

Estabelecer uma política DLP do costume para detectar números da Segurança Sociais formatados e sem formatação

Índice

[Introdução](#)

[Estabelecer uma política DLP do costume para detectar números da Segurança Sociais formatados e sem formatação](#)

[Crie uma política feita sob encomenda](#)

[Crie um classificador](#)

[Ajuste os ajustes da severidade](#)

[Ajuste a escala da severidade](#)

[Submeta e comprometa mudanças](#)

[Passos finais](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como estabelecer uma política DLP do costume para detectar os números da Segurança Sociais formatados e sem formatação (SSN) na ferramenta de segurança do email de Cisco (ESA).

Estabelecer uma política DLP do costume para detectar números da Segurança Sociais formatados e sem formatação

Pelo projeto o motor da exploração DLP detecta somente números da Segurança Sociais formatados. Isto é devido ao nível alto dos falsos positivos causados pelos números 9-digit contidos nos dados usados por várias indústrias. Por exemplo, os números do roteamento ABA do banco são 9-digits e provocariam ao fazer a varredura para um número da Segurança Social sem formatação. Como tal ele é recomendado evitar fazer a varredura para números da Segurança Sociais sem formatação a menos que exigido restritamente por sua organização. Se se exige que sua organização faz a varredura para números da Segurança Sociais sem formatação, você pode criar uma política DLP do costume seguindo as etapas fornecidas na solução abaixo.

AsyncOS fornece a opção para criar a partir do zero sua própria política que usa os classificadores desenvolvidos pelo RSA ou pela sua organização. Esta opção está considerada avançada e deve ser usada somente nos casos raros quando os moldes de política predefinidos não cumprem os requisitos exclusivos de seu ambiente de rede.

Crie uma política feita sob encomenda

1. Na GUI: **Políticas do correio > de política DLP gerente.**
2. Clique o botão da **política DLP adicionar....**
3. Selecione a **política feita sob encomenda** na parte inferior da tela e o clique **adiciona** ao lado da política feita sob encomenda.
4. Dê entrada com um nome da política DLP. Por exemplo: *Política feita sob encomenda SSN.*

Crie um classificador

Criar classificadores feitos sob encomenda dá-lhe a grande flexibilidade sobre os critérios feitos a varredura no motor DLP. Nós usaremos este a nossa vantagem para fazer a varredura para o SSN formatado e SSN sem formatação.

1. Da gota-para baixo de harmonização satisfeita do classificador, seleta **crie um classificador** e clique o **botão Add.**
2. Dê entrada com um nome de harmonização satisfeito do classificador. Por exemplo: *SSN todos os formatos.*
3. Sob a seção das regras, ajuste a gota para baixo das palavras ou das frases à **entidade.**
4. Selecione a entidade: **Número da Segurança Social E.U., formatado.**
5. O clique **adiciona a regra.**
6. Selecione outra vez a **entidade.**
7. Selecione a entidade: **Número da Segurança Social E.U., sem formatação.**
8. Clique em Submit.

Ajuste os ajustes da severidade

Os seguintes ajustes são um bom ponto de início, porém são meramente uma diretriz para lhe ajudar e podem exigir alguns ajustes da calibração ou da configuração alternada baseados em suas necessidades das organizações.

- **Ajustes críticos da severidade**

Ação aplicada às mensagens: **Quarentena**

Enable Encryption (verificado)

Regra de criptografia: **Use sempre a criptografia da mensagem**

Perfil da criptografia (selecione seu perfil configurado da criptografia da gota-para baixo)

Assunto do mensagem codificada: **\$subject**

- **Ajustes da severidade elevada**

Ação aplicada às mensagens: **Entregue**

Enable Encryption (verificado)

Regra de criptografia: **Use sempre a criptografia da mensagem**

Perfil da criptografia (selecione seu perfil configurado da criptografia da gota-para baixo)

Assunto do mensagem codificada: **\$subject**

- **Ajustes médios da severidade**

Ação aplicada às mensagens: *Entregue*

Enable Encryption (verificado)

Regra de criptografia: **Use somente a criptografia da mensagem se o TLS falha**

Perfil da criptografia (selecione seu perfil configurado da criptografia da gota-para baixo)

Assunto do mensagem codificada: **\$subject**

- **Baixos ajustes da severidade**

Ação aplicada às mensagens: **Entregue**

Enable Encryption (desmarcado)

Ajuste a escala da severidade

Além disso, os seguintes ajustes são um bom ponto de início, porém são meramente uma diretriz para lhe ajudar e podem exigir alguns ajustes da calibração ou da configuração alternada baseados em suas necessidades das organizações.

1. À direita do diagrama da escala da severidade, o clique **edita a escala**.
2. Deslize o primeiro punho até **IGNORAM = 0**.
3. Deslize o segundo punho até o **PONTO BAIXO = 1** ao 9.
4. Deslize o terceiro punho até o **MEDIA = o 10** aos 50 pés.
5. Deslize o quarto punho até a **ELEVAÇÃO = 60** a 89.
6. Se você ajustou este corretamente, **CRÍTICO** estará ajustado automaticamente 90 a 100.
7. Clique **feito** quando terminado.

Submeta e comprometa mudanças

Para finalizar a criação desta política, clique o **botão Submit Button**. Clique as **mudanças comprometer** abotoam-se no canto superior direito do GUI. Você será tomado à tela descomprometido das mudanças, clique **compromete mudanças**. Você deve não ver **nenhuma mudança pendente** no canto superior direito do GUI se bem sucedido.

Passos finais

Você precisará agora de permitir a política DLP em uma política que parte do correio sob **políticas do correio de Polícies->Outgoing do correio**. Para testar fora da produção que você pode criar uma política que parte feita sob encomenda com o senhor mesmo designou como um remetente e permitem a política DLP nesta política do teste.

Informações Relacionadas

- [Cisco envia por correio eletrônico a ferramenta de segurança - Guias do utilizador final](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)