ESA FAQ: Como trabalhar com submissão do email de Cisco e portal do seguimento

Índice

Introdução

Este documento descreve a submissão do email de Cisco e seguindo o portal, o uso do portal, e o general obtêm Como instruções começadas em usar o portal.

Que é o uso da submissão do email de Cisco e portal do seguimento?

O gateway de e-mail de Cisco permaneceu o melhor no Spam, no presunto, no mercado, e em mensagens de travamento do graymail com > os falsos positivos da taxa de captura de 99 por cento e dos 0.001 por cento. (Refira o relatório do opus um para mais detalhes). Contudo, para manter a barra alta e para melhorar a eficácia total, Cisco incentiva clientes submeter as mensagens que são classificadas incorretamente ocasionalmente. Para instruções detalhadas, veja como submeter mensagens de Email a Cisco.

Cada submissão do cliente forma uma parte crítica de sistema da inteligência de ameaça de Cisco. Daqui é importante ter submissões com informação completa e no formato direito (RFC 822). Em alguns casos, as submissões perdem a informação crítica devido à maneira que foram submetidas e ninguém conhece essa informação.

Cisco envia por correio eletrónico a submissão e seguir o portal é uma maneira para que os clientes sigam todas as submissões de sua organização e ao mesmo tempo conheçam o estado de cada submissão. O portal é igualmente meios submeter Spam faltados.

A informação lá pode ser usada para umas interações mais adicionais com Cisco

Quem usará Cisco envia por correio eletrónico a submissão e portal do seguimento?

Todo o usuário que tiver o usuário do CCO Cisco - identificação e senha poderá alcançar o portal.

Contudo, o portal é útil para dois tipos dos usuários:

1. **Administradores de uma organização:** Um administrador do gateway de e-mail que fosse interessado conhecer o estado de todas as submissões fez pelos usuários em seus organização/domínios. Poderia haver mais de um administrador para toda a organização e um administrador poderiam controlar domínios múltiplos dentro de uma organização.
2. **Visores das submissões:** Indivíduo (por exemplo, tac Cisco ou representante de cliente) que é autorizado por um administrador ver as submissões da sua organização. Um visor pode ver submissões das organizações múltiplas. Um visor usará tipicamente a informação no portal para investigar mais. Por exemplo, se um cliente quer Cisco verificar a submissão na prioridade, não têm que submeter as mesmas mensagens a Cisco outra vez. Em lugar de, podem compartilhar de sua submissão ID com o tac Cisco e o tac Cisco pode olhar no portal para uns detalhes mais adicionais.

Como pode um administrador obter começado com o portal?

Um administrador do email que controla um grupo de domínios pode obter começado com o portal seguindo estas instruções:

1. Vá ao hub do Cisco Security e clique as submissões do email e o seguimento do link portal. Esta etapa exige-o ter uma conta de Cisco. Se você não tem Cisco explique, você deve registrar-se e então obter começado.
2. Registrar-se como um “administrador” e incorpore-se 16-character um registro válido ID.

   Nota: Se você está usando AsyncOS 10.0 ou mais atrasado, assegure-se de que o mesmo registro original ID esteja incorporado primeiramente em todos seus dispositivos. Do GUI, **registro portal de seguimento da submissão da administração do sistema > do Spam**. O mesmo registro ID é incorporado então no portal.

   Se usando uma liberação antes de AsyncOS 10.0, incorpore um registro aleatório ID no portal e continue. Quando você migra a AsyncOS 10.0 ou acima, certifique-se de que o mesmo registro ID está usado então em todos os dispositivos ao terminar do ESA.

3. Adicionar todos seus domínios controlados no portal. Vai o **domínio novo ao >** Add da **configuração >** do **domínio**. Uma vez que um domínio é adicionado, um email está enviado a *postmaster@your_domain.com* para confirmar que é uma pessoa autêntica que alcança as submissões desse domínio.

   Nota: Esta etapa supõe que o domínio é queixa do RFC 5321 e somente os povos confiados têm o acesso à caixa postal de postmaster@domain.

   Se *postmaster@your_domain.com* não existe por qualquer motivo, ou assegure que está feito disponível e adicionar então o domínio, ou então configurar o comando CLI de utilização do **aliasconfig do** ESA distribuir email a *postmaster@your_domain.com a um* endereço email válido.

4. Finalmente, vá à caixa postal de *postmaster@your_domain.com* e clique sobre o link da confirmação recebido no email.

Uma vez que todas as etapas acima são executadas, toda a submissão fez o cargo que (por algum usuário de sua organização) pode ser visto pelo administrador.

Que pode um administrador fazer no portal?

