Revisar o cuestionar los falsos positivos de IPS con Umbrella

Contenido

Introducción

Este documento describe cómo revisar o cuestionar los falsos positivos del Servicio de prevención de intrusiones (IPS) con Cisco Umbrella.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

El sistema de prevención de intrusiones de Cisco Umbrella detecta (y opcionalmente bloquea) paquetes que se consideran asociados a una amenaza o vulnerabilidad conocida, pero también

simplemente cuando el formato del paquete es inusual.

Los administradores eligen la lista de firmas IPS que se utiliza para detectar amenazas en función de estas listas predeterminadas:

- Conectividad sobre seguridad
- Seguridad y conectividad equilibradas
- Seguridad sobre conectividad
- Detección máxima

Es importante recordar que la lista de firmas elegida puede influir en gran medida en el número de falsos positivos IPS encontrados. Se espera que los modos más seguros (como la detección máxima y la seguridad sobre la conectividad) creen detecciones de IPS no deseadas, ya que hacen hincapié en la seguridad. Los modos más seguros sólo se recomiendan cuando se requiere total seguridad, y el administrador debe anticiparse a la necesidad de supervisar y revisar un gran número de eventos IPS.

Para obtener más información sobre los diferentes modos, consulte la documentación de IPS.

Revisar detecciones de IPS

Utilice la búsqueda de actividad del panel de Umbrella para ver los eventos IPS. Para cada evento hay dos elementos de información importantes:

- ID de firma/categoría/nombre de IPS. Se pueden realizar búsquedas en https://snort.org
- Número CVE (si procede). Se pueden realizar búsquedas en https://www.cve.org/

No todas las detecciones de IPS indican un ataque/vulnerabilidad conocido. Muchas de las firmas (especialmente en el modo de detección máxima) simplemente indican la presencia de un cierto tipo de tráfico o una violación de protocolo. Es importante revisar las fuentes de información mencionadas anteriormente junto con otros detalles sobre el evento (como el origen/destino) para determinar si el evento requiere una investigación adicional por parte de su equipo de seguridad.

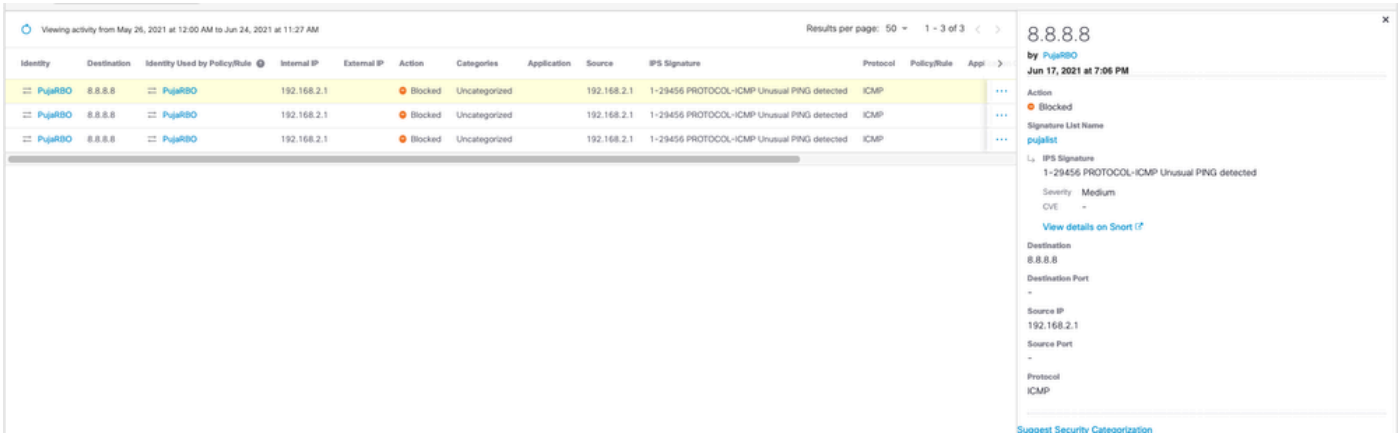
La categoría de firma puede ser útil para proporcionar contexto adicional sobre el tipo de detección IPS. Revise las categorías disponibles en snort.org.

Infracciones de protocolo

En este ejemplo, un evento IPS está vinculado a esta firma : https://www.snort.org/rule_docs/1-29456

La descripción de la firma es:

"La regla busca tráfico PING entrante en la red que no siga el formato normal de un PING".



4403885889428

En este caso, la regla Snort no necesariamente detecta ninguna vulnerabilidad en particular, sino que detecta un paquete ICMP mal formado que fue bloqueado. Según la información disponible en snort.org y otros detalles sobre el evento (como el origen o el destino), el administrador puede decidir que este evento no requiere más investigación

Compatibilidad de aplicaciones

Algunas aplicaciones legítimas no son compatibles con las firmas IPS, especialmente cuando se configuran los modos más agresivos (Detección máxima). En estos escenarios, la aplicación se puede bloquear por los motivos descritos en la sección Violación de protocolo. La aplicación puede utilizar un protocolo de forma inesperada o un protocolo personalizado en un puerto que normalmente está reservado para otro tráfico.

Aunque la aplicación es legítima, estas detecciones suelen ser válidas y Cisco no siempre puede corregirlas.

Si IPS bloquea una aplicación legítima, Umbrella recomienda ponerse en contacto con el proveedor de la aplicación para obtener información sobre el evento o la firma. Se debe comprobar la compatibilidad de las aplicaciones de terceros con las firmas IPS en snort.org.

Actualmente no es posible excluir una aplicación/destino individual del análisis de IPS.

Desactivación de firmas IPS

Si se descubre que una firma causa problemas de compatibilidad con una aplicación de terceros, la firma se puede deshabilitar (temporal o permanentemente). Esto sólo se debe hacer cuando se confía en la aplicación y se ha determinado que el valor de la aplicación es mayor que las ventajas de seguridad de la firma específica.

Complete los pasos de la documentación Agregar una lista de firmas personalizada para obtener información sobre cómo crear una lista de firmas personalizada. Puede utilizar la configuración actual como plantilla y, a continuación, deshabilitar las reglas deseadas configurándolas en Sólo registro o Omitir.

Support

Eventos históricos

Umbrella Support no puede proporcionar detalles adicionales sobre los eventos IPS históricos. Los eventos IPS le informan de que el tráfico no coincide con la firma IPS. Los detalles de la firma están a disposición del público en snort.org. Umbrella no almacena una copia del tráfico/paquetes sin procesar y, por lo tanto, no puede proporcionar más contexto o confirmación sobre la naturaleza de un evento IPS.

Problemas de IPS/falsos positivos

Si desea impugnar un problema de IPS actual (como un falso positivo), póngase en contacto con el servicio de asistencia técnica de Umbrella.

Para investigar estos problemas, Umbrella Support requiere una captura de paquetes. El contenido sin procesar de los paquetes es necesario para determinar cómo el tráfico activó la detección IPS. Debe poder replicar el problema para generar la captura de paquetes.

Antes de generar un ticket, utilice una herramienta como Wireshark para generar la captura de paquetes al replicar el problema. Las instrucciones están disponibles en nuestra base de conocimientos.

Alternativamente, Umbrella Support puede ayudar a generar la captura de paquetes. Deben programar una hora en la que se pueda volver a crear el problema con el usuario o la aplicación afectados.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).