Detectar e evitar falsificação de email

Contents

Introdução

Este documento descreve como detectar e evitar falsificação de e-mail ao usar o Cisco Secure Email.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos.

- E-mail seguro da Cisco

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Sobre este documento

Este documento destina-se a clientes da Cisco, parceiros de canal da Cisco e engenheiros da Cisco que implantam o Cisco Secure Email. Este documento abrange:

- O que é falsificação de e-mail?
- Fluxo de Trabalho de Defesa contra Falsificação de Email
- O que mais você pode fazer com a prevenção contra falsificação?

O que é falsificação de email

Falsificação de e-mail é uma falsificação de cabeçalho de e-mail em que a mensagem parece ter se originado de alguém ou em algum outro lugar que não seja a origem real. O Email Spoofing é usado em campanhas de phishing e spam, pois as pessoas tendem a abrir um email quando acham que uma fonte legítima e confiável o enviou. Para obter mais informações sobre falsificação, consulte O que é falsificação de email e Como detectá-la.

O Spoofing de e-mail se enquadra nestas categorias:

Categoria	Descrição	Destino principal
Falsificação direta de domínio	Representar um domínio semelhante no Envelope De como o domínio do destinatário.	Funcionários
Decepção de Nome de Exibição	O cabeçalho De mostra um remetente legítimo com um nome executivo de uma organização. Eles também são conhecidos como Business Email Compromise (BEC).	Funcionários
Representação de Nome de Marca	O cabeçalho De mostra um remetente legítimo com o nome de marca de uma empresa bem conhecida.	Clientes/parceiros
Ataque baseado em URL de phishing	Um e-mail com um URL que tenta roubar dados confidenciais ou informações de login da vítima. Um e-mail falso de um banco que solicita que você clique em um link e verifique os detalhes de sua conta é um exemplo de um ataque de phishing baseado em URL.	Funcionários/parceiros
Ataque de Domínio de Primo ou Parecido	O valor do cabeçalho Envelope de ou De mostra um endereço de remetente semelhante que se passa por um endereço real para ignorar as inspeções Sender Policy Framework (SPF), DomainKeys Identified Mail	Funcionários/parceiros

	(DKIM) e Domain-based Message Authentication, Reporting and Conformance (DMARC).	
Transferência de conta / Conta comprometida	Obtenha acesso não autorizado a uma conta de e-mail real que pertença a alguém e envie e-mails para outras vítimas como o proprietário legítimo da conta de e-mail.	Todos

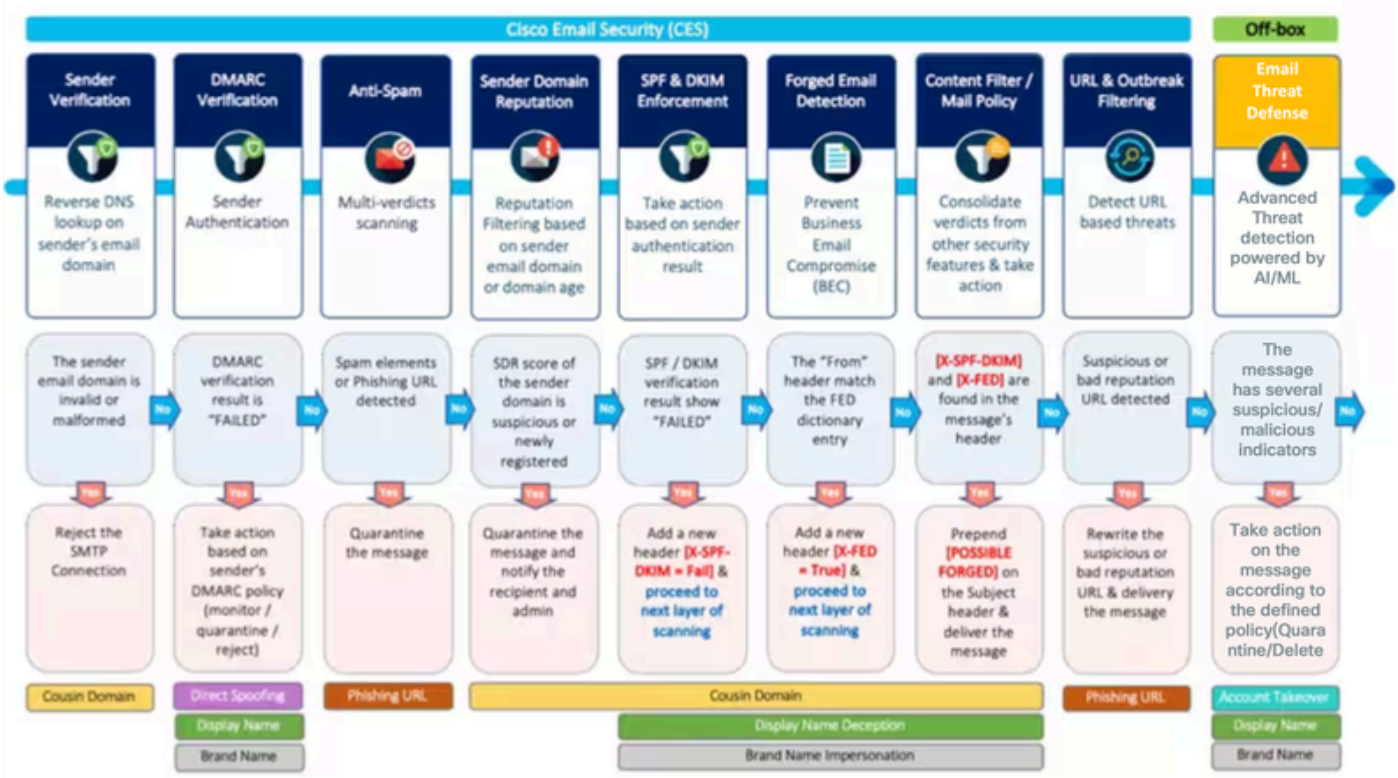
A primeira categoria refere-se a abusos do nome de domínio do proprietário no valor Envelope From no cabeçalho de Internet de um e-mail. O Cisco Secure Email pode corrigir esse ataque usando a verificação do Servidor de Nome de Domínio (DNS) do remetente para permitir apenas remetentes legítimos. O mesmo resultado pode ser obtido globalmente usando a verificação DMARC, DKIM e SPF.

No entanto, as outras categorias violam apenas parcialmente a parte do domínio do endereço de e-mail do remetente. Por isso, não é fácil ser dissuadido quando você usa registros de texto DNS ou verificação de remetente apenas. Idealmente, seria melhor combinar alguns recursos do Cisco Secure Email e do Cisco Secure Email Threat Defense (ETD) para combater essas ameaças avançadas. Como você já sabe, a administração e a configuração de recursos do Cisco Secure Email podem variar de empresa para empresa, e aplicativos inadequados podem levar a uma alta incidência de falsos positivos. Portanto, é essencial entender as necessidades comerciais da organização e personalizar os recursos.

Fluxo de Trabalho de Defesa contra Falsificação de Email

Os recursos de segurança que abordam as melhores práticas para monitorar, avisar e impor contra ataques de falsificação são mostrados no diagrama (Imagem 1). Os detalhes de cada recurso são fornecidos neste documento. A prática recomendada é uma abordagem de defesa aprofundada para detectar falsificação de e-mail. Os invasores podem alterar seus métodos em relação a uma empresa ao longo do tempo, portanto um administrador deve monitorar todas as alterações e verificar os avisos e a aplicação apropriados.

