Un nuevo nivel de seguridad para las aplicaciones web y las API

Las aplicaciones nativas en la nube no dejan de crecer y se están empaquetando con contenedores, funciones sin servidor y microservicios en diversas soluciones tecnológicas. Lejos de estabilizarse con el tiempo, estas arquitecturas complejas se volverán cada vez más prevalentes. La protección de las aplicaciones web y las API en que se sustentan estas arquitecturas siempre ha sido un reto para los equipos de DevOps y para quienes se ocupan de la seguridad de las aplicaciones. Las aplicaciones web y las API cambian constantemente, y las soluciones de seguridad web existentes carecen de la cobertura necesaria.

Para responder a esta necesidad, Palo Alto Networks ofrece una solución insuperable de seguridad para API y aplicaciones web (WAAS, por sus siglas en inglés) como parte de la plataforma Prisma Cloud. En este informe, ofrecemos un análisis cuantitativo del módulo y lo comparamos con otras soluciones del sector. Y al hacerlo, demostramos la superioridad de la exactitud de la solución WAAS de Prisma Cloud.

Medición 101: exactitud de la solución de ciberseguridad

El requisito más básico para una solución de seguridad para API y aplicaciones web es que bloquee los ataques basados en la web, como la inyección de SQL, las secuencias de comandos entre sitios y la inclusión de archivos locales. Sin embargo, las soluciones de ciberseguridad nunca deberían evaluarse únicamente por su capacidad de bloquear los ataques. Si lo hiciéramos, la mejor solución de ciberseguridad probablemente sería un cable Ethernet desconectado de todo. Por desgracia, la otra cara de este enfoque tan drástico probablemente sería una pérdida considerable de tráfico legítimo.

Las mejores pruebas comparativas, a la hora de evaluar la competencia de una solución, tienen en cuenta varios factores de exactitud de clasificación binaria estándar relacionados con la ciberseguridad. En este informe, consideramos:

- **Falsos positivos (FP)**: actividad legítima señalada erróneamente como maliciosa
- **Falsos negativos (FN)**: actividad maliciosa no detectada
- **Positivos reales (PR)**: actividad maliciosa correctamente detectada como maliciosa
- **Negativos reales (NR)**: actividad legitima correctamente detectada como legítima

Todo análisis que trate de evaluar y comparar la eficacia de las soluciones de ciberseguridad debe tener en cuenta los cuatro factores para permitir a los usuarios y compradores elegir la solución más adecuada según su caso de uso. Al fin y al cabo, no todos los casos son iguales; el equilibrio ideal entre la continuidad empresarial y los niveles de protección puede variar.

Estos cuatro factores se pueden medir con dos conceptos estadísticos denominados precisión y exhaustividad:

- La **precisión** es la fracción (o porcentaje) de peticiones señaladas que resultaron ser realmente maliciosas. Dicho de otro modo, la precisión se refiere a hasta qué punto un control de seguridad es dado a generar falsos positivos. Un valor de precisión más alto significa que el control de seguridad genera menos falsos positivos.
- La **exhaustividad** es la fracción (o porcentaje) de ataques que se señalaron correctamente. Un valor de exhaustividad más alto significa que la solución está detectando los ataques correctamente.

Con los cuatro factores mencionados anteriormente, también resulta útil calcular una puntuación de exactitud única que cuantifique correctamente las capacidades generales de una solución. Una puntuación de este tipo es el coeficiente de correlación de Matthews (MCC, por sus siglas en inglés), o coeficiente phi. La fórmula del MCC da lugar a un único valor MCC.

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP \times FP)(TP + FN)(TN + FP)(TN + FN}}$$

Figura 1: Fórmula para calcular el coeficiente de correlación de Matthews

Básicamente, un valor MCC de **+1,0** significa que la solución acierta en todo momento: siempre detecta la actividad maliciosa y siempre permite la actividad legítima. Un valor MCC de **-1,0** significa que la solución se equivoca en todas las decisiones que toma: bloquea siempre la actividad legítima y permite toda la actividad maliciosa. Por último, un valor MCC de **0,0** significa que utilizar la solución es como tomar decisiones aleatorias.

Ahora que sabemos qué medir para evaluar una solución de ciberseguridad, pasemos a la práctica con nuestra solución WAAS.

Medición de la exactitud: módulo Web Application and API Security

En el contexto de la seguridad de las aplicaciones web, un falso positivo significa que el mecanismo de protección ha bloqueado por error una transacción HTTP legítima (por ejemplo, el envío de un formulario por parte de un usuario legítimo). Un falso negativo significa que el mecanismo de protección no ha señalado un ataque basado en la web, como un intento de inyección de SQL. Los positivos reales aluden a ataques basados en la web que se han señalado correctamente, mientras que los negativos reales se refieren a tráfico de usuarios legítimo al que se ha permitido llegar a la aplicación web o al endpoint de la API.

Según esto, en el contexto de la seguridad de las aplicaciones web, la **precisión** representa la cantidad de falsos positivos que genera el control de seguridad. La **exhaustividad**, por su parte, describe la eficacia del control de seguridad a la hora de detectar ataques.

