Solução de problemas do Cisco XDR e Secure Malware Analytics Cloud Integration

Contents

Introdução

Este documento descreve como solucionar problemas do módulo Secure Malware Analytics Cloud com o Cisco XDR.

Contribuição de Javi Martinez, Engenheiro do Cisco TAC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Nuvem de análise de malware segura
- Cisco XDR

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Console do Secure Malware Analytics Cloud (conta de usuário com direitos de administrador)
- Console Cisco XDR (conta de usuário com direitos de administrador)

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.

Informações de Apoio

O Cisco Secure Malware Analytics Cloud é uma plataforma avançada e automatizada de análise de malware e inteligência contra ameaças de malware na qual arquivos suspeitos ou destinos da Web podem ser detonados sem afetar o ambiente do usuário.

Na integração com o Cisco XDR, o Secure Malware Analytics é um módulo de referência e fornece a capacidade de se deslocar para o Secure Malware Analytics Portal para reunir inteligência adicional sobre hashes de arquivo, IPs, domínios e URLs na área de armazenamento de conhecimento Secure Malware Analytics Cloud (SMA Cloud).

Consulte o Guia de integração de nuvem do Secure Malware Analytics mais recente,

- Nuvem NAM.
- EU Cloud.

Troubleshooting

Licença

- Verifique se você tem uma licença SMA adequada para obter acesso ao console Secure Malware Analytics Cloud

Blocos do Módulo

- Verifique se você selecionou os ***blocos*** apropriados para Secure Malware Analytics Cloud Module
  Navegue até o portal Cisco XDR > Painel > botão Personalizar > Selecione o módulo de nuvem do SMA > Adicionar os blocos apropriados

Função de administrador

- Verifique se você tem uma conta Secure Malware Analytics com função de Administrador no portal Secure Malware Analytics
  Navegue até o portal Cisco XDR > Administração > Sua conta

- Verifique se você tem uma conta SecureX com direitos de Administrador no portal SecureX
  Navegue até o portal Análise de malware > Minha conta de Análise de malware

Observação: se você não tiver a função de administrador no console Secure Malware Analytics e no console Cisco XDR, o administrador poderá alterar a função da conta diretamente no portal em questão

Cronograma

- Verifique se Timestamp está definido corretamente no portal Cisco XDR.
  Navegue até o portal Cisco XDR > Painel > opção Cronograma > Selecione o cronograma apropriado na base da atividade do SMA

Recriar módulo

- Exclua o módulo SMA antigo e crie um novo.
  Navegue até Secure Malware Analytics Cloud console > Minha conta Malware Analytics > Chave de API > Copiar a chave de API
  Navegue até o portal Cisco XDR > Módulos de integração > Selecione o módulo de nuvem do SMA > Adicione a chave de API e a URL (selecione a nuvem do SMA) > Crie o painel

Nota: Somente usuários com a função Administrador da empresa ou Usuários podem obter a chave de API que ativa o módulo de integração Secure Malware Analytics no Cisco XDR.

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.