A Política de Correlação do FMC Permite que os Eventos de Lista exijam que a Política de Descoberta de Rede seja Habilitada

Contents

Problema

Ao configurar políticas de correlação com listas de permissão no Cisco Secure Firewall Management Center (FMC), é importante observar que Permitir Eventos de Lista e Permitir Violações de Lista não são gerados a menos que a Política de Descoberta de Rede esteja configurada para o IP da Rede de Destino. Sem essa configuração, nenhum evento aparece em Analysis > Correlation > Allow List Events e Analysis > Correlation > Allow List Violations.

Durante os testes laboratoriais, estes comportamentos foram observados:

- Os eventos de correlação são gerados corretamente para a rede de destino configurada.
- Nenhum evento de lista de permissões ou violações de lista de permissões são gerados quando o host da rede de destino se torna não compatível.

Ambiente

- Cisco Firepower Threat Defense (FTD) gerenciada pelo Secure Firewall Management Center (FMC)
- Política de correlação configurada com a lista de permissões direcionada a endereços IP específicos
- Lista de permissões configurada para permitir uma aplicação Web, aplicação ou protocolo específico

Resolução

Após extensos testes de laboratório e consultas com a equipe de desenvolvimento, foi confirmado que a política de Descoberta de Rede deve ser habilitada como pré-requisito para que Permitir Eventos de Lista e Permitir Violações de Lista sejam gerados.

A resolução envolve estas etapas:

Passo 1: Habilitar Política de Descoberta de Rede

Navegue para Policies > Network Discovery na interface do FMC e crie uma regra se não houver nenhuma.

Passo 2: Configurar Regra de Descoberta de Rede

Defina a regra de descoberta de rede com as configurações de rede de origem apropriadas:

- Especifique a rede de origem como seu intervalo de rede interna.
- Como alternativa, use todas as redes (0.0.0.0/0) se estiver monitorando todas as fontes de tráfego.
- Certifique-se de que a regra cobre as redes a partir das quais você espera gerar Eventos da Lista de Permissões.

Passo 3: Ativar Regras de Política de Correlação

Verifique se as regras da política de correlação estão ativas e não em um estado desabilitado.

Passo 4: Verificar Geração de Evento de Lista de Permissões

Depois de habilitar a descoberta de rede e ativar as regras de política de correlação:

1.- Acesse sites da Rede de Destino configurada usando um navegador (tornando o host não compatível).

2.- Monitorar Análise > Correlação > Permitir Eventos de Lista e Análise > Correlação > Permitir Violações de Lista para geração de eventos.

3.- Verificar se os eventos estão preenchidos quando o host não está em conformidade.

Os testes de laboratório confirmaram que, uma vez que a Descoberta de Rede esteja habilitada, Permitir Eventos de Lista e as Permitir Violações de Lista são gerados com êxito para um host não compatível.

Causa

A causa raiz é que a Política de Descoberta de Rede é um pré-requisito obrigatório para gerar Eventos de Lista de Permissões em Políticas de Correlação do FMC. Sem uma Política de Descoberta de Rede ativa, o sistema não pode avaliar corretamente a conformidade do host em relação à Lista de Permissões configurada, resultando na geração de Eventos de Lista de Permissões quando o host da Rede de Destino se torna não compatível.

Conteúdo relacionado

- Documentação das listas de conformidade de correlação do Cisco FMC
- Suporte técnico e downloads da Cisco

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.