Obviamente, lo que nos interesa es que los valores de precisión, exhaustividad y MCC sean lo más altos posible. Para saber si lo son, necesitamos un método que permita probar estos valores.

Medición de los falsos negativos y los positivos reales

Para medir la eficacia de una solución en lo que se refiere a la generación de falsos negativos y positivos reales, lo que hay que hacer es preparar un enorme arsenal de casos de prueba de ataques que abarque todos los vectores de ataque conocidos. Para compilar dicho arsenal, se puede recopilar tráfico de ataques reales, grabar herramientas de automatización de *hacking* y usurpar contenidos de los sitios de *hacking*.

Una vez preparado el arsenal, basta implementar el mecanismo de protección ante una aplicación web e iniciar el ataque. Todo ataque que sea bloqueado equivale a un positivo real, mientras que un ataque que se pase por alto representa un falso negativo.

Medición de falsos positivos y negativos reales

Aquí la cosa se complica. Para medir los falsos positivos, se puede proteger una aplicación web y, a continuación, observar si hay tráfico de usuarios legítimo que active el control de seguridad. Este método exige definir qué cantidad de tráfico se considera suficiente. Además, los datos estadísticos obtenidos solo serán pertinentes para esa aplicación web en concreto.

Una ligera variación de este método consistiría en grabar una gran cantidad de tráfico legítimo procedente de la mayor cantidad posible de aplicaciones web y API reales, que abarquen numerosos tipos de aplicaciones diferentes (por ejemplo, API de *back-end* de aplicaciones móviles, sitios web de comercio electrónico, sistemas CRM, sitios web de marketing, etc.). Cuando haya recopilado un conjunto de tráfico legítimo suficientemente diverso, será el momento de reproducirlo mediante el mecanismo de protección que se esté poniendo a prueba. Cada vez que este tráfico active el control de seguridad, estamos ante un falso positivo, mientras que cada solicitud que logre llegar a la aplicación equivale a un negativo real.

Una vez calculados estos cuatro factores, se podrá obtener la puntuación MCC y evaluar la exactitud general de la solución.

Conviene señalar que este método no es precisamente nuevo. El autor desarrolló un marco para probar la precisión de los cortafuegos de aplicaciones web en 2013 y lo presentó ese mismo año en la conferencia del Proyecto abierto de seguridad de aplicaciones web (OWASP, por sus siglas en inglés) de la Ciudad de Nueva York.

Prueba de exactitud: módulo WAAS de Prisma Cloud

Para nuestra prueba, recopilamos más de 200 000 transacciones HTTP legítimas procedentes de un conjunto diverso de grandes aplicaciones web, sitios web y API web. Además, compilamos un amplio arsenal de más de 5000 vectores de ataque web únicos, que abarcan las principales 10 categorías de OWASP y más. Implementamos el módulo WAAS y ejecutamos las distintas situaciones.

La puntuación MCC general calculada para el módulo WAAS de Prisma Cloud fue **0,956**.

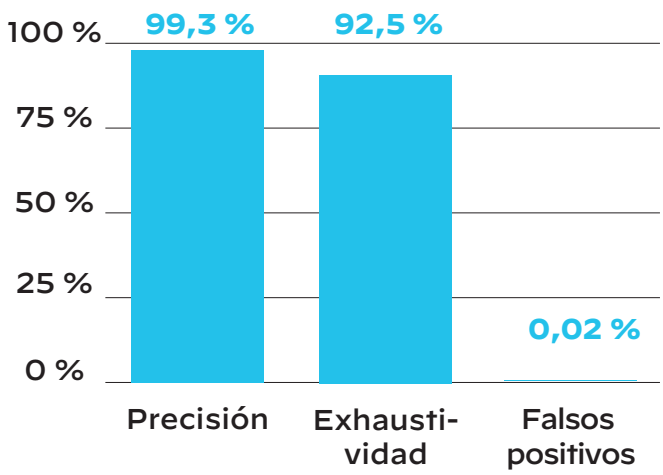

Figura 2: Módulo WAAS de Prisma Cloud: precisión, exhaustividad y falsos positivos

Comparaciones con otras soluciones del sector

Estos datos son muy interesantes, pero para que sean realmente significativos hay que compararlos con los de otras soluciones destacadas del sector. Con la misma metodología de prueba, llevamos a cabo el mismo conjunto de pruebas con otras seis soluciones:

- Dos soluciones y servicios líderes de cortafuegos de aplicaciones web (WAF, por sus siglas en inglés)
- Una solución WAF de código abierto
- Dos de las principales soluciones WAF de proveedores de servicios en la nube (CSP, por sus siglas en inglés)
- Una solución de autoprotección de aplicaciones en tiempo de ejecución (RASP, por sus siglas en inglés)

En la tabla 1 se muestran los resultados compilados y se compara el módulo WAAS de Prisma Cloud con otras soluciones similares.