Imagem 1. Pipeline de Defesa do Spoof do E-mail Seguro da Cisco

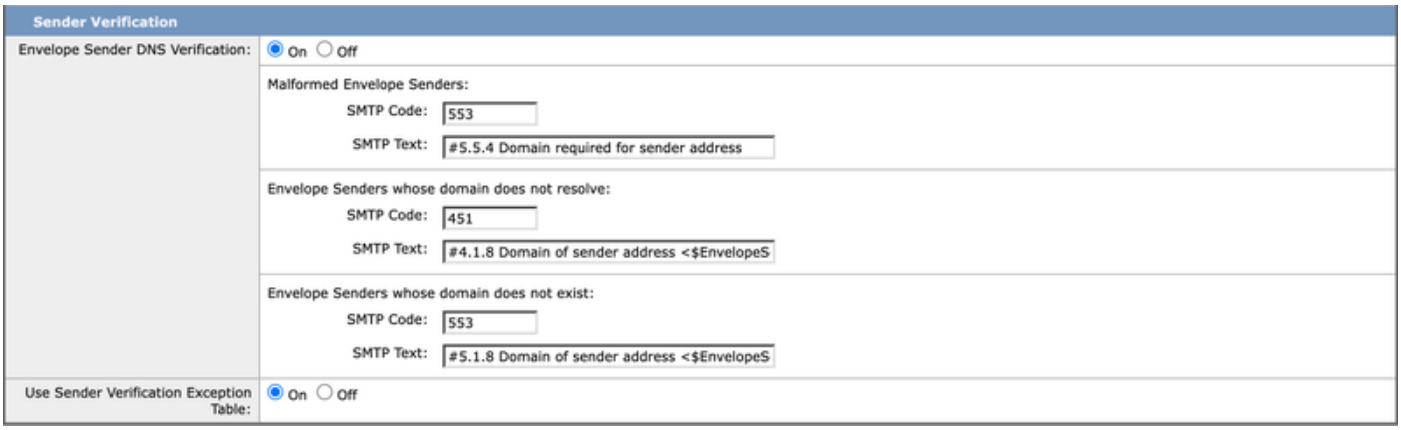


Camada 1: Verificação de validade no domínio do remetente

A verificação de remetente é uma maneira mais simples de evitar emails enviados de um domínio de email falso, como falsificação de domínio primo (por exemplo, c1sc0.com é o impostor de cisco.com). O Cisco Secure Email faz uma consulta de registro MX para o domínio do endereço de e-mail do remetente e executa uma pesquisa de registro A no registro MX durante a conversação SMTP. Se a consulta DNS retornar NXDOMAIN, ela poderá tratar o domínio como inexistente. É uma técnica comum para invasores forjar as informações do remetente do envelope para que o e-mail de um remetente não verificado seja aceito e processado posteriormente. O Cisco Secure Email pode rejeitar todas as mensagens recebidas que falharem na verificação de verificação que usa esse recurso, a menos que o domínio ou endereço IP do remetente seja pré-adicionado na Tabela de Exceções.

Prática recomendada: configurar o Cisco Secure Email para rejeitar a conversação SMTP se o domínio de e-mail do campo do remetente de envelope for inválido. Permitir apenas remetentes legítimos configurando a política de fluxo de mensagens, a verificação do remetente e a tabela de exceções (opcional). Para obter mais informações, visite Spoof Protection using Sender Verification.

Imagem 2. Seção Verificação de Remetente na Política de Fluxo de E-mail Padrão



Camada 2: Verificar o cabeçalho De usando DMARC

A verificação de DMARC é um recurso muito mais poderoso para combater a Falsificação direta de domínio e também inclui ataques de Nome de exibição e Representação de marca. O DMARC une informações autenticadas com SPF ou DKIM (origem ou assinatura do domínio de envio) com o que é apresentado ao destinatário final no cabeçalho De e verifica se os identificadores SPF e DKIM estão alinhados com o identificador de cabeçalho DE.

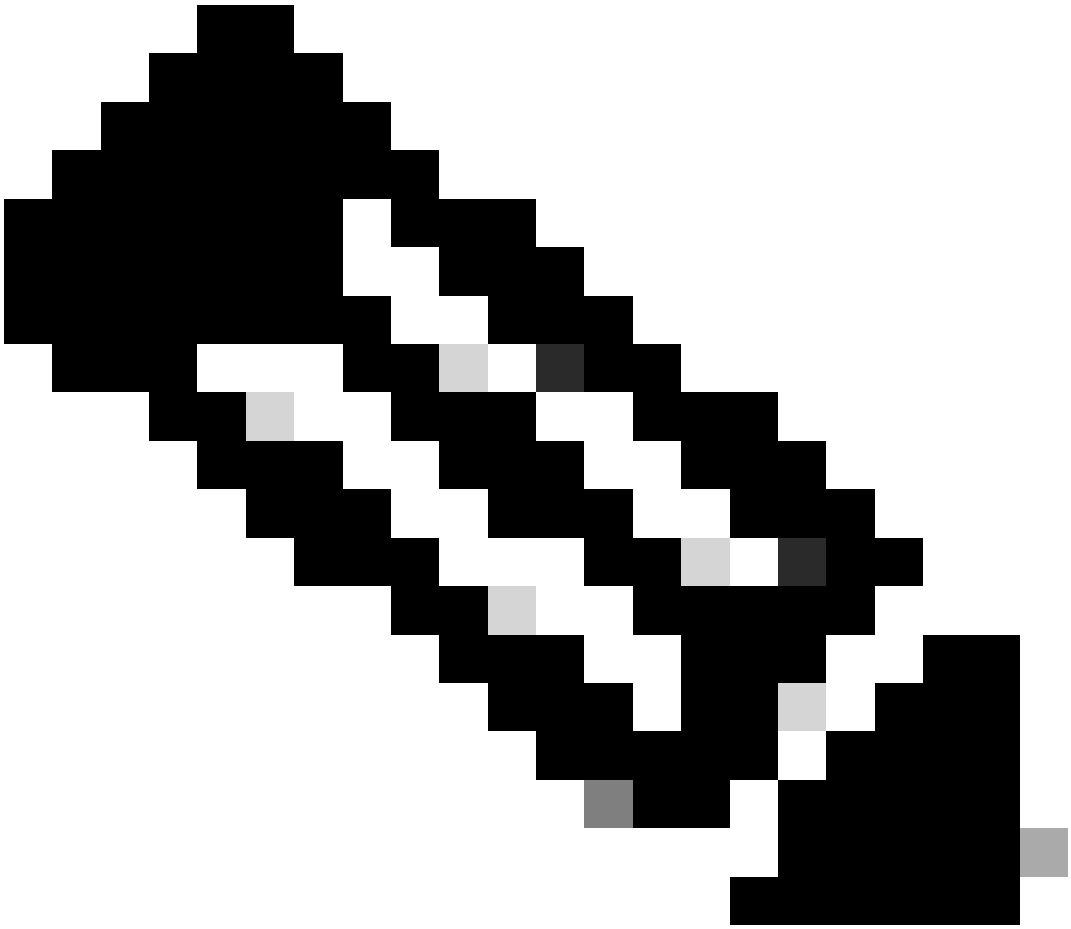
Para passar na verificação DMARC, um e-mail de entrada deve passar em pelo menos um desses mecanismos de autenticação. Além disso, o Cisco Secure Email também permite que o administrador defina um perfil de verificação de DMARC para substituir as políticas de DMARC do proprietário do domínio e enviar relatórios agregados (RUA) e de falha/análise (RUF) aos proprietários do domínio. Isso ajuda a fortalecer as implantações de autenticação.

Prática recomendada: edite o perfil DMARC padrão que usa as ações de política de DMARC aconselhadas pelo remetente. Além disso, as configurações globais da verificação DMARC devem ser editadas para permitir a geração correta de relatórios. Quando o perfil estiver configurado corretamente, o serviço de verificação DMARC deverá ser habilitado na política padrão das Políticas de fluxo de e-mail.

Imagem 3. Perfil de verificação 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.



