Si elige utilizar entradas de diccionario, preste atención solamente a los dominios registrados, y asegúrese de no exceder 500-600 entradas por diccionario.

Imagen 8. Directorio personalizado para detección de correo electrónico falsificado



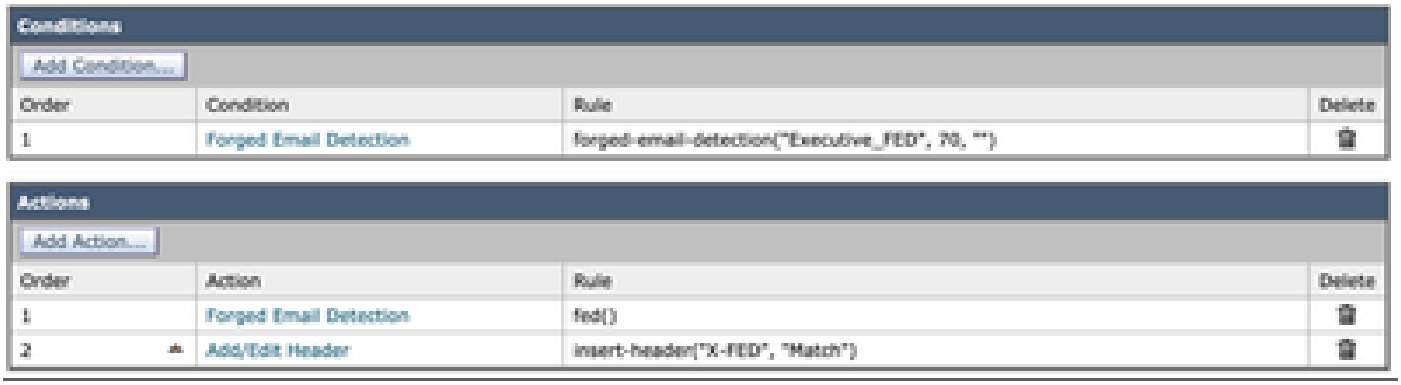
Es opcional agregar una condición de excepción para el dominio de correo electrónico en el envío de sobre para omitir la inspección de la FED. También se puede crear una lista de direcciones personalizada para omitir la inspección de la FED y pasar a una lista de direcciones de correo electrónico que se muestran en el encabezado Desde (Imagen 9).

Imagen 9. Crear una lista de direcciones para omitir la inspección FED



Aplique la acción de propietario Detección de correo electrónico falsificado para eliminar el valor De y revise la dirección de correo electrónico del remitente del sobre real en la bandeja de entrada del mensaje. A continuación, en lugar de aplicar una acción final, agregue un nuevo encabezado X (por ejemplo, X-FED=Match) en el mensaje que coincida con la condición y continúe entregando el mensaje a la siguiente capa de inspección (Imagen 10).