Tabla 1: Módulo WAAS de Prisma Cloud comparado con otras soluciones similares

Solución	Precisión	Exhaustividad	Falsos positivos	MCC
Módulo WAAS de Prisma Cloud	**99,3 %**	**92,5 %**	**0,02 %**	**0,956**
WAF n.º 1	65,5 %	91,1 %	1,61 %	0,764
WAF n.º 2	87 %	85,9 %	0,43 %	0,866
WAF de código abierto	91,3 %	91 %	0,29 %	0,908

Tabla 1: Módulo WAAS de Prisma Cloud comparado con otras soluciones similares (continuación)				
Solución	**Precisión**	**Exhaustividad**	**Falsos positivos**	**MCC**
WAF de CSP n.º 1	57,6 %	83,5 %	2 %	0,681
WAF de CSP n.º 2	61,4 %	91,3 %	0,85 %	0,729
Solución RASP	79,9 %	50,1 %	0,85 %	0,614

WAAS de Prisma Cloud: exactitud superior, sin duda

Hemos examinado la metodología óptima para poner a prueba la exactitud de una solución de seguridad de aplicaciones web y API. Hemos constatado que no basta con examinar el rigor de una solución y la cantidad de ataques que bloquea si no tenemos en cuenta cómo se comporta con el tráfico legítimo y la cantidad de falsos positivos que genera. Utilizando la metodología de prueba presentada, hemos comparado los datos estadísticos del módulo WAAS de Prisma Cloud con otras soluciones líderes en el sector: los resultados hablan por sí solos y demuestran claramente su superioridad en términos de exactitud.

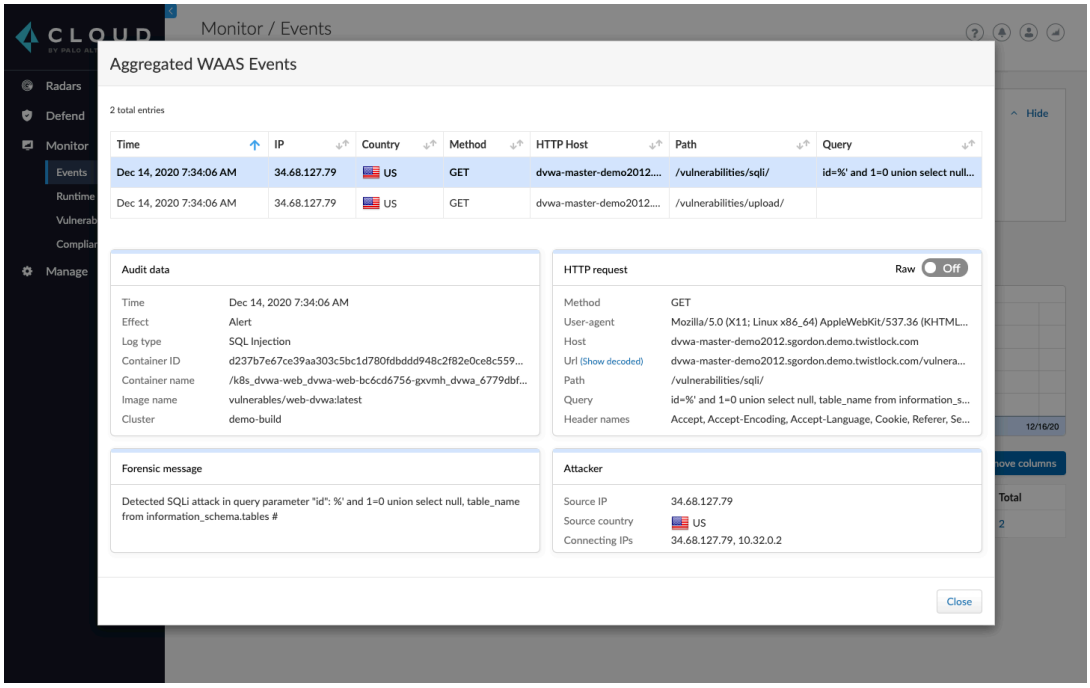

Figura 3: Datos de auditoría de WAAS agregados en Prisma Cloud

Acerca de Prisma Cloud de Palo Alto Networks

Prisma® Cloud es la plataforma de protección de aplicaciones nativa en la nube (CNAPP, por sus siglas en inglés) más completa del sector, cuya visión es una seguridad en la nube integrada insuperable para garantizar que los entornos en la nube y las aplicaciones nativas en la nube estén bien protegidos, a lo largo de todo el ciclo de vida del desarrollo y tanto en entornos híbridos como de varias nubes.

Este enfoque integrado elimina las limitaciones que presentan las arquitecturas nativas en la nube en materia de seguridad —en lugar de ocultarlas— y acaba con la separación de las operaciones de seguridad en todo el ciclo de vida de las aplicaciones, al tiempo que permite a los equipos de DevSecOps/DevOps y a quienes se ocupan de la seguridad de las aplicaciones automatizar la seguridad para responder a las necesidades de las arquitecturas nativas en la nube, que cambian constantemente.

Para obtener más información, visite nuestro sitio web o vea una demostración hoy mismo.

paloalto NETWORKS | El socio de ciberseguridad por excelencia

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883
www.paloaltonetworks.es