Migliorare la sicurezza per applicazioni Web e API

Le applicazioni cloud-native continuano a crescere e vengono incluse in pacchetti utilizzando container, funzioni serverless e microservizi su una serie di stack tecnologici. Anziché livellarsi nel tempo, queste architetture complesse sono solo destinate a diventare più prevalenti. La protezione di applicazioni Web e API che sono alla base di queste architetture complesse ha tradizionalmente rappresentato una sfida per i team di sicurezza delle applicazioni e DevOps. Le applicazioni Web e le API sono in continua evoluzione, di conseguenza le soluzioni di sicurezza Web esistenti non offrono la copertura necessaria.

In risposta a questo problema, Palo Alto Networks offre la migliore soluzione per la Sicurezza di applicazioni Web API (WAAS) come parte della piattaforma Prisma Cloud. In questo documento viene presentata un'analisi quantitativa del modulo unitamente a un confronto con altre soluzioni del settore. Questo approccio consentirà quindi di dimostrare la precisione superiore offerta dalla soluzione WAAS di Prisma Cloud.

Misurazione 101: Precisione della soluzione di sicurezza informatica

Il requisito più elementare per una soluzione di protezione per applicazioni Web e API è bloccare gli attacchi basati su Web, come SQL injection, Cross-Site Scripting e Local File Inclusion. Le soluzioni di sicurezza informatica, tuttavia, non devono mai essere valutate solo in base all'efficacia nel bloccare gli attacchi. In tal caso, la soluzione migliore per la sicurezza informatica sarebbe probabilmente un cavo Ethernet scollegato, disconnesso da tutto. Purtroppo, il rovescio della medaglia di questo approccio drastico sarebbe probabilmente una perdita significativa di attività legittime.

I migliori test comparativi tengono conto di più fattori di precisione della classificazione binaria standard correlati alla sicurezza informatica nella valutazione della competenza della soluzione. In questo documento vengono considerati:

- **Falsi positivi (FP)**: attività legittima erroneamente contrassegnata come dannosa
- **Falsi negativi (FN)**: attività dannosa non rilevata
- **Veri positivi (VP)**: attività dannosa correttamente rilevata come dannosa
- **Veri negativi (VN)**: attività legittima correttamente rilevata come legittima

Tutte le analisi che tentano di valutare e confrontare la precisione delle soluzioni di sicurezza informatica devono considerare tutti e quattro i fattori per consentire agli utenti e agli acquirenti di scegliere la soluzione più adatta al proprio caso d'uso. Dopo tutto, non tutti i casi d'uso sono uguali: alcuni potrebbero preferire un diverso equilibrio tra la continuità aziendale e i livelli di protezione della sicurezza.

Questi quattro fattori di precisione possono essere misurati utilizzando due concetti statistici noti come precisione e recupero:

- **Precisione** è la parte (o percentuale) delle richieste contrassegnate risultate effettivamente dannose. In altre parole, la precisione descrive la predisposizione di un controllo di sicurezza ai falsi positivi. Un valore di precisione più elevato significa che il controllo genera meno falsi positivi.
- **Recupero** è la parte (o percentuale) di attacchi contrassegnati correttamente. Un valore di recupero più elevato significa che la soluzione rileva gli attacchi in modo appropriato.

Utilizzando i quattro fattori di precisione indicati sopra, è inoltre utile calcolare un singolo punteggio di precisione che quantifichi in modo appropriato le capacità complessive di una soluzione. Uno di questi punteggi è il Coefficiente di correlazione di Matthews (Matthews Correlation Coefficient, MCC), o coefficiente Phi. La formula MCC restituisce un singolo valore MCC.

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

Figura 1: formula per il calcolo del coefficiente di correlazione di Matthews

In sostanza, un valore MCC di **+1,0** significa che la soluzione è sempre corretta: rileva sempre le attività dannose e consente sempre attività legittime. Un valore MCC di **-1.0** indica che la soluzione commette un errore in ogni decisione che prende: l'attività legittima viene sempre bloccata e l'attività dannosa viene sempre consentita. Infine, un valore MCC di **0,0** significa che la soluzione non offre alcun vantaggio rispetto alla pura applicazione di una scelta casuale.

Ora che si conoscono gli aspetti da misurare durante la valutazione di una soluzione di sicurezza informatica, questo approccio verrà applicato alla soluzione WAAS.

Misurazione della precisione: Sicurezza di applicazioni Web e API

Nel contesto della sicurezza delle applicazioni Web, un falso positivo significa che una transazione HTTP legittima, ad esempio l'invio di un modulo di un utente legittimo, è stata erroneamente bloccata dal meccanismo di protezione. Un falso negativo significa che un attacco basato su Web, come un tentativo di SQL injection, non è stato contrassegnato dal meccanismo di protezione. I veri positivi indicano gli attacchi basati su Web contrassegnati correttamente, mentre i veri negativi indicano che al traffico utente legittimo è stato consentito di raggiungere l'applicazione Web o l'endpoint API.

