Revise ou conteste os falsos positivos do IPS com o Umbrella

Contents

Introdução

Este documento descreve como revisar ou contestar falsos positivos do IPS (Serviço de prevenção contra intrusão) com o Cisco Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

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.

Overview

O Sistema de prevenção de intrusão do Cisco Umbrella detecta (e opcionalmente bloqueia) pacotes que são considerados associados a uma ameaça conhecida, vulnerabilidade, mas

também simplesmente quando o formato do pacote é incomum.

Os administradores escolhem qual lista de assinaturas IPS é usada para detectar ameaças com base nessas listas padrão:

- Conectividade sobre segurança
- Segurança e conectividade equilibradas
- Segurança sobre conectividade
- Detecção máxima

É importante lembrar que a lista de assinaturas escolhida pode ter um grande impacto no número de falsos positivos de IPS encontrados. Espera-se que os modos mais seguros (como Detecção máxima e Segurança sobre conectividade) criem detecções de IPS indesejadas, pois enfatizam a segurança. Os modos mais seguros são recomendados somente quando a segurança total é necessária, e o administrador deve antecipar a necessidade de monitorar e revisar um grande número de eventos de IPS.

Para obter mais informações sobre os diferentes modos, consulte a Documentação do IPS.

Revisar detecções de IPS

Use a pesquisa de atividades no painel Umbrella para exibir eventos de IPS. Para cada evento, há duas informações importantes:

- ID/Categoria/Nome da assinatura IPS. Pesquisável em https://snort.org
- Número CVE (se aplicável). Pesquisável em https://www.cve.org/

Nem todas as detecções de IPS indicam uma exploração/ataque conhecido. Muitas das assinaturas (particularmente no modo Max Detection) simplesmente indicam a presença de um determinado tipo de tráfego ou uma violação de protocolo. É importante revisar as fontes de informações mencionadas anteriormente junto com outros detalhes sobre o evento (como origem/destino) para determinar se o evento requer investigação adicional da equipe de segurança.

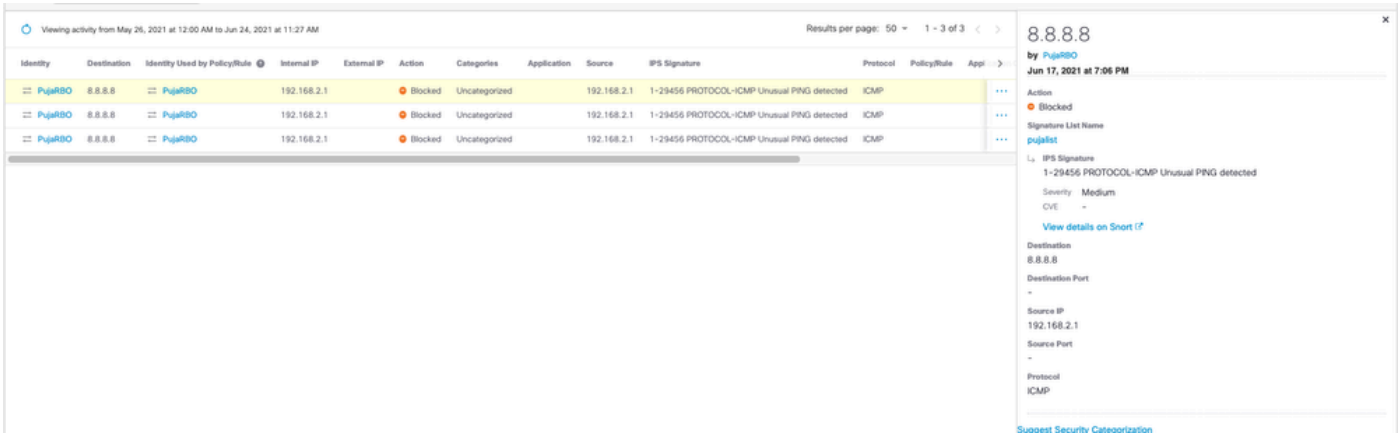
A categoria de assinatura pode ser útil para fornecer contexto adicional sobre o tipo de detecção de IPS. Revise as categorias disponíveis em snort.org.

Violações de protocolo

Neste exemplo, um evento de IPS é vinculado a esta assinatura:
https://www.snort.org/rule_docs/1-29456

A descrição da assinatura é:

"A regra procura o tráfego PING que entra na rede e que não segue o formato normal de um PING."



4403885889428

Nesse caso, a regra Snort não está necessariamente detectando nenhuma exploração em particular, mas sim um pacote ICMP malformado que foi bloqueado. Com base nas informações disponíveis em snort.org e em outros detalhes sobre o evento (como origem/destino), o administrador pode decidir que esse evento não requer investigação adicional

Compatibilidade de aplicativos

Alguns aplicativos legítimos não são compatíveis com assinaturas de IPS, especialmente quando os modos mais agressivos (Detecção máxima) são configurados. Nesses cenários, o aplicativo pode ser bloqueado pelos motivos discutidos na seção Violação de protocolo. O aplicativo pode usar um protocolo de forma inesperada ou usar um protocolo personalizado sobre uma porta que normalmente é reservada para outro tráfego.

Embora o aplicativo seja legítimo, essas detecções são geralmente válidas e nem sempre podem ser corrigidas pela Cisco.

Se um aplicativo legítimo for bloqueado pelo IPS, a Umbrella recomenda entrar em contato com o fornecedor do aplicativo com detalhes do evento/assinatura. Os aplicativos de terceiros devem ser testados quanto à compatibilidade com as assinaturas de IPS em snort.org.

No momento, não é possível excluir um Aplicativo/Destino individual da verificação de IPS.

Desabilitando assinaturas de IPS

Se uma assinatura for encontrada para causar problemas de compatibilidade com um aplicativo de terceiros, a assinatura poderá ser desabilitada (temporariamente ou permanentemente). Isso só deve ser feito quando você confiar no aplicativo e tiver determinado que o valor do aplicativo supera os benefícios de segurança da assinatura específica.

Conclua as etapas na documentação Adicionar uma lista de assinaturas personalizada para obter informações sobre como criar uma lista de assinaturas personalizada. Você pode usar suas configurações atuais como um modelo e, em seguida, desativar as regras desejadas definindo-as como Log Only ou Ignore.

Support

Eventos históricos

O suporte Umbrella não pode fornecer detalhes adicionais sobre eventos IPS históricos. Os eventos IPS informam que o tráfego não correspondeu à assinatura IPS. Os detalhes da assinatura estão disponíveis publicamente em snort.org. O Umbrella não armazena uma cópia de tráfego/pacotes brutos e, portanto, não pode fornecer contexto adicional ou confirmação sobre a natureza de um evento de IPS.

Problemas de IPS/falsos positivos

Se você quiser contestar um problema atual de IPS (como um falso positivo), entre em contato com o suporte Umbrella.

Para investigar esses problemas, uma captura de pacote é necessária pelo Umbrella Support. O conteúdo bruto dos pacotes é necessário para determinar como o tráfego disparou a detecção de IPS. Você deve ser capaz de replicar o problema para gerar a captura de pacotes.

Antes de criar um ticket, use uma ferramenta como o Wireshark para gerar a captura de pacotes ao replicar o problema. As instruções estão disponíveis em nossa base de conhecimento.

Como alternativa, o Umbrella Support pode ajudar a gerar a captura de pacotes. Eles precisam agendar um horário em que o problema com o usuário ou aplicativo afetado possa ser recriado.

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.