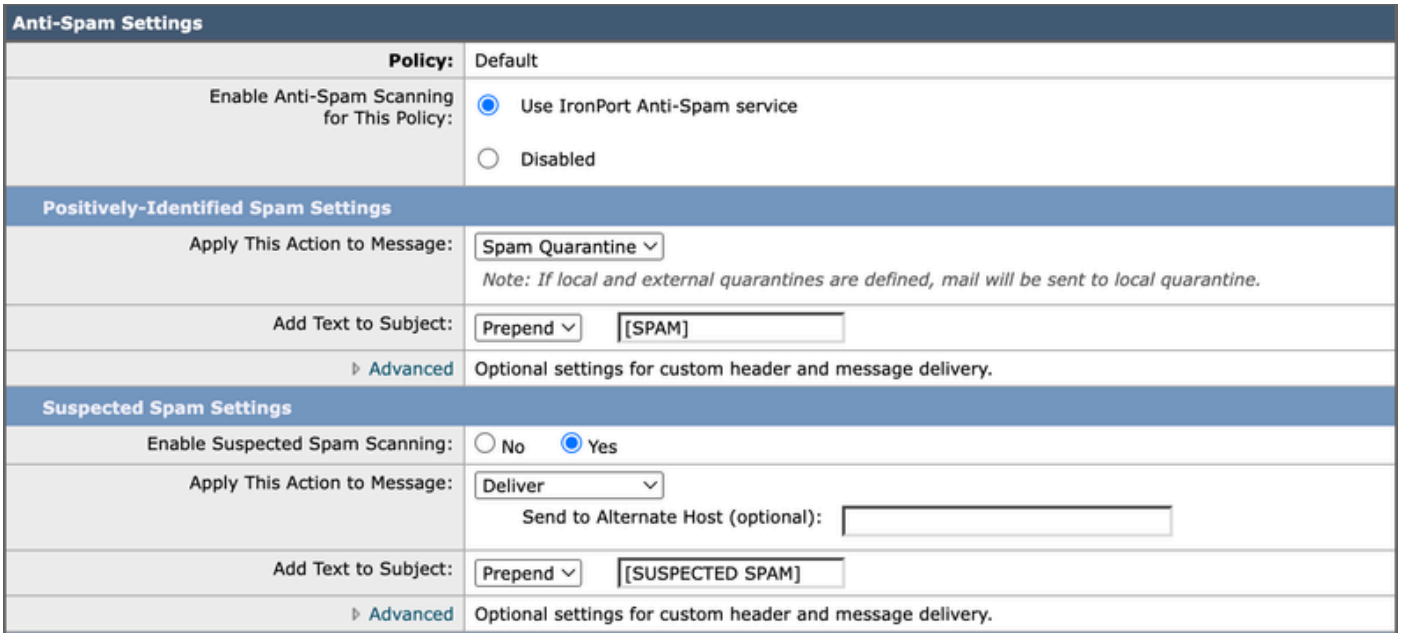
Observação: o DMARC deve ser implementado enviando o proprietário do domínio em conjunto com uma ferramenta de monitoramento de domínio, como o Cisco Domain Protection. Quando implementado adequadamente, a aplicação de DMARC no Cisco Secure Email ajuda a proteger contra e-mails de phishing enviados a funcionários de remetentes ou domínios não autorizados. Para obter mais informações sobre o Cisco Domain Protection, acesse este link: Resumo do Cisco Secure Email Domain Protection.

Camada 3: Impedir que spammers enviem emails falsificados

Os ataques de falsificação podem ser outra forma comum de campanha de spam. Portanto, ativar a proteção antisspam é essencial para identificar com eficiência e bloquear e-mails fraudulentos que contenham elementos de spam/phishing. O antisspam, combinado com outras práticas recomendadas amplamente descritas neste documento, fornece os melhores resultados sem perder e-mails legítimos.

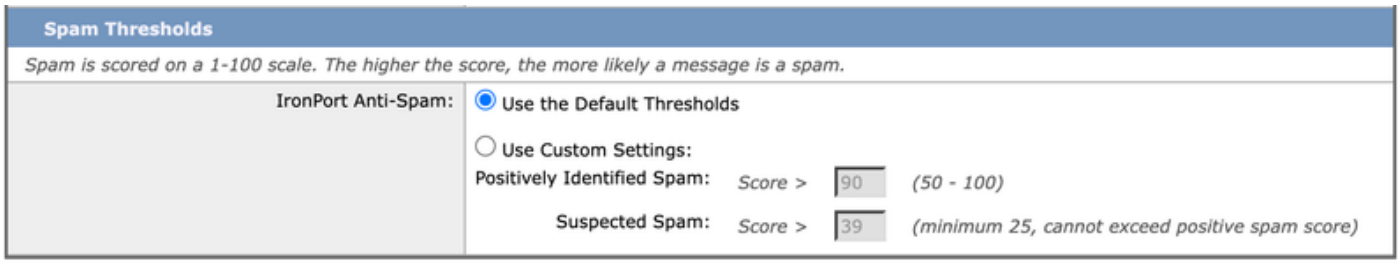
Prática recomendada: ativar a varredura antisspam na política de e-mail padrão e definir a ação de quarentena para identificar as configurações de spam de forma positiva. Aumente o tamanho mínimo de varredura para mensagens de spam para pelo menos 2M globalmente.

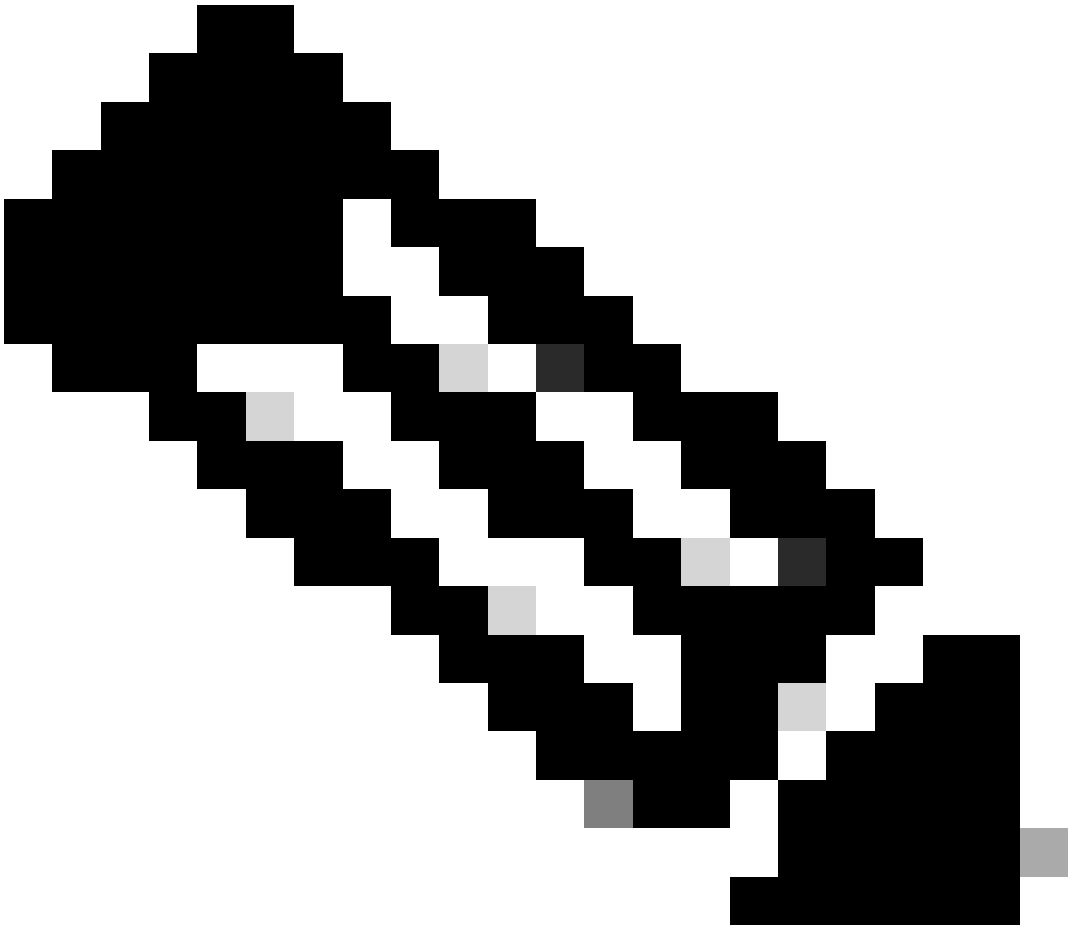
Imagem 4. Configuração de antisspam na política de e-mail padrão



O Limite de spam pode ser ajustado para Spam positivo e Suspeito para aumentar ou diminuir a sensibilidade (Imagem 5); no entanto, a Cisco desencoraja o administrador de fazer isso e de usar apenas os limites padrão como uma linha de base, a menos que a Cisco informe o contrário.

