¿Cuáles son las métricas utilizadas para determinar el conjunto de reglas predeterminado para cada política de base de intrusiones de Firepower?

Contenido

Introducción
Talos Base Policy Intent definido en los metadatos de regla
Métricas Utilizadas para Determinar el Conjunto de Reglas Predeterminado
Conectividad sobre la política de base de seguridad
Política de base equilibrada
Política de seguridad sobre la base de conectividad
Política básica de detección máxima (detección máxima):
Frecuencia de las actualizaciones de políticas

Introducción

Cisco Talos lanza actualizaciones de reglas de Snort (SRU) para hacer frente a las últimas amenazas y vulnerabilidades. Una nueva versión de SRU puede contener conjuntos de reglas actualizados para cada política base. Este documento explica el proceso utilizado por Talos para decidir cómo se asignan las reglas a cada política de base de intrusiones para los dispositivos Firepower.

Talos Base Policy Intent definido en los metadatos de regla

Las políticas básicas son mantenidas por metadatos dentro de las propias SRU. El estado de cualquier regla determinada en cualquiera de las políticas predeterminadas se define en la parte de metadatos del cuerpo de reglas. Por ejemplo:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC 1.php outbound connection
attempt"; sid:38753; gid:3; rev:1; classtype:trojan-activity; metadata:engine shared, soid
3|38753, policy balanced-ips drop, policy security-ips drop, impact_flag red; )
```

Observe que en la regla de ejemplo que se muestra arriba, la sección de metadatos contiene descarte de ips de equilibrio de políticas, descarte de ips de seguridad de políticas. **Esto indica que esta regla 1:38753 está habilitada y configurada para caer en la *política de seguridad equilibrada y conectividad* así como la *política de seguridad sobre conectividad*.**

Métricas Utilizadas para Determinar el Conjunto de Reglas Predeterminado

- La métrica principal utilizada es la puntuación del sistema de puntuación de vulnerabilidades

comunes (CVSS) asignada a cada vulnerabilidad que podría estar cubierta por una regla.
- La segunda métrica se basa en el tiempo y se refiere a la edad de una vulnerabilidad particular.
- La métrica final es el área particular de cobertura para la regla. Por ejemplo, las reglas de inyección de SQL se consideran lo suficientemente importantes como para influir en la inclusión de políticas.

Nota: Las vulnerabilidades cubiertas por las reglas en estas categorías se consideran importantes, independientemente de la edad.

Conectividad sobre la política de base de seguridad

Nota: La política de **conectividad** está diseñada específicamente para favorecer el rendimiento del dispositivo por encima de los controles de seguridad de la política. Debería permitir a un cliente implementar uno de nuestros dispositivos con un número mínimo de falsos positivos y un rendimiento total de la caja en la mayoría de las implementaciones de red. Además, esta política debería detectar las amenazas más comunes y prevalentes que experimentarán nuestros clientes.

1. La puntuación de CVSS debe ser 10

2. La vulnerabilidad es de los últimos dos años (inclusive). Por ejemplo:

- Año actual (por ejemplo, 2019)
- El año pasado (2018 en este ejemplo)
- Año anterior al último (2017 en este ejemplo)

3. Categoría de regla

- No se utiliza para esta política

Política de base equilibrada

Nota: La política **Equilibrada** es la política predeterminada que se recomienda para las implementaciones iniciales. Esta política intenta equilibrar las necesidades de seguridad y las características de rendimiento de nuestros sistemas. Los clientes deben ser capaces de empezar con esta política y obtener una tasa de bloqueos muy buena con herramientas de evaluación públicas, y una tasa de rendimiento relativamente alta con herramientas de evaluación y prueba. Además, esta política debe funcionar al 80% de la capacidad nominal del dispositivo en condiciones normales en las redes silvestres. Lo principal que siempre hay que tener en cuenta con la política Equilibrada es que este es el punto de partida de los clientes, si tienen una mala experiencia con falsos positivos, detección limitada o bajo rendimiento, la mayoría de los clientes investigarán otros dispositivos para su implementación en su infraestructura. Es el estado de envío predeterminado del conjunto de reglas de suscriptor de Snort para Snort de código abierto vendido en Snort.org.