Um administrador pode:

- Veja o painel de todas as submissões e siga seu estado em uma única placa
- Veja a tabela que alista cada submissão, seu estado e filtre-os baseou no timestamp, na submissão ID, no entregador e nos outros parâmetros.
- Transfira os relatórios
- Adicionar ou remova os domínios cujas as submissões têm que ser controladas
- Controle todos os visores e suas permissões
- Submit faltou Spam com o portal (somente o formato EML é apoiado atualmente.)

Como pode um visor obter começado com o portal?

Um visor pode registrar-se seguindo estas instruções:

1. Vá ao hub do Cisco Security e clique as submissões do email e o seguimento do link portal. Esta etapa exige-o ter uma conta de Cisco. Se você não tem Cisco explique, você deve registrar-se e então obter começado.
2. Registro como o “visor”.
3. Para ver as submissões do Spam de uma organização, você deve enviar um pedido ao administrador dessa organização. Vá à **configuração > enviam o pedido**.
4. Entre em um do seguinte: Endereço email do administrador da organização como entrado no portal.Submissão ID (pelo menos um submissões ID que o visor está tentando procurar detalhes adicionais)

Uma vez que incorporado, um pedido de autorização é enviado ao administrador correspondente. O administrador terá que entrar ao portal usando suas credenciais e para autorizar indo aos **pedidos da configuração > da permissão** e clicando **RESERVE** ou **NEGUE**. O pedido é permitido uma vez ou negado, o visor receberá uma confirmação do email.

Como pode um visor se transformar um administrador ou vice versa?

Se você se registrou como um visor e quer se transformar um administrador (ou vice versa), faça o seguinte:

1. Do canto superior direito, clique sobre o ***seu username*** **> supressão minha conta**.
2. Segundo sua exigência, execute as etapas mencionadas em um dos seguintes assuntos: “Como pode um administrador obter começado com o portal?” ou “como pode um visor obter começado com o portal?”

Que são os estados diferentes vistos no portal e que significam?

Cada submissão automaticamente é processada e avaliada em cima de incorporar o sistema da inteligência de Cisco. Baseado na análise, o sistema ajustará um dos seguintes estados para uma submissão:

Status	Definição
Acionável	As submissões que são feitas no formato direito, contendo todos os encabeçamentos originais do Internet, os encabeçamentos introduzidos pelo gateway de e-mail, corpo da mensagem completo serão consideradas acionáveis. As amostras da submissão determinadas ser acionáveis são combinadas junto com amo acionáveis de outros clientes, de dados de tempo real dos sensores globais, da inteligên humana, da telemetria do dispositivo e das alimentações externos/do sócio dados. Todo o este alimentações no múltiplo automatizado e os sistemas e as Tecnologias de aprendizagem da máquina que estão analisando estes dados 24x7 para criar probabilida novas e ponderação para dez às centenas de milhares de características do email usada índice da detecção do Anti-Spam de IronPort (IPA) que é consumido então por dispositiv segurança do email.
Acionável mas incompleto	As submissões que são feitas como acessórios no formato direito, contendo o corpo da mensagem completo, etc. mas encabeçamentos críticos dos desaparecidos tais como X- encabeçamentos diagnósticos adicionaram pelo ESA. Isto poderia acontecer devido ao c (por exemplo probabilidade) usado para fazer a submissão. NOTA: As versões do Outlook diferentes souberam para remover de vez em quando os encabeçamentos. Os encabeçamentos críticos faltantes podem impedir da análise e limitar o impacto da submissão. Contudo, estas submissões ainda são alimentadas no sistema da inteligência processadas como descrito em “acionável” ao grau possível.
Un-acionável	Se uns ou vários critérios alistados (mas não limitados a) da “atributos e razões mensage para na tabela do estado Un-acionável” abaixo são encontrados, a submissão é Un-acion marcado. Siga por favor as recomendações em como submeter mensagens de Email a Cisco e submeter-se outra vez. As submissões neste estado não serão tomadas para o processamento adicional.

> Nota: As amostras da submissão podem mais tarde mudar de acionável a Un-acionável, ou vice versa enquanto o processamento adicional e/ou a revisão humana ocorrem.

Atributos e razões da mensagem para o estado Un-acionável:

Atributo da mensagem	Un-acionável

Formato da mensagem	A mensagem não é submetida como um acessório codificado MIME do RFC-822. Exemplo: A submissão da mensagem inline-é enviada
Cabeçalhos da mensagem	Uns ou vários encabeçamentos originais do Internet são faltantes ou deformados.
Idade/frescor	A data original da varredura do dispositivo da mensagem é demasiado velha/expirado se utilizada na formação IPA.
Índice do corpo	• São uma notificação, uma auto-resposta ou uma resposta de desafio do salto. A mensagem contém o índice deformado ou NULO do corpo. • Exercícios de formação internos do phishing da empresa. • Mensagem legítima que discute o índice do Spam. Exemplo: Boletins de segurança e notificações.