Elevando o nível das soluções de segurança de APIs e aplicativos da Web

Os aplicativos nativos da nuvem continuam a crescer e estão sendo reunidos usando contêineres, funções sem servidor e microsserviços em uma variedade de pilhas de tecnologia. Em vez de se estabilizar ao longo do tempo, essas arquiteturas complexas só vão se tornar mais prevalentes. Proteger os aplicativos da web e as APIs que sustentam essas arquiteturas complexas tem sido tradicionalmente um desafio para as equipes de segurança de aplicativos e DevOps. Os aplicativos e APIs da web estão mudando continuamente e as soluções de segurança da web existentes não têm a cobertura necessária.

Em resposta, a Palo Alto Networks oferece a melhor segurança de APIs e aplicativos da web (WAAS) como parte da plataforma Prisma Cloud. Neste artigo, oferecemos uma análise quantitativa do módulo e comparamos com outras soluções do setor. Ao fazer isso, demonstramos a precisão superior do WAAS do Prisma Cloud.

Conceitos básicos de medição: precisão da solução de segurança cibernética

O requisito mais básico para um aplicativo da web e solução de proteção de API é bloquear ataques baseados na web, como injeção SQL, scripts entre sites e inclusão de arquivos locais. No entanto, as soluções de segurança cibernética nunca devem ser avaliadas com base apenas na capacidade de bloquear ataques. Se fosse esse o caso, a melhor solução de segurança cibernética provavelmente seria um cabo ethernet desconectado, não conectado a nada. Infelizmente, o outro lado dessa abordagem drástica provavelmente seria uma perda significativa de negócios legítimos.

Os melhores testes comparativos levam em consideração vários fatores de precisão de classificação binária padrão relacionados à segurança cibernética ao avaliar a competência da solução. Neste artigo, consideramos:

- **Falsos positivos (FP)**—atividade legítima sinalizada incorretamente como maliciosa
- **Falsos negativos (FN)**—atividade maliciosa não detectada
- **Verdadeiros positivos (VP)**—atividade maliciosa detectada corretamente como maliciosa
- **Verdadeiros negativos (VN)**—atividade legítima detectada corretamente como legítima

Qualquer análise que tente avaliar e comparar a precisão das soluções de segurança cibernética deve considerar todos os quatro fatores para permitir que usuários e compradores escolham qual solução melhor se encaixa em seu caso de uso. Afinal, nem todos os casos de uso são iguais; alguns podem preferir um equilíbrio diferente entre a continuidade dos negócios e os níveis de proteção de segurança.

Esses quatro fatores de precisão podem ser medidos usando dois conceitos estatísticos conhecidos como precisão e recolha:

- **Precisão** é a fração (ou porcentagem) de solicitações sinalizadas que foram realmente maliciosas. Em outras palavras, a precisão descreve a propensão de um controle de segurança a falsos positivos. Um valor de precisão mais alto significa que o controle gera menos falsos positivos.
- **Recolha** é a fração (ou porcentagem) de ataques que foram sinalizados corretamente. Um valor de recolha mais alto significa que a solução está detectando ataques adequadamente.

Usando os quatro fatores de precisão acima mencionados, também é útil calcular uma única pontuação de precisão que quantifique adequadamente as habilidades gerais de uma solução. Uma dessas pontuações é o coeficiente de correlação de Matthews (CCM), ou coeficiente phi. A fórmula do CCM resulta em um único valor de CCM.

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

Figura 1: Fórmula para calcular o coeficiente de correlação de Matthews (CCM)

Em essência, um valor de CCM de **+1,0** significa que a solução está correta o tempo todo: sempre detecta atividades maliciosas e sempre permite atividades legítimas. Um valor de CCM de **-1,0** significa que a solução está errada em cada decisão que toma: a atividade legítima é sempre bloqueada e a atividade maliciosa nunca é bloqueada. Por fim, um valor de CCM de **0,0** significa que a solução não é melhor do que apenas aplicar uma escolha aleatória.

Agora que sabemos o que medir ao avaliar uma solução de segurança cibernética, vamos aplicar isso à nossa solução WAAS.

Medição de precisão: Segurança de APIs e aplicativos da Web

No contexto da segurança de aplicativos da web, um falso positivo significa que uma transação HTTP legítima (por exemplo, o envio de formulário de um usuário legítimo) foi bloqueada incorretamente pelo mecanismo de proteção. Um falso negativo significa que um ataque baseado na web, como uma tentativa de injeção SQL, não foi sinalizado pelo mecanismo de proteção. Os verdadeiros positivos indicam ataques baseados na web que foram sinalizados corretamente, e os verdadeiros negativos significam que o tráfego legítimo do usuário foi permitido alcançar o endpoint da API ou do aplicativo da web.