1. Puntuación 9 o superior de CVSS

2. La vulnerabilidad es de los últimos dos años (inclusive). Por ejemplo:

- Año actual (por ejemplo, 2019)
- El año pasado (2018 en este ejemplo)
- Año anterior al último (2017 en este ejemplo)

3. Categoría de regla

- Malware-CnC
- Lista negra
- Inyección SQL
- Kit de aprovechamiento de vulnerabilidades

4. Si la regla está en la política **de conectividad**

Política de seguridad sobre la base de conectividad

> **Nota:** La política de **seguridad** está diseñada para el pequeño segmento de nuestra base de clientes que se preocupa excepcionalmente por la seguridad organizativa. Los clientes implementan esta política en redes protegidas, que tienen unos requisitos de ancho de banda más bajos, pero requisitos de seguridad mucho mayores. Además, a los clientes les preocupan menos los falsos positivos y las firmas ruidosas. El control de aplicaciones y el uso bloqueado de la red también son motivo de preocupación para los clientes que implementan esta política. Debe proporcionar la máxima protección y control de aplicaciones, pero no debe hacer caer la red.

1. Puntuación 8 o superior de CVSS

2. La vulnerabilidad es de los últimos tres años (inclusive). Por ejemplo:

- Año actual (por ejemplo, 2019)
- El año pasado (2018 en este ejemplo)
- Año anterior al último (2017 en este ejemplo)
- Año anterior (2016 en este ejemplo)

3. Categoría de regla

- Malware-CnC
- Lista negra
- Inyección SQL
- Kit de aprovechamiento de vulnerabilidades

4. Si la regla está en la política **Equilibrada** y **Conectividad**

Política básica de detección máxima (detección máxima):

> **Nota:** La regla **Maximum Detection** está diseñada para ser utilizada en entornos de prueba y, como tal, no está optimizada para el rendimiento. Se toleran y/o esperan falsos positivos para muchas de las normas de esta política y normalmente no se emprenderán investigaciones en el marco del programa.

1. La cobertura es necesaria para las pruebas in situ.

2. Incluye reglas en los conjuntos de reglas **Seguridad**, **Equilibrado** y **Conectividad**.

3. Incluye todas las reglas activas sobre Sid: 10000, a menos que se especifique lo contrario.

Frecuencia de las actualizaciones de políticas

Todas las nuevas reglas se colocan en las políticas basadas en estos criterios. **Todos los años** las políticas se volverán a evaluar y las normas de años anteriores, a medida que la edad de las vulnerabilidades, se eliminarán de la política para mantener la política en conformidad con nuestros criterios de selección temporal.

Si la puntuación de CVSS cambia por una vulnerabilidad específica que está cubierta por una regla, se vuelve a evaluar su presencia en una política basada en la métrica de CVSS.

Las políticas crecen continuamente. Aparte de los principales reequilibrados para alinearlos con un objetivo específico, no siempre se producen grandes caídas de las normas de las políticas si estamos satisfechos con el número de reglas y el rendimiento de la política sobre el producto

> **Nota:** Las políticas básicas pueden distanciarse del importante reequilibrio anual para alinearlas con un objetivo específico. Las principales pérdidas de reglas de las políticas no siempre ocurren si Talos está satisfecho con el número de reglas y el rendimiento de la política en el producto en condiciones de red normales. Las reglas de las políticas enumeradas se evalúan por regla. Habrá algunas reglas que son más antiguas y que no están en los criterios anteriores que se incluirán en las políticas predeterminadas. Lo anterior es el criterio de selección de las reglas predeterminadas y siempre está sujeto a cambios según el panorama de amenazas.

> **Nota**: Las reglas de las políticas enumeradas se evalúan por regla. Habrá algunas reglas que son más antiguas y que no están en los criterios anteriores que se incluirán en las políticas predeterminadas. Lo anterior es el criterio de selección de las reglas predeterminadas y siempre está sujeto a cambios según el panorama de amenazas