La sécurité des applications web et des API franchit un nouveau cap

Regroupées sur une variété de stacks technologiques via des containers, des fonctions sans serveur et des microservices, les applications cloud-native ne cessent de se multiplier. Et plutôt que de s'équilibrer au fil du temps, ces architectures complexes ne feront que se répandre davantage dans le futur. Pour les équipes DevOps et de sécurité, protéger les applications web et les API qui sous-tendent ces architectures a toujours été un défi. Et pour cause : les applications web et les API évoluent en permanence, et les solutions de sécurité web existantes n'offrent pas la couverture nécessaire.

En réponse à cette problématique, Palo Alto Networks propose un module de pointe de sécurité des applications web et des API (WAAS) intégré à sa plateforme Prisma Cloud. Ce livre blanc présente une analyse quantitative de ce module et le compare à d'autres solutions du secteur, démontrant ainsi la supériorité du WAAS de Prisma Cloud en termes d'exactitude.

Les bases : exactitude d'une solution de cybersécurité

Le strict minimum que l'on exige d'une solution de protection des applications web et des API est de pouvoir bloquer les attaques web telles que les injections SQL, les scripts intersites et les inclusions de fichiers locaux. Ceci étant, une solution de sécurité ne devrait jamais être évaluée uniquement par sa capacité à bloquer les attaques. Si tel était le cas, il n'y aurait probablement pas de meilleure solution de sécurité qu'un câble Ethernet déconnecté – de tout. Mais l'inconvénient de cette approche drastique est qu'elle écarte un grand nombre d'activités légitimes.

Lors de l'évaluation d'une solution de sécurité, les tests comparatifs les plus pointus prennent en compte plusieurs facteurs d'exactitude pour une classification binaire standard. Ce livre blanc se penche sur quatre d'entre eux :

- **Faux positifs (FP)** – activité légitime signalée à tort comme malveillante
- **Faux négatifs (FN)** – activité malveillante non détectée
- **Vrais positifs (TP)** – activité malveillante détectée à raison comme malveillante
- **Vrais négatifs (TN)** – activité légitime signalée à raison comme légitime

Pour aider les utilisateurs et les acheteurs à faire le bon choix, toute analyse visant à évaluer et à comparer l'exactitude des solutions de cybersécurité doit tenir compte de ces quatre facteurs. Après tout, tous les cas d'usage ne se ressemblent pas. Chaque entreprise privilégiera un niveau d'équilibre différent entre la continuité d'activité et le niveau de protection.

Ces quatre facteurs d'exactitude peuvent être mesurés à l'aide de deux concepts statistiques : la précision et le rappel.

- La **précision** est la fraction (ou le pourcentage) de demandes signalées qui se sont avérées être malveillantes. En d'autres termes, la précision décrit à quel point un contrôle de sécurité peut être sujet à des faux positifs. Plus la valeur de la précision est élevée, moins le contrôle génère de faux positifs.
- Le **rappel** est la fraction (ou le pourcentage) d'activités signalées à raison comme malveillantes. Une valeur de rappel élevée montre que la solution détecte correctement les attaques.

En plus des quatre facteurs d'exactitude susmentionnés, il est utile de calculer un score d'exactitude pour quantifier convenablement les capacités globales de la solution. L'un de ces scores est le coefficient de corrélation de Matthews (MCC), ou coefficient phi. La formule de calcul du MCC donne lieu à une valeur unique.

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

Figure 1. Formule de calcul du coefficient de corrélation de Matthews

Concrètement, un MCC de **+1,0** signifie que la solution voit juste à tous les coups : elle détecte toujours les activités malveillantes et autorise toujours les activités légitimes. Un MCC de **-1,0** signifie que la solution se trompe à chaque fois : une activité légitime est toujours bloquée et une activité malveillante ne l'est jamais. Enfin, un MCC de **0,0** signifie que la solution ne fait pas mieux que si l'on appliquait un choix aléatoire.

Maintenant que nous savons ce qu'il faut mesurer lors de l'évaluation d'une solution de cybersécurité, appliquons cela à notre solution WAAS.

Mesure de l'exactitude : sécurité des applications web et des API

En matière de sécurité des applications web, on parle de faux positif lorsqu'une transaction HTTP légitime (par exemple, l'envoi d'un formulaire par un utilisateur légitime) a été incorrectement bloquée par le mécanisme de protection. Un faux négatif signifie qu'une attaque web, telle qu'une tentative d'injection SQL, n'a pas été signalée par le mécanisme de protection. Les vrais positifs indiquent des attaques web ayant été correctement signalées, et les vrais négatifs signifient qu'un trafic utilisateur légitime a été autorisé à atteindre l'application web ou le terminal de l'API.

