¡LAS OPERACIONES DE MI CORTAFUEGOS HAN COBRADO VIDA!

THE OPERATIONS OF MY FIREWALL HAVE COME TO LIFE!

Autor:
Jesús Díaz Barrero. Palo Alto Networks. jdiaz@paloaltonetworks.com

Resumen:
En este artículo se reflexiona sobre la importancia de introducir Inteligencia Artificial (IA) para automatizar las operaciones de seguridad (SecOps).

Abstract:
This article reflects on the importance of introducing AI as a key factor for the automation of the security operations (SecOps)

Palabras clave:
Ciberseguridad; Seguridad de la información; Inteligencia Artificial
Keywords:
Cibersecurity; Information Security; AIOps

¿Cuántas veces hemos escuchado que una doble barrera de cortafuegos de fabricantes diferentes ofrecería un nivel de protección superior? Si uno de los sistemas de seguridad del perímetro se ve comprometido tendré un segundo, de otro proveedor, que seguramente no será susceptible a la supuesta vulnerabilidad que afecta al primero y estaré protegido.

Sin ánimo de cuestionar ni mucho menos ese diseño de seguridad ─con el que he de reconocer no estoy de acuerdo en cualquier caso, aunque eso es harina de otro costal─, me gustaría plantear dos cuestiones:

Primera cuestión: ¿Pasa todo el tráfico que consideras relevante y crítico para tu organización por ambos sistemas de cortafuegos? Si sólo lo hace por uno, ¿dónde está el valor de la doble barrera? Y si lo hace por los dos, pero solamente haces

inspección de nivel 4 y no de nivel 7 (es decir, si no analizas aplicación y contenido), ¿qué aporta la inspección dual, además de introducir latencia?

Segunda cuestión y más importante para el objetivo de este artículo: ¿has cuantificado el coste en capital humano asociado al aprendizaje y mantenimiento de dos sistemas de seguridad diferentes, cada uno con su particularidad en la disponibilidad (¡en HA por supuesto!) ¿y de gestión? ¿Y el coste humano de operarlos? ¿Y la posibilidad de introducir un error humano al administrar dos sistemas?

Abundando en el problema asociado a la complejidad de la gestión de los cortafuegos de nueva generación, Gartner ya predijo el año pasado que en el 2023 los errores humanos de configuración provocarían el 99% de las brechas de seguridad en los firewalls.

Por ese motivo, pensamos que es fundamental revolucionar el mercado de la operación y, de manera similar a lo que se está proponiendo en otros ámbitos de la operación de ciberseguridad, como en los SOC autónomos capaces de gestionar por completo y de manera automatizada la mayoría de las alertas, sistematizar las tareas más repetitivas asociadas a la gestión de los *firewalls*, a través del uso de la Inteligencia Artificial. Para ello, se introduce el término de “Operaciones basadas en Inteligencia Artificial”, que es un término acuñado por Gartner, y que define que un sistema AIOps es capaz de analizar la telemetría y los flujos de eventos para transformar los datos en patrones significativos y permitir respuestas proactivas que reduzcan el trabajo y los gastos generales.

Como objetivos fundamentales de estos sistemas de operación estarían la mejora de las operaciones de los *Firewalls* de Nueva Generación (NGFW), para evitar configuraciones incorrectas, y la resolución de problemas potenciales de manera proactiva, antes de que ocurran incidentes reales de seguridad.

Profundizando en los aspectos técnicos, un sistema de gestión AIOps es un módulo de análisis que normalmente va a estar disponible como servicio en la nube, para garantizar que sea ágil y fácilmente escalable. Para ello, y en primer lugar, el sistema recopila los datos y la telemetría sobre los dispositivos de seguridad disponibles: HW, SW o plataforma de gestión. Los datos recogidos se analizan en la nube AIOps, donde

se ejecutan los algoritmos de aprendizaje automático, para realizar el análisis inicial. Una vez que los datos han sido analizados, se proponen mejoras/cambios de configuración que se ofrecen a los administradores.

De manera general, un módulo de gestión basado en AIOps ofrece:

- **Detección de anomalías:** basada en *Machine Learning*. Puede predecir problemas no solamente asociados al uso de las políticas de seguridad implantadas, sino también dentro de la propia plataforma (por ejemplo fallos hardware).

- **Buenas prácticas**: recomendaciones para mejorar las configuraciones, además de adecuarlas al cumplimiento específico de normativas. Por ejemplo, la implementación de perfiles de protección *malware* o prevención de ataques que abusan del DNS.

- **Simplificación en la apertura de tickets de soporte:** integración de información analítica y automatizada en los ficheros que se adjuntan para resolver los incidentes de soporte más rápidamente.

- **Análisis proactivo de la postura de seguridad:** predicción de problemas potenciales asociados por ejemplo a configuraciones erróneas, o pérdida de rendimiento. Aviso del fin de vida de las versiones SW implantadas para su actualización.

- **Informes sobre la eficacia de las políticas implementadas:** visibilidad y análisis del estado de salud de las plataformas estudiadas.

- **Reducción del error asociado al factor humano:** por ejemplo, detección de políticas erróneas o eliminación de duplicados.

El mundo de las operaciones de seguridad basadas en la Inteligencia Artificial ha dejado de ser ciencia ficción y se trata ya de una realidad. Permite maximizar la inversión y optimizar los recursos humanos de los que operan las plataformas, para que inviertan su tiempo en las tareas en las que aportan más valor, como el establecimiento de nuevos procedimientos o políticas más eficaces.

Operar un parque de sistemas de seguridad sin herramientas que automaticen estas tareas y detecten anomalías va a resultar cada vez más complejo y costoso. Como decía Terminator, también basado en IA: "*Sayonara, baby*"