Imagen 10. Configuración de filtro de contenido recomendada para FED

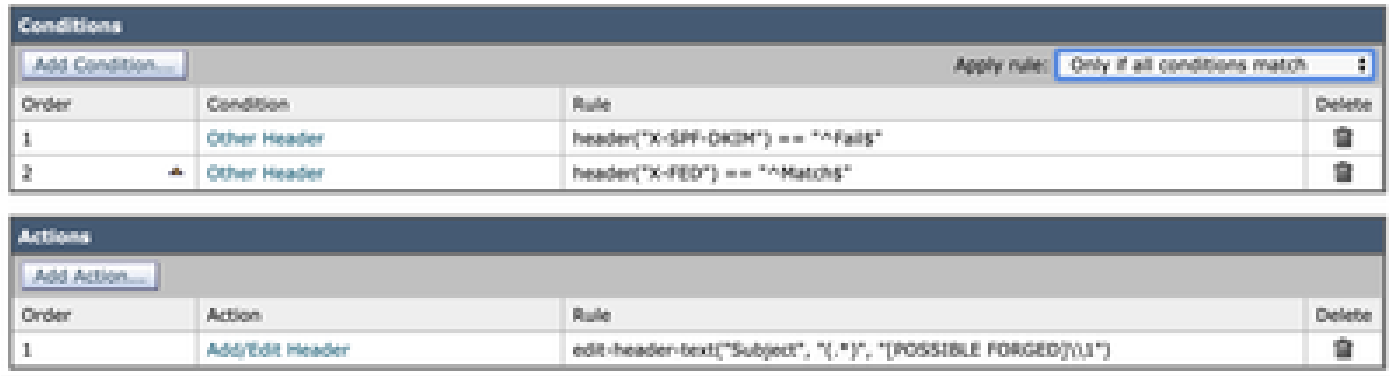


Capa 7: correo electrónico de simulación identificado positivamente

La identificación de una verdadera campaña de simulación es más eficaz al hacer referencia a otros veredictos de diversas funciones de seguridad de la planificación, como la información del encabezado X producida por SPF/DKIM Enforcement y FE. Por ejemplo, los administradores pueden crear un filtro de contenido para identificar los mensajes agregados con los nuevos encabezados X debido a resultados de verificación SPF / DKIM fallidos (X-SPF-DKIM=Fail) y que el encabezado From coincide con las entradas del diccionario FED (X-FED=Match).

La acción recomendada puede ser poner en cuarentena el mensaje y notificarlo al destinatario, o continuar entregando el mensaje original pero anteponiendo las palabras [POSIBLE FORJADO] a la línea Asunto como una advertencia al destinatario, como se muestra (Imagen 11).

Imagen 1. Combinar todos los X-encabezados en una sola regla (final)



Capa 8: protección frente a URL de phishing

La protección contra los enlaces de suplantación de identidad se incorpora en el filtrado de brotes y URL de Cisco Secure Email. Las amenazas combinadas combinan la suplantación de identidad y los mensajes de suplantación de identidad para parecer más legítimos para el objetivo. Habilitar el filtrado de brotes de virus es fundamental para detectar, analizar y detener estas amenazas en tiempo real. Merece la pena saber que la reputación de las URL se evalúa dentro del motor antispam y se puede utilizar como parte de la decisión para la detección de spam. Si el motor antispam no detiene el mensaje con la URL como spam, el filtrado de brotes y URL lo evalúa en la última parte del proceso de seguridad.

Recomendación: cree una regla de filtro de contenido que bloquee una URL con una puntuación

de reputación maliciosa y redirija la URL con una puntuación de reputación neutral a Cisco Security Proxy (Imagen 12). Active Threat Outbreak Filters activando la modificación de mensajes. La reescritura de URL permite que Cisco Security Proxy analice las URL sospechosas (Imagen 13). Para obtener más información, visite: [Configuración del filtrado de URL para Secure Email Gateway y Cloud Gateway]