Imagem 5. Definição de Limites de Anti-Spam na Política de E-mail Padrão





Observação: o Cisco Secure Email oferece um mecanismo complementar Intelligent Multi-Scan (IMS) que oferece diferentes combinações do mecanismo antisspam para aumentar as taxas de captura de spam (a taxa de captura mais agressiva).

Camada 4: Determinar remetentes mal-intencionados via domínio de e-mail

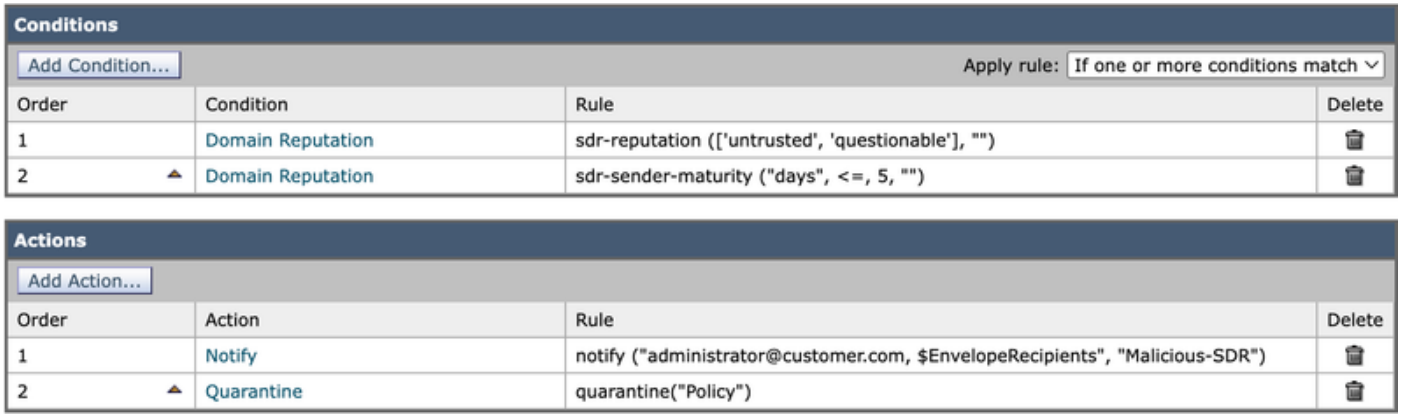
O Cisco Talos Sender Domain Reputation (SDR) é um serviço de nuvem que fornece um veredito de reputação para mensagens de e-mail com base nos domínios no cabeçalho e no envelope de e-mail. A análise de reputação baseada em domínio permite uma taxa de captura de spam mais alta, olhando além da reputação de endereços IP compartilhados, hospedagem ou provedores de

infraestrutura. Em vez disso, ele deriva vereditos com base em recursos associados a nomes de domínio totalmente qualificados (FQDNs) e outras informações de remetente na conversação SMTP (Simple Mail Transfer Protocol) e cabeçalhos de mensagem.

A maturidade do remetente é um recurso essencial para estabelecer a reputação do remetente. A maturidade do remetente é gerada automaticamente para classificação de spam com base em várias fontes de informação e pode ser diferente da idade do domínio baseado em Whois. A maturidade do remetente é definida para um limite de 30 dias e, além desse limite, um domínio é considerado maduro como um remetente de e-mail e nenhum detalhe adicional é fornecido.

Prática recomendada: crie um filtro de conteúdo de entrada que capture o domínio de envio no qual o veredito de reputação do SDR se enquadra em Não confiável/Questionável ou a Maturidade do remetente é menor ou igual a 5 dias. A ação recomendada é colocar a mensagem em quarentena e notificar o administrador de segurança de e-mail e o destinatário original. Para obter mais informações sobre como configurar o SDR, assista ao vídeo da Cisco em Cisco Email Security Update (Version 12.0): Sender Domain Reputation (SDR)

Imagem 6. Filtro de conteúdo para Reputação SDR e Idade do domínio com ações de notificação e quarentena.

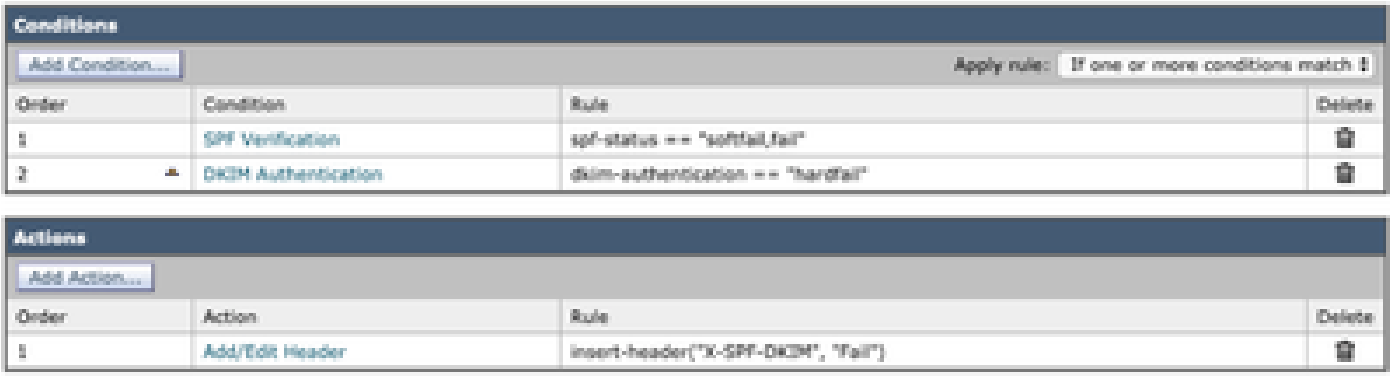


Camada 5: Reduzir falsos positivos com resultados de verificação de SPF ou DKIM

É essencial aplicar a verificação de SPF ou DKIM (ambos ou um dos dois) para criar várias camadas de detecção de e-mail falso para a maioria dos tipos de ataque. Em vez de tomar uma ação final (como descartar ou quarentena), a Cisco recomenda adicionar um novo cabeçalho, como [X-SPF-DKIM], na mensagem que falhar na verificação de SPF ou DKIM e cooperar com o resultado com o recurso Forged Email Detection (FED), que é abordado posteriormente, em favor de uma taxa de captura aprimorada de emails de falsificação.

Prática recomendada: criar um filtro de conteúdo que inspecione os resultados de verificação SPF ou DKIM de cada mensagem recebida que passou por inspeções anteriores. Adicione um novo cabeçalho X (por exemplo, X-SPF-DKIM=Fail) à mensagem que falhar na verificação de SPF ou DKIM e entregar à próxima camada de verificação - Detecção de e-mail forjado (FED).