In base a ciò, **precisione**, nel contesto della sicurezza delle applicazioni Web, descrive il livello di falsi positivi generati dal controllo di sicurezza. **Recupero**, quindi, descrive l'efficacia del controllo di protezione nel rilevamento degli attacchi.

Naturalmente, si desidera che i valori di precisione, recupero e MCC siano il più alti possibile. Per ottenere questa garanzia, è necessario disporre di una soluzione per testare questi valori.

Misurazione di falsi negativi e veri positivi

Per misurare l'efficacia di una soluzione nella gestione di falsi negativi e veri positivi, è sufficiente preparare un vasto arsenale di casi di test di attacco, che includano tutti i vettori di attacco noti. Un tale arsenale può essere compilato mediante la raccolta del traffico degli attacchi reali, registrando gli strumenti di automazione degli hacker ed eseguendo lo scraping del contenuto del sito degli hacker.

Non appena l'arsenale è pronto per il lancio, è sufficiente distribuire il meccanismo di protezione all'applicazione Web e attivarlo. Qualsiasi attacco bloccato indica un vero positivo, mentre un attacco non rilevato indica un falso negativo.

Misurazione di falsi positivi e veri negativi

Questa è la fase in cui tutto si complica. È possibile misurare i falsi positivi proteggendo un'applicazione Web e verificando se il traffico utente legittimo attiva un controllo di sicurezza. Tale approccio richiede di definire la quantità di traffico sufficiente. Inoltre, le statistiche raccolte saranno pertinenti solo per l'applicazione Web specifica.

Un'alternativa leggermente diversa prevede la registrazione di una grande quantità di traffico legittimo da quante più applicazioni Web e API reali possibili, da numerosi tipi diversi di applicazioni, ad esempio, API back-end per app mobili, siti Web di e-commerce, sistemi CRM, siti Web di marketing. Una volta raccolto un set eterogeneo di test di traffico legittimo, il traffico viene riprodotto attraverso il meccanismo di protezione verificato. Ogni trigger di sicurezza di questo set indica un falso positivo, mentre ogni richiesta a cui viene consentito di raggiungere l'applicazione indica un vero negativo.

Dopo aver calcolato tutti e quattro i fattori di precisione, è possibile calcolare il punteggio MCC e valutare la precisione complessiva della soluzione.

È opportuno notare che questo approccio non è esattamente nuovo. L'autore ha sviluppato un framework per testare la precisione dei firewall delle applicazioni Web nel 2013 e lo ha presentato alla conferenza OWASP di New York City lo stesso anno.

Test di precisione: Modulo WAAS di Prisma Cloud

Per il presente test di accuratezza, è stato raccolto un set di oltre 200.000 transazioni HTTP legittime da una serie diversificata di applicazioni Web, siti Web e API Web. È stato inoltre compilato un ampio arsenale di oltre 5.000 vettori di attacco web univoci, che coprono le prime 10 categorie OWASP e oltre. Il modulo WAAS è stato distribuito e sono stati eseguiti gli scenari.

Il punteggio MCC complessivo calcolato per il modulo WAAS di Prisma Cloud è **0,956**.

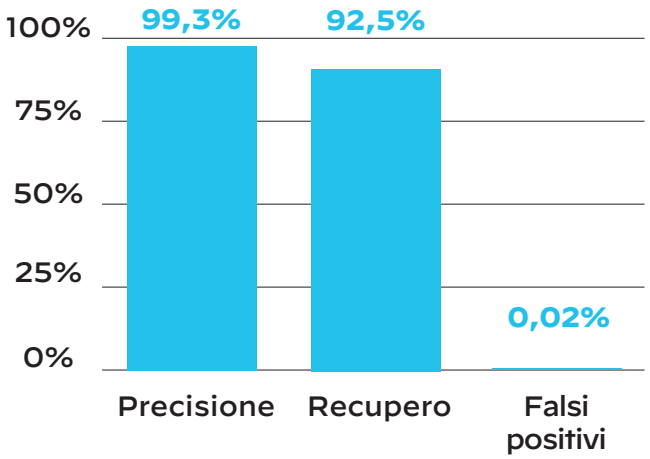

Figura 2: Modulo WAAS di Prisma Cloud: precisione, recupero e falsi positivi

Confronti tra le soluzioni del settore

Sebbene queste statistiche siano interessanti, non sono del tutto significative a meno che non si confronti la precisione del modulo con altre soluzioni leader del settore. Utilizzando la medesima metodologia di test, è stato eseguito lo stesso set di test per altre sei soluzioni:

- Due soluzioni e servizi WAF (Web Application Firewall) leader del settore
- Una soluzione WAF open source
- Due soluzioni WAF di provider di servizi cloud (CSP) leader di settore
- Una soluzione di autoprotezione delle applicazioni di runtime (RASP)

La Tabella 1 mostra i risultati compilati, con il confronto del modulo WAAS di Prisma Cloud con le soluzioni correlate.

