Rohde & Schwarz Cybersecurity

MANAGEMENT CONSOLE

Configuration, gestion et surveillance centralisées des instances dans R&S®Web Application Firewall

Bien souvent, les entreprises n'ont pas une vision claire sur ce qui se passe dans leur système. Elles ont besoin d'informations actualisées, comme des données en temps réel sur toute attaque qui aurait pu se produire. Les attaques de la couche application sont courantes en raison de la surface d'attaque massive de la couche 7. Par conséquent, cette couche OSI doit être surveillée de manière très précise et en temps réel. Les entreprises éprouvent des difficultés à suivre les messages des logs et leur flux. Soucieux de la sécurité de leurs données, les administrateurs veulent pouvoir configurer, gérer et appliquer de manière centralisée des politiques de sécurité cohérentes. La console de gestion centralisée est une solution unifiée, facile à déployer dans le cloud, qui permet de gérer de manière très simple tous les aspects administratifs des instances des utilisateurs.

Aperçu des solutions

La console de gestion fait partie intégrante de R&S®Web Application Firewall, utilisé pour mettre en œuvre et superviser les politiques de sécurité déployées de manière centralisée.

Elle synchronise les configurations sur les serveurs gérés avec des politiques de sécurité centralisées évitant ainsi de configurer un workflow distinct pour chaque application. Elle bénéficie d'un workflow générique pour toutes les instances du pare-feu applicatif Web. La console fournit également des tableaux de bord, des fonctions d'investigation et des traitements de logs hors des boîtes de production. Elle permet la collecte, le stockage, l'analyse et de la corrélation d'un très grand nombre de logs et d'événements. L'analyse des logs fournit des informations sur tout comportement ou erreur inattendu. En outre, les tableaux de bord fournissent des vues personnalisées aux différents utilisateurs pour analyser les performances de leurs composants. La console de gestion permet d'administrer en temps réel une ou plusieurs instances du pare-feu d'application web et permet des déploiements souples et hybrides. Toutefois, son principal avantage est de rassembler toutes les fonctionnalités mentionnées ci-dessus dans une interface centralisée pour la gestion de R&S®Web Application Firewall. Cela permet de réduire les tâches répétitives et les coûts opérationnels en économisant ainsi du temps et des ressources.

Tableau de bord de la sécurité

ROHDE&SCHWARZ

Make ideas real

Avantages

Centraliser

- Gestion aisée de toutes les applications protégées par R&S®Web Application Firewall

  Au sein des environnements hétérogènes, le monitoring des règles de sécurité et leur application homogène sont pilotés à partir d'une plateforme centralisée. Cette approche permet une mutualisation des coûts sur l'ensemble des clients. Les règles de sécurité, les exceptions ainsi que la mise en log des évènements sont gérées de manière centralisée.

- Intégration d'un pare-feu d'application Web dans un framework DevSecOps à l'aide de l'orchestration API et Terraform