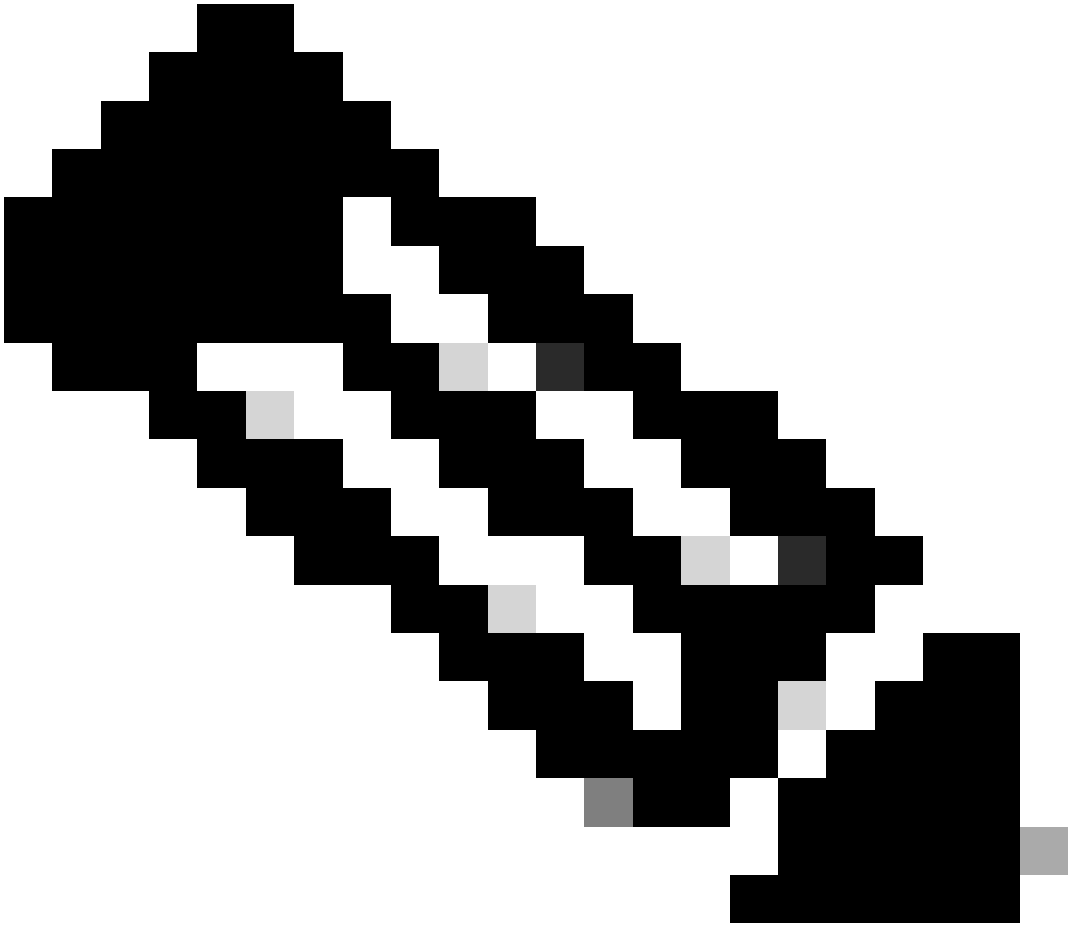
Imagem 7. Filtro de conteúdo que inspeciona mensagens com resultados SPF ou DKIM com falha



Camada 6: Detectar mensagens com nome de remetente possivelmente forjado

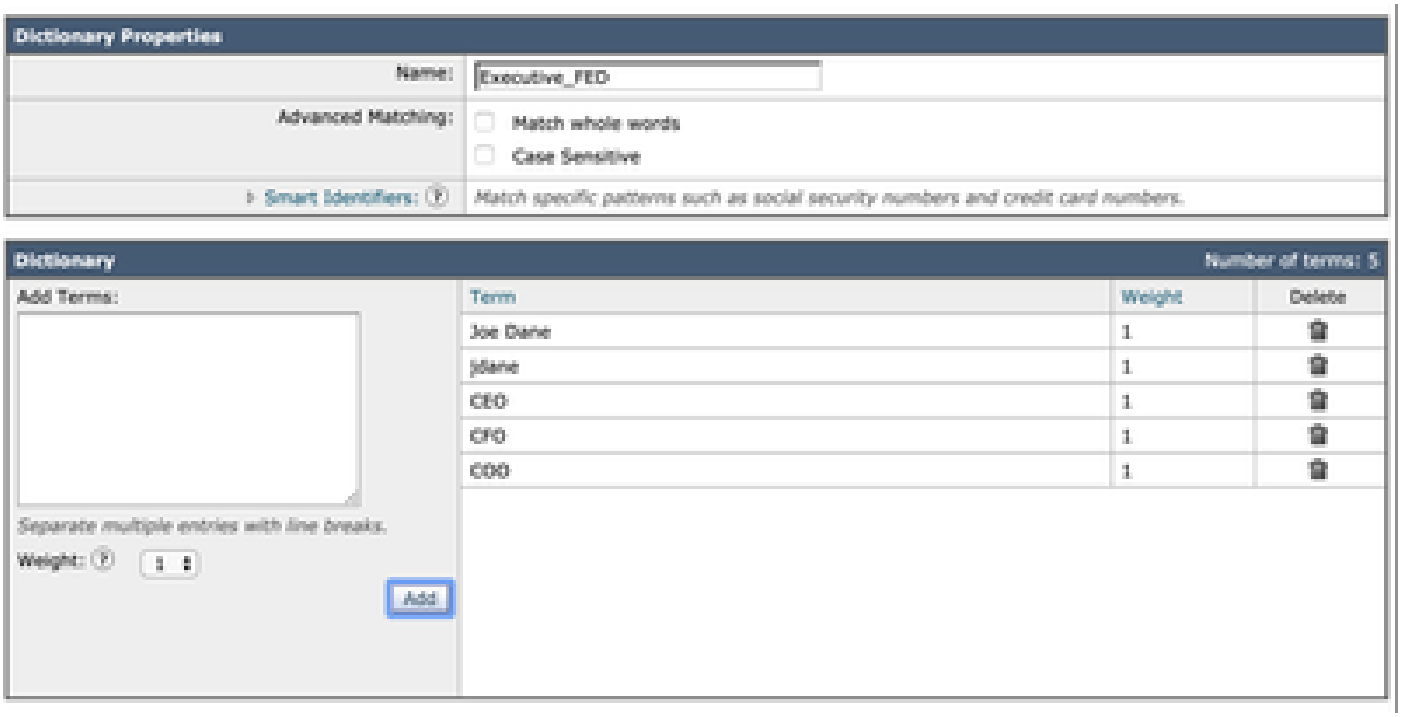
Complementando as verificações de SPF, DKIM e DMARC, a detecção de e-mail forjado (FED) é outra linha de defesa crucial contra falsificação de e-mail. O FED é ideal para remediar ataques de paródia que abusam do valor De no corpo da mensagem. Como você já sabe os nomes executivos na organização, é possível criar um dicionário desses nomes e depois referenciar esse dicionário com a condição FED nos filtros de conteúdo. Além disso, além dos nomes executivos, você pode criar um dicionário de domínios de primos ou sósias com base em seu domínio usando DNSTWIST (DNSTWIT) para comparar com falsificação de domínio de sósias.

Prática recomendada: identifique os usuários em sua organização cujas mensagens provavelmente são forjadas. Crie um dicionário personalizado que seja responsável pelos executivos. Para cada nome executivo, o dicionário deve incluir o nome de usuário e todos os nomes de usuário possíveis como termos (Imagem 8). Quando o dicionário estiver concluído, use a Detecção de e-mail forjado no filtro de conteúdo para corresponder o valor De das mensagens recebidas com essas entradas do dicionário.