Partant de là, la **précision** représente le niveau de faux positifs générés par le contrôle de sécurité. Quant au **rappel**, il décrit l'efficacité du contrôle de sécurité en termes de détection des attaques.

Bien évidemment, on souhaite que les valeurs de la précision, du rappel et du MCC soient aussi satisfaisantes que possible. Pour s'en assurer, il nous faut un moyen de tester ces valeurs.

Mesurer les faux négatifs et les vrais positifs

Pour évaluer la manière dont une solution traite les faux négatifs et les vrais positifs, il vous suffit de préparer un vaste arsenal de tests d'attaques couvrant tous les vecteurs connus. Un tel arsenal peut être compilé en collectant le trafic d'attaques réelles, en enregistrant des outils d'automatisation de hackers et en extrayant du contenu de sites malveillants.

Une fois prêt, il ne vous reste plus qu'à déployer le mécanisme de protection pour l'application web concernée. Toute attaque bloquée indique un vrai positif, et une attaque manquée sera considérée comme un faux négatif.

Mesurer les faux positifs et les vrais négatifs

C'est là que les choses se compliquent. Pour mesurer les faux positifs, vous pouvez protéger une application web, puis vérifier si le trafic utilisateur légitime déclenche ou non un contrôle de sécurité. Or, une telle approche nécessite de définir une quantité de trafic suffisante. Par ailleurs, les statistiques collectées ne seront pertinentes que pour cette application web spécifique.

Une approche légèrement différente consisterait à enregistrer une grande quantité de trafic légitime provenant d'autant d'API et d'applications web réelles que possible, et d'une variété de sources (API back-end d'applications mobiles, sites web d'e-commerce, CRM, sites web marketing, etc.). Ce trafic légitime est ensuite repassé à travers le mécanisme de protection testé. Chaque alerte de sécurité déclenchée indique un faux positif, et chaque demande autorisée à atteindre l'application indique un vrai négatif.

Une fois les quatre facteurs déterminés, vous pouvez calculer le MCC et évaluer l'exactitude globale de la solution.

Notons toutefois que cette approche n'a rien de nouveau. En 2013, son créateur a développé un framework visant à tester l'exactitude des pare-feu d'applications web qu'il a présenté la même année lors de la conférence NYC OWASP.

Test d'exactitude : module Prisma Cloud WAAS

Pour notre test d'exactitude, nous avons collecté plus de 200 000 transactions HTTP légitimes à partir d'un ensemble diversifié d'applications web, de sites web et d'API web de premier plan. Nous avons également compilé plus de 5 000 vecteurs d'attaque web, couvrant toutes les catégories du top 10 de l'OWASP, et au-delà. Enfin, nous avons déployé le module WAAS et exécuté les scénarios.

Le MCC global obtenu pour le module Prisma Cloud WAAS était de **0,956**.

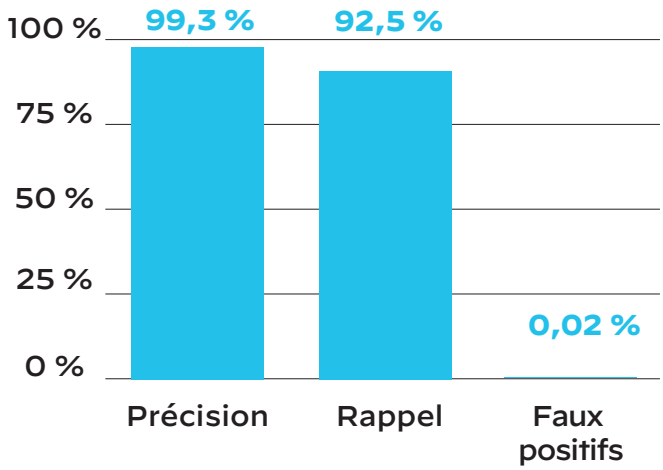

Figure 2. Module Prisma Cloud WAAS – précision, rappel et faux positifs

Comparatifs sectoriels

Bien que ces statistiques soient intéressantes, elles ne peuvent être véritablement pertinentes que si l'on compare le niveau d'exactitude du module à d'autres solutions leaders du secteur. En utilisant une méthodologie de test similaire, nous avons exécuté le même ensemble de tests sur six autres solutions :

- Deux solutions et services WAF (pare-feu d'applications web) leaders
- Un WAF open-source
- Deux WAF de CSP leaders
- Une solution RASP (autoprotection des applications au runtime)

Le Tableau 1 montre les résultats compilés, comparant le module Prisma Cloud WAAS aux autres solutions.