Imagen 12. Filtro de contenido para reputación de URL

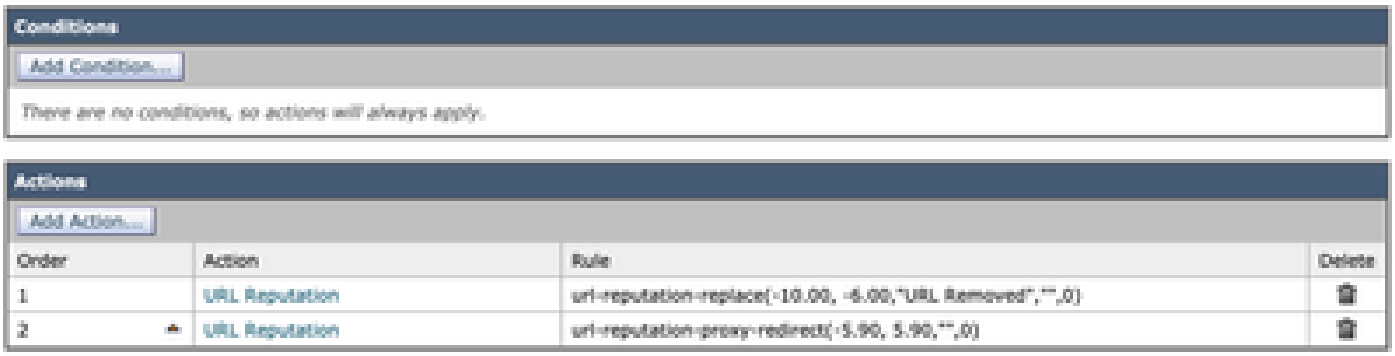
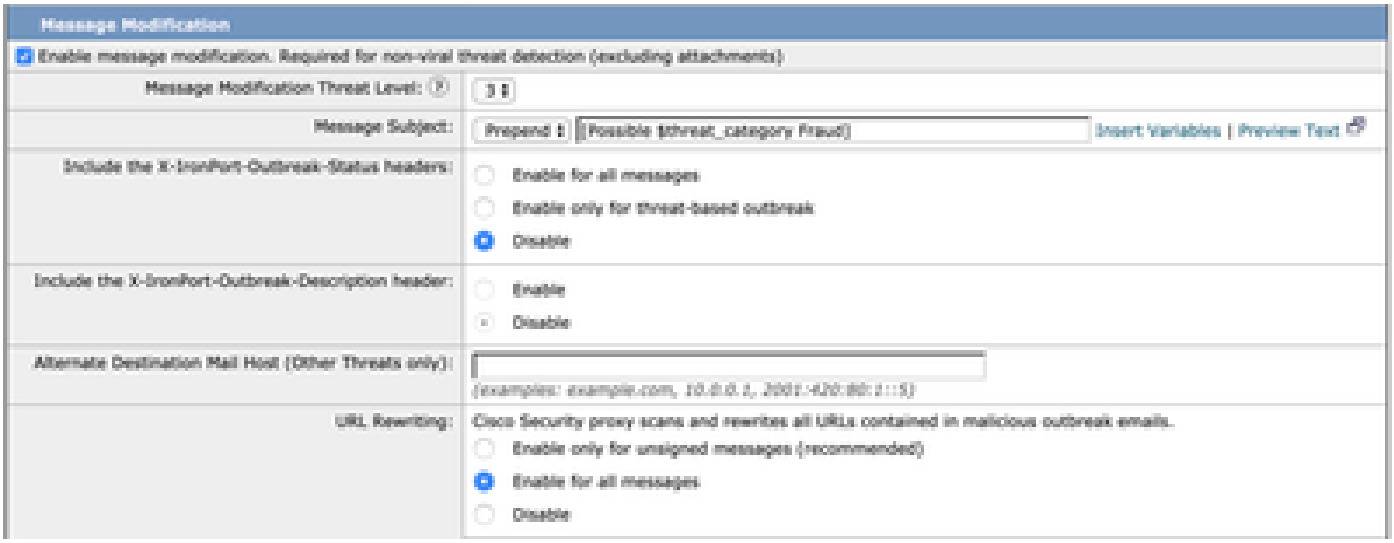


Imagen 13. Habilitar la reescritura de URL en el filtrado de brotes



Capa 9: aumente la capacidad de detección de suplantación con Cisco Secure Email Threat Defence (ETD)

Cisco ofrece Email Threat Defence, una solución nativa de la nube que aprovecha la excelente inteligencia de amenazas de Cisco Talos. Cuenta con una arquitectura habilitada por API para tiempos de respuesta más rápidos, visibilidad completa del correo electrónico, incluidos los correos electrónicos internos, una vista de conversación para obtener mejor información contextual y herramientas para la remediación automática o manual de las amenazas que acechan en los buzones de Microsoft 365. Visite la [hoja de datos de Cisco Secure Email Threat Defence] para obtener más información.

Cisco Secure Email Threat Defence combate la suplantación de identidad mediante la autenticación de remitentes y las funciones de detección de BEC. Integra el aprendizaje automatizado y los motores de inteligencia artificial que combinan la identidad local y el modelado

de relaciones con los análisis de comportamiento en tiempo real para proteger frente a amenazas basadas en el engaño de identidad. Modela el comportamiento del correo electrónico de confianza dentro de las organizaciones y entre individuos. Entre otras funciones clave, Email Threat Defence ofrece las siguientes ventajas:

- Descubra amenazas conocidas, emergentes y dirigidas con funciones avanzadas de detección de amenazas.
- Identificar técnicas maliciosas y obtener contexto para riesgos empresariales específicos.
- Busque rápidamente amenazas peligrosas y repárelas en tiempo real.
- Utilice la telemetría de amenazas en la que se pueden realizar búsquedas para categorizar las amenazas y comprender qué partes de su organización son más vulnerables a los ataques.

Figura 14. Cisco Secure Email Threat Defence proporciona información sobre cómo se dirige su organización.