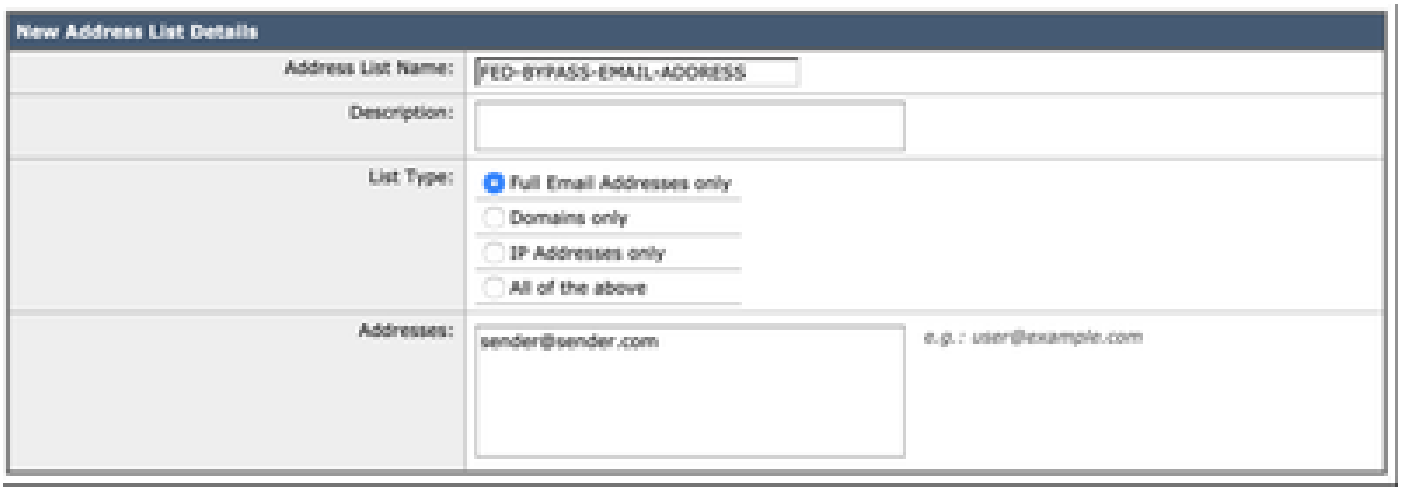
Observação: considerando que a maioria dos domínios não são permutações registradas, a verificação do remetente DNS protege contra elas. Se você optar por usar entradas de dicionário, preste atenção apenas aos domínios registrados e certifique-se de não exceder 500 a 600 entradas por dicionário.

Imagem 8. Diretório personalizado para detecção de e-mail forjado



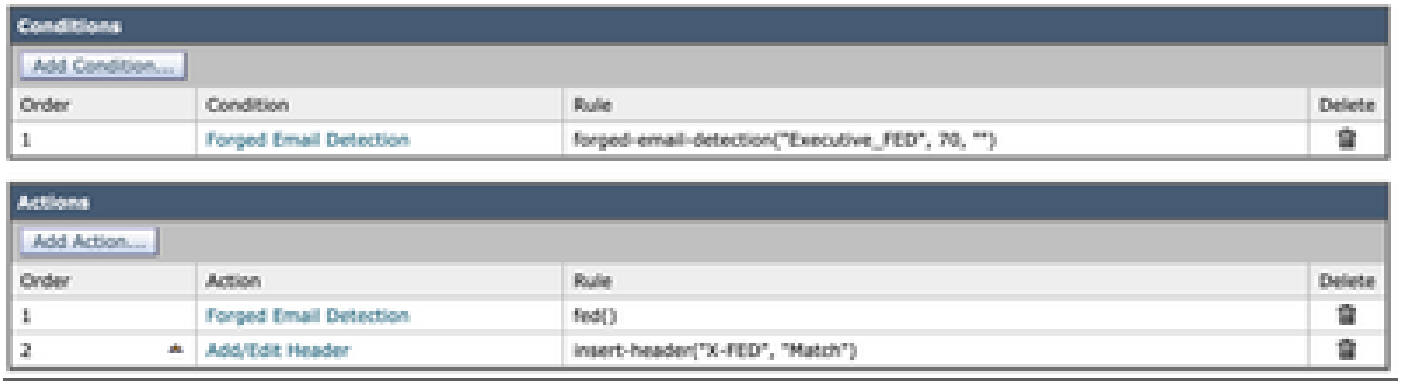
É opcional adicionar uma condição de exceção para seu domínio de e-mail no Envelope Send para ignorar a inspeção de FED. Como alternativa, uma lista de endereços personalizada pode ser criada para ignorar a inspeção de FED para uma lista de endereços de e-mail exibidos no cabeçalho Formulário (Imagem 9).

Imagem 9. Criar uma Lista de Endereços para Ignorar a Inspeção de FED



Aplique a ação de propriedade Forged Email Detection para remover o valor De e revisar o endereço de e-mail real do remetente do envelope na caixa de entrada da mensagem. Em seguida, em vez de aplicar uma ação final, adicione um novo cabeçalho X (por exemplo, X-FED=Match) na mensagem que corresponde à condição e continue a entregar a mensagem à próxima camada de inspeção (Imagem 10).

Imagem 10. Configuração de Filtro de Conteúdo Recomendada para FED

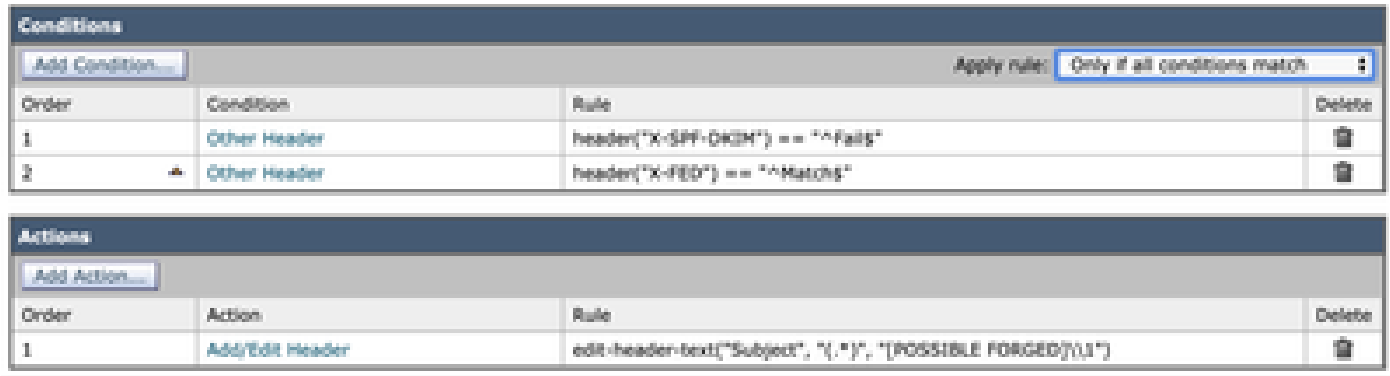


Camada 7: E-mail de falsificação identificado positivamente

Identificar uma campanha de falsificação real é mais eficaz fazendo referência a outros vereditos de vários recursos de segurança no pipeline, como as informações do cabeçalho X produzidas pela aplicação SPF/ DKIM e FE. Por exemplo, os administradores podem criar um filtro de conteúdo para identificar mensagens adicionadas com os dois novos cabeçalhos X devido a resultados com falha na verificação de SPF / DKIM (X-SPF-DKIM=Fail) e qual cabeçalho De corresponde às entradas do dicionário FED (X-FED=Match).

A ação recomendada pode ser colocar a mensagem em quarentena e notificar o destinatário ou continuar a entregar a mensagem original, mas precedendo [POSSIBLE FORGED] palavras na linha de assunto como um aviso para o destinatário, conforme descrito (Imagem 11).

Imagem 11. Combinar todos os cabeçalhos X em uma única regra (final)



Camada 8: Proteção contra URLs de phishing

A proteção contra links de phishing é incorporada ao URL e à filtragem de ataques no Cisco Secure Email. As ameaças combinadas combinam mensagens de falsificação e phishing para parecerem mais legítimas para o destino. A ativação da filtragem de ataques é essencial para ajudar a detectar, analisar e interromper essas ameaças em tempo real. Vale a pena saber que a reputação da URL é avaliada dentro do mecanismo Anti-Spam e pode ser usada como parte da decisão para detecção de spam. Se o mecanismo Anti-Spam não parar a mensagem com o URL como Spam, ela será avaliada pela filtragem de URL e epidemia na última parte do pipeline de segurança.