Tableau 1. Module Prisma Cloud WAAS comparé à des solutions connexes

Solution	Précision	Rappel	Faux positifs	MCC
Module Prisma Cloud WAAS	**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

Tableau 1. Module Prisma Cloud WAAS comparé à des solutions connexes (suite)				
Solution	**Précision**	**Rappel**	**Faux positifs**	**MCC**
WAF de CSP n° 1	57,6 %	83,5 %	2 %	0,681
WAF de CSP n° 2	61,4 %	91,3 %	0,85 %	0,729
Solution RASP	79,9 %	50,1 %	0,85 %	0,614

Prisma Cloud WAAS : une supériorité incontestable

Nous avons examiné la méthodologie optimale permettant de tester l'exactitude d'une solution de sécurité des applications web et des API. Grâce à nos analyses, nous avons compris qu'il est inutile de discuter de la rigueur d'une solution ou du nombre d'attaques qu'elle peut bloquer si l'on ne tient pas compte de son comportement vis-à-vis du trafic légitime et de son niveau de faux positifs. En utilisant la méthodologie de test présentée, nous avons comparé les statistiques du module Prisma Cloud WAAS à d'autres solutions de pointe. Les chiffres parlent d'eux-mêmes et démontrent clairement la supériorité de Prisma Cloud WAAS en termes d'exactitude.

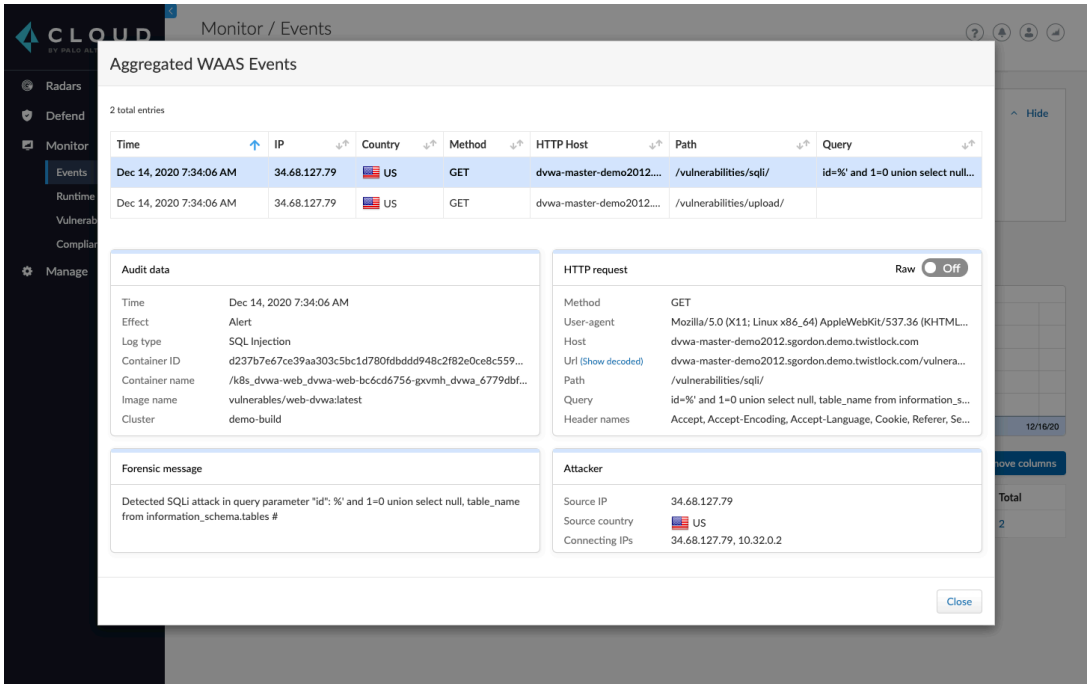

Figure 3. Détails d'audits WAAS agrégés dans Prisma Cloud

À propos de Prisma Cloud Palo Alto Networks

Prisma® Cloud est la plateforme de protection des applications cloud-native (CNAPP) la plus complète du marché. Sa mission : fournir une sécurité intégrée hors pair pour garantir la protection des environnements cloud et des applications cloud-native tout au long du cycle du développement et dans les environnements hybrides et multicloud.

Plutôt que de masquer les contraintes de sécurité autour des architectures cloud-native, une approche intégrée les élimine et brise les silos opérationnels sur l'ensemble du cycle de vie des applications. Les équipes DevSecOps/DevOps et de sécurité des applications peuvent ainsi automatiser leur protection pour répondre aux besoins en constante évolution des architectures cloud-native.

Pour en savoir plus, rendez-vous sur notre site web ou visionnez notre démo.

paloalto® NETWORKS | Cybersecurity Partner of Choice

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas

Téléphone : +31 20 888 1883
www.paloaltonetworks.fr

prisma_wp_raising-the-bar_031422-fr