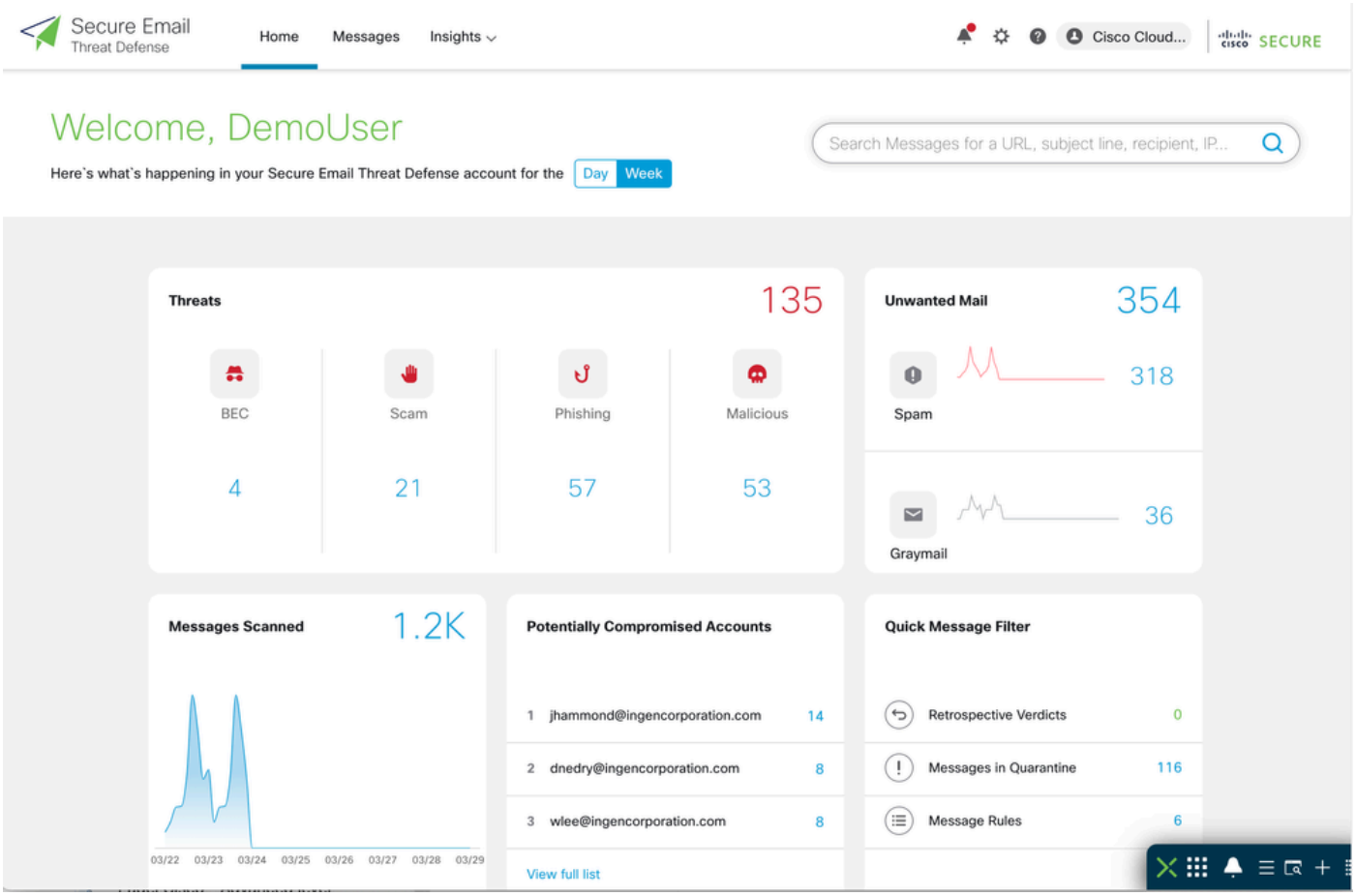
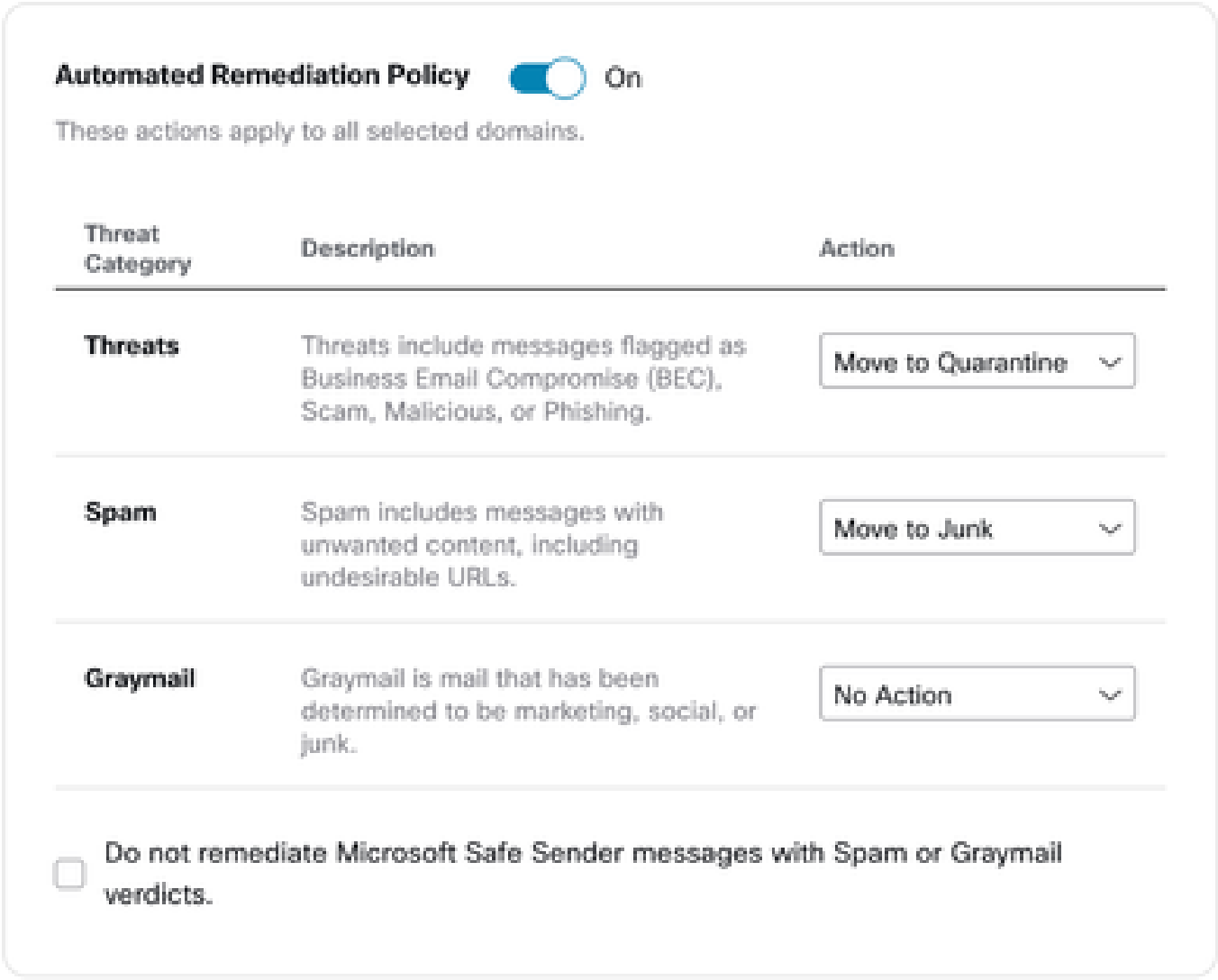