Recomendação: crie uma regra de filtro de conteúdo que bloqueie uma URL com uma pontuação

de reputação mal-intencionada e redirecione a URL com uma pontuação de reputação neutra para o Cisco Security Proxy (Imagem 12). Habilite os filtros de detecção de ameaças habilitando a modificação de mensagens. A regravação de URL permite que URLs suspeitos sejam analisados pelo Cisco Security Proxy (Imagem 13). Para obter mais informações, visite: Configurar filtragem de URL para gateway de e-mail seguro e gateway de nuvem

Imagem 12. Filtro de conteúdo para reputação de URL

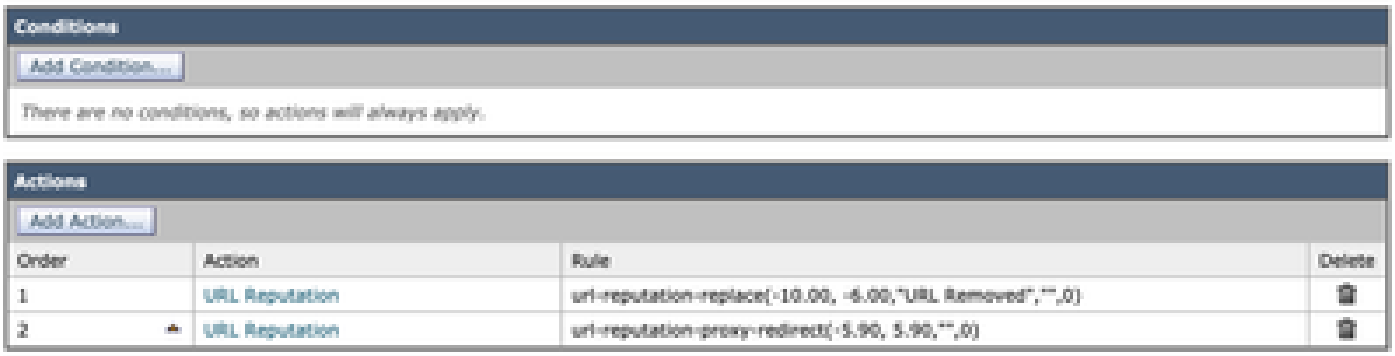
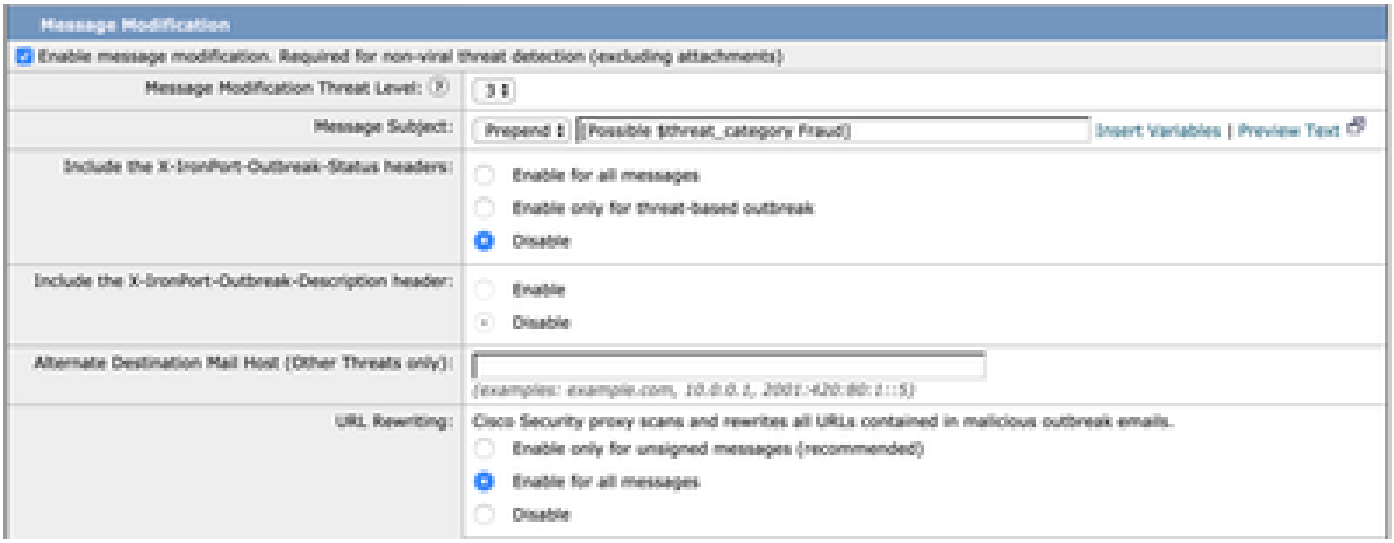


Imagem 13. Habilitar regravação de URL na filtragem de epidemia



Camada 9: Aumente a capacidade de detecção de falsificação com o Cisco Secure Email Threat Defense (ETD)

A Cisco oferece o Email Threat Defense, uma solução nativa de nuvem que aproveita a inteligência de ameaças superior do Cisco Talos. Ele tem uma arquitetura habilitada por API para tempos de resposta mais rápidos, visibilidade completa de e-mail, incluindo e-mails internos, uma exibição de conversação para informações contextuais melhores e ferramentas para correção automática ou manual de ameaças à espreita nas caixas de correio do Microsoft 365. Visite a Folha de dados do Cisco Secure Email Threat Defense para obter mais detalhes.

O Cisco Secure Email Threat Defense combate o phishing usando recursos de autenticação de remetente e detecção de BEC. Ele integra mecanismos de aprendizagem automática e Inteligência Artificial que combinam identidade local e modelagem de relacionamento com análises de comportamento em tempo real para proteger contra ameaças baseadas em engano

de identidade. Ele modela o comportamento confiável de e-mail dentro das organizações e entre indivíduos. Entre outros recursos importantes, o Email Threat Defense oferece estes benefícios:

- Descubra ameaças conhecidas, emergentes e direcionadas com recursos avançados de detecção de ameaças.
- Identifique técnicas mal-intencionadas e obtenha contexto para riscos comerciais específicos.
- Procure rapidamente ameaças perigosas e corrija-as em tempo real.
- Utilize telemetria de ameaças pesquisável para categorizar ameaças e entender quais partes da sua empresa são mais vulneráveis a ataques.

Figura 14. O Cisco Secure Email Threat Defense fornece informações sobre como sua empresa está sendo atingida.

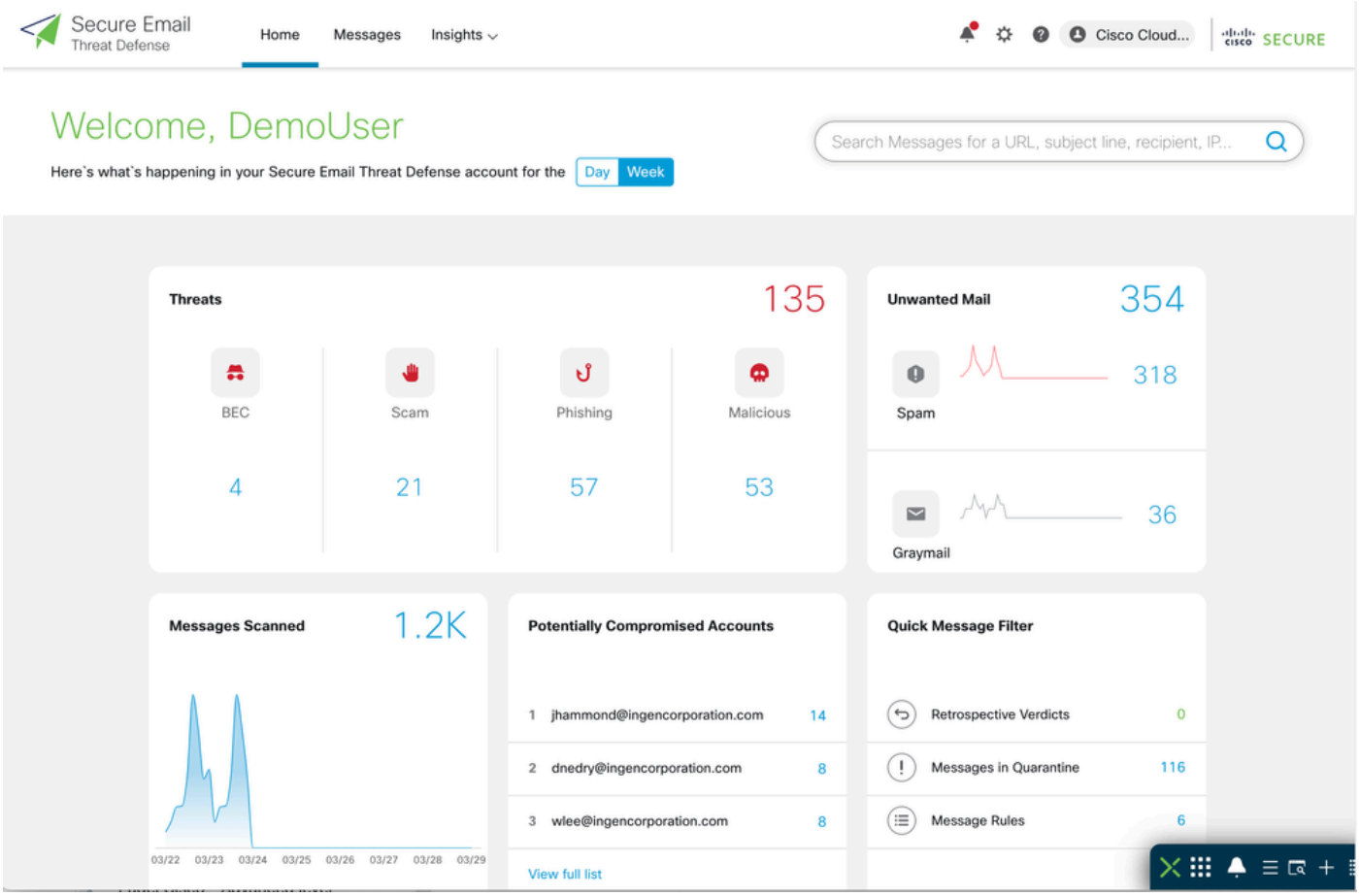
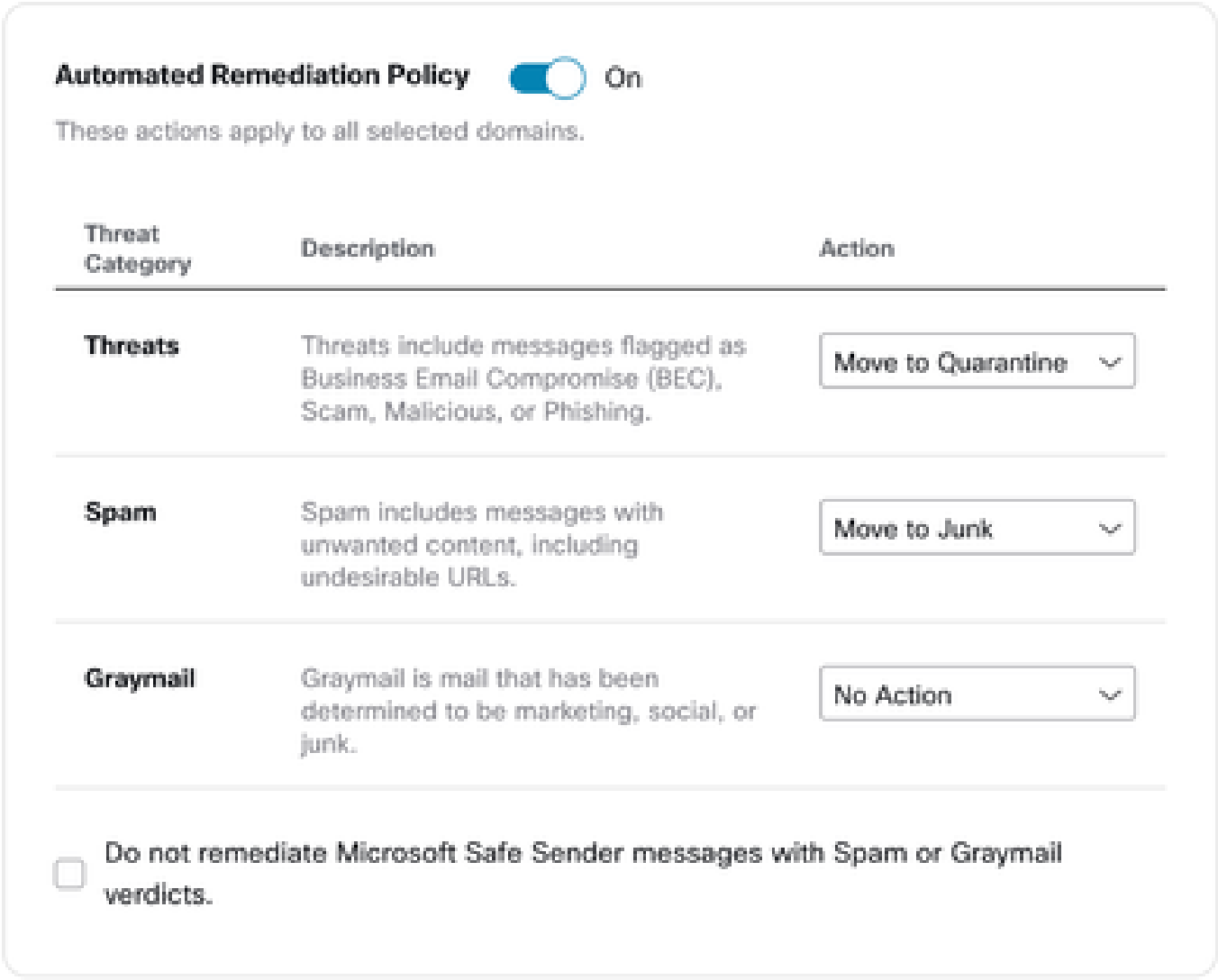


Imagem 15. A configuração da política do Cisco Email Threat Defense determina automaticamente se a mensagem corresponde à categoria de ameaça selecionada



O que mais você pode fazer com a prevenção de falsificação

Muitos spoofs podem ser remediados com algumas precauções simples que incluem, mas não se limitam a:

- Limitar a permissão de domínios listados na Tabela de Acesso de Host (HAT) a um número muito pequeno de parceiros comerciais principais.
- Monitore e atualize continuamente os membros do grupo de remetente SPOOF_ALLOW se você tiver criado um e use as instruções fornecidas no link de práticas recomendadas.
- Ative a detecção de mensagens em cinza e coloque-as na quarentena de spam também.

Mas, o mais importante de tudo, habilite o SPF, o DKIM e o DMARC e os implemente adequadamente. No entanto, a orientação sobre a publicação de registros SPF, DKIM e DMARC está além do escopo deste documento. Para isso, consulte este white paper: Práticas recomendadas de autenticação de e-mail: as maneiras ideais de implantar SPF, DKIM e DMARC.

Entenda o desafio de remediar ataques por e-mail, como as campanhas de falsificação discutidas aqui. Se tiver dúvidas sobre a implementação dessas práticas recomendadas, entre em contato com o Suporte Técnico da Cisco e abra um caso. Como alternativa, entre em contato com sua

equipe de contas da Cisco para obter uma solução e orientações sobre o projeto. Para obter mais informações sobre o Cisco Secure Email, consulte o site do Cisco Secure Email.

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.