Tabella 1: Confronto tra il modulo WAAS di Prisma Cloud e le soluzioni correlate

Soluzione	Precisione	Recupero	Falsi positivi	MCC
Modulo WAAS di Prisma Cloud	**99,3%**	**92,5%**	**0,02%**	**0,956**
WAF n. 1	65,5%	91,1%	1,61%	0,764
WAF n. 2	87%	85,9%	0,43%	0,866
WAF open source	91,3%	91%	0,29%	0,908

Tabella 1: Confronto tra il modulo WAAS di Prisma Cloud e le soluzioni correlate (continua)				
Soluzione	**Precisione**	**Recupero**	**Falsi positivi**	**MCC**
WAF CSP n. 1	57,6%	83,5%	2%	0,681
WAF CSP n. 2	61,4%	91,3%	0,85%	0,729
Soluzione RASP	79,9%	50,1%	0,85%	0,614

WAAS di Prisma Cloud Precisione superiore oltre ogni dubbio

È stata esaminata la metodologia ottimale per testare la precisione di una soluzione di sicurezza di applicazioni Web e API. Si è appreso che non è sufficiente discutere di quanto sia rigorosa una soluzione, o di quanti attacchi possa bloccare, se non si tiene conto del suo comportamento sul traffico legittimo e del suo livello di falsi positivi. Utilizzando la metodologia di test presentata, sono state confrontate le statistiche sulla precisione del modulo WAAS di Prisma Cloud con altre soluzioni leader di settore: le statistiche parlano da sole ed evidenziano in modo chiaro la sua precisione superiore.

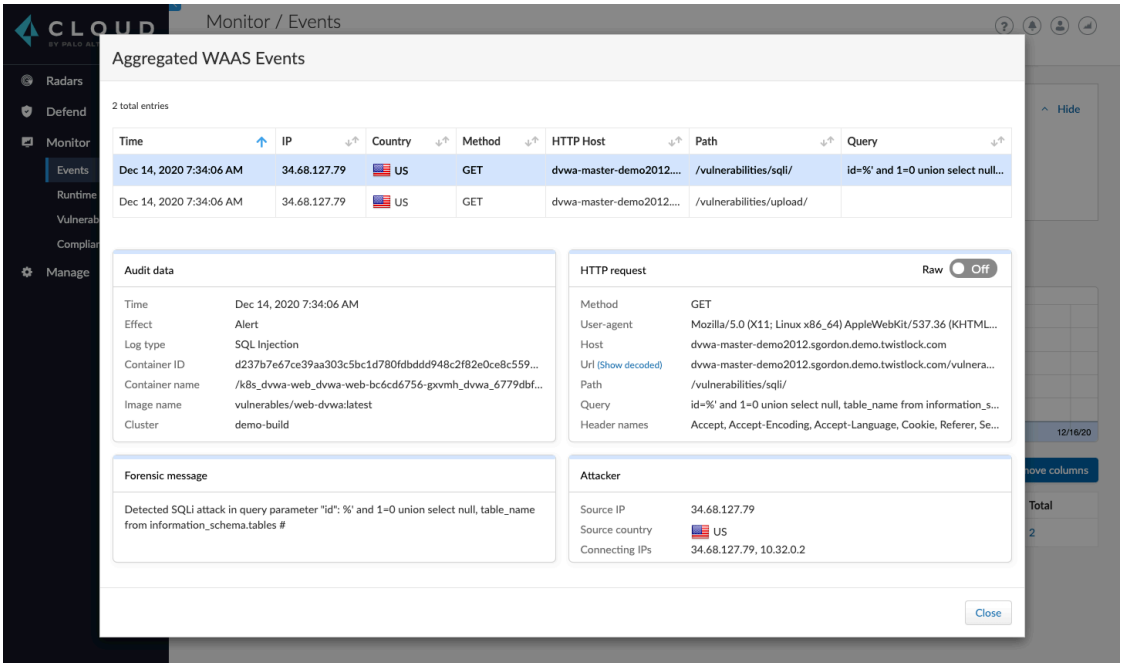

Figura 3: dettagli aggregati della verifica della soluzione WAAS in Prisma Cloud

Informazioni su Prisma Cloud di Palo Alto Networks

Prisma® Cloud è la piattaforma di protezione delle applicazioni cloud-native (CNAPP) più completa del settore, con una visione per la sicurezza cloud integrata e impareggiabile, che mira a garantire la sicurezza degli ambienti cloud e delle applicazioni cloud-native per tutto il ciclo di vita dello sviluppo e in ambienti ibridi e multicloud.

L'approccio integrato elimina, anziché mascherarli, i limiti di sicurezza delle architetture native per il cloud e abbatte i compartimenti stagni tra le operazioni di sicurezza nell'intero ciclo di vita delle applicazioni per consentire ai team di sicurezza delle applicazioni e DevSecOps/DevOps di automatizzare la sicurezza per soddisfare le esigenze di sicurezza in continua evoluzione delle architetture native del cloud.

Per ulteriori informazioni visita il nostro sito Web o guarda una demo.

paloalto® NETWORKS | Cybersecurity Partner of Choice

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

Telefono: +1.408.753.4000
Vendite: +1.866.320.4788
Assistenza: +1.866.898.9087