Imagen 15. La configuración de la política de Cisco Email Threat Defence determina automáticamente si el mensaje coincide con la categoría de amenaza seleccionada



¿Qué más puede hacer con la prevención de la suplantación?

Muchas suplantaciones se pueden remediar con algunas precauciones simples que incluyen, entre otras:

- Limite el permiso de dominios enumerados en la tabla de acceso de host (HAT) a muy pocos partners empresariales principales.
- Realice un seguimiento continuo de los miembros del grupo de remitentes SPOOF_ALLOW y actualícelos si ha creado uno y utilice las instrucciones que se proporcionan en el enlace de prácticas recomendadas.
- Habilite la detección de graymail y colóquelos también en la cuarentena de spam.

Pero lo más importante de todo, habilite SPF, DKIM y DMARC e impleméntelo de forma adecuada. Sin embargo, la guía sobre la publicación de registros SPF, DKIM y DMARC está fuera del alcance de este documento. Para ello, consulte este informe técnico: Prácticas recomendadas de autenticación de correo electrónico: formas óptimas de implementar SPF, DKIM y DMARC.

Comprenda el reto de remediar los ataques de correo electrónico como las campañas de suplantación aquí descritas. Si tiene dudas sobre la implementación de estas prácticas

recomendadas, póngase en contacto con el soporte técnico de Cisco y abra un caso. También puede ponerse en contacto con su equipo de cuentas de Cisco para obtener una solución y orientación sobre el diseño. Para obtener más información sobre Cisco Secure Email, consulte el sitio web de Cisco Secure Email.

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).