Com base nisso, a **precisão**, no contexto da segurança de aplicativos da web, retrata o nível de falsos positivos gerados pelo controle de segurança. A **recolha** descreve a eficácia do controle de segurança na detecção de ataques.

Naturalmente, é bom que os valores de precisão, recolha e CCM sejam o mais altos possível. Para obter essa garantia, precisamos ter uma maneira de testar esses valores.

Medição de falsos negativos e verdadeiros positivos

Para medir o quão bem uma solução lida com falsos negativos e verdadeiros positivos, tudo o que você precisa fazer é preparar um vasto arsenal de casos de teste de ataque, abordando todos os vetores de ataque conhecidos. Esse arsenal pode ser compilado coletando tráfego de ataque do mundo real, monitorando ferramentas de automação de hackers e analisando conteúdo de sites de hackers.

Uma vez que o arsenal estiver pronto para o uso, você só precisa implantar o mecanismo de proteção na frente de um aplicativo da web e acionar. Qualquer ataque bloqueado denota um verdadeiro positivo e um ataque perdido denota um falso negativo.

Medição de falsos positivos e verdadeiros negativos

É aqui que as coisas ficam complicadas. Você pode medir falsos positivos protegendo um aplicativo da web e, em seguida, inspecionando se o tráfego legítimo do usuário aciona um controle de segurança. Tal abordagem requer que você defina quanto tráfego é suficiente. Além disso, as estatísticas recolhidas só serão relevantes para esse aplicativo da web específico.

Uma abordagem ligeiramente diferente seria registrar uma grande quantidade de tráfego legítimo do maior número possível de aplicativos da web e APIs do mundo real, de muitos tipos diferentes de aplicativos (por exemplo, APIs de back-end de aplicativos móveis, sites de comércio eletrônico, CRMs, sites de marketing). Depois de coletar um conjunto de testes diversificado de tráfego legítimo, o tráfego é reproduzido através do mecanismo de proteção testado. Cada acionador de segurança desse conjunto denota um falso positivo, e cada solicitação permitida a atingir o aplicativo denota um verdadeiro negativo.

Com todos os quatro fatores de precisão calculados, você pode calcular a pontuação CCM e avaliar a precisão geral da solução.

Deve-se notar que essa abordagem não é exatamente nova. O autor desenvolveu uma estrutura para testar a precisão dos firewalls de aplicativos da web em 2013 e a apresentou na conferência OWASP de Nova York naquele ano.

Teste de precisão: Módulo WAAS do Prisma Cloud

Para nosso teste de precisão, coletamos um conjunto de mais de 200.000 transações HTTP legítimas de um conjunto diversificado de aplicativos, sites e APIs da web. Além disso, compilamos um rico arsenal de mais de 5.000 vetores de ataque da web exclusivos, que abarcam todas as 10 principais categorias do OWASP e além. Implantamos o módulo WAAS e executamos os cenários.

A pontuação global do CCM calculada para o módulo WAAS do Prisma Cloud foi de **0,956**.

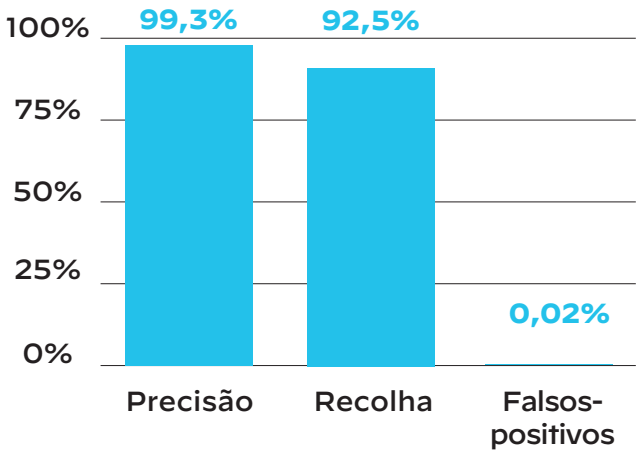

Figura 2: Módulo WAAS do Prisma Cloud—precisão, recolha e falsos-positivos

Comparações do setor

Embora essas estatísticas sejam interessantes, elas não são inteiramente significativas, a menos que você compare a precisão do módulo com outras soluções líderes do setor. Usando a mesma metodologia de teste, executamos o mesmo conjunto de testes em relação a seis outras soluções:

- Duas principais soluções e serviços de firewall de aplicativos da web (WAF)
- Uma solução WAF de código aberto
- Duas principais soluções WAF para provedores de serviços de nuvem (CSP)
- Uma solução de autoproteção de aplicativo de tempo de execução (RASP)

A tabela 1 apresenta os resultados compilados, comparando o módulo Prisma Cloud WAAS com soluções relacionadas.

Tabela 1: Módulo WAAS do Prisma Cloud em comparação com soluções relacionadas

Solução	Precisão	Recolha	Falsos-positivos	CCM
Módulo WAAS do Prisma Cloud	**99,3%**	**92,5%**	**0,02%**	**0,956**
WAF #1	65,5%	91,1%	1,61%	0,764
WAF #2	87%	85,9%	0,43%	0,866
WAF de código aberto	91,3%	91%	0,29%	0,908

Tabela 1: Módulo WAAS do Prisma Cloud em comparação com soluções relacionadas (cont.)				
Solução	**Precisão**	**Recolha**	**Falsos-positivos**	**CCM**
CSP WAF #1	57,6%	83,5%	2%	0,681
CSP WAF #2	61,4%	91,3%	0,85%	0,729
Solução RASP	79,9%	50,1%	0,85%	0,614

WAAS do Prisma Cloud: Precisão superior sem dúvida

Examinamos a metodologia ideal para testar a precisão de uma solução de segurança de API e aplicativo da Web. Aprendemos que não é suficiente discutir o quão rigorosa é uma solução ou quantos ataques ela pode bloquear se não levarmos em conta seu comportamento no tráfego legítimo e seu nível de falsos positivos. Usando a metodologia de teste apresentada, comparamos as estatísticas de precisão do módulo WAAS do Prisma Cloud com outras soluções líderes. As estatísticas falam por si e demonstram claramente sua precisão superior.

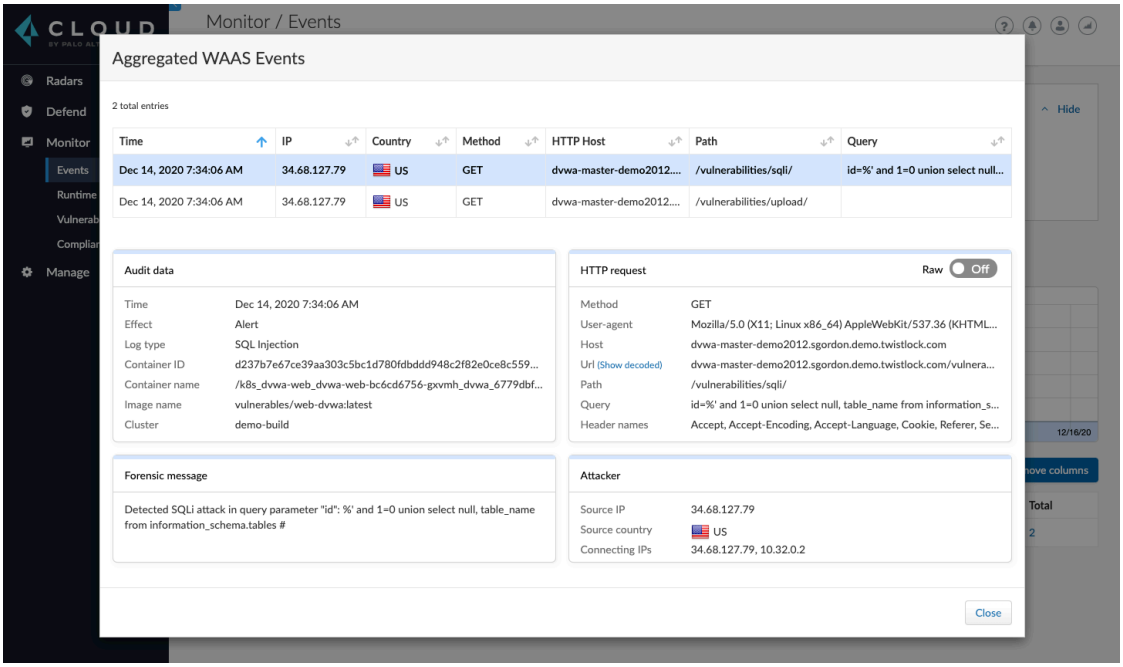

Figura 3: Detalhes agregados da auditoria do WAAS no Prisma Cloud

Sobre o Prisma Cloud da Palo Alto Networks

O Prisma® Cloud é a plataforma de proteção de aplicativos nativos da nuvem (CNAPP) mais completa do setor, com uma visão de segurança na nuvem integrada e incomparável para garantir que os ambientes de nuvem e os aplicativos nativos da nuvem estejam protegidos durante todo o ciclo de vida do desenvolvimento e em ambientes híbridos e de várias nuvens.

A abordagem integrada elimina as restrições de segurança envolvendo arquiteturas nativas da nuvem, em vez de mascará-las, e divide os silos operacionais de segurança ao longo de todo o ciclo de vida do aplicativo, permitindo que as equipes de segurança de aplicativos e DevSecOps/DevOps automatizem a segurança para atender às necessidades variáveis das arquiteturas nativas da nuvem.

Para saber mais, você pode acessar o nosso site ou assistir a uma demonstração agora mesmo.

paloalto® NETWORKS | Cybersecurity Partner of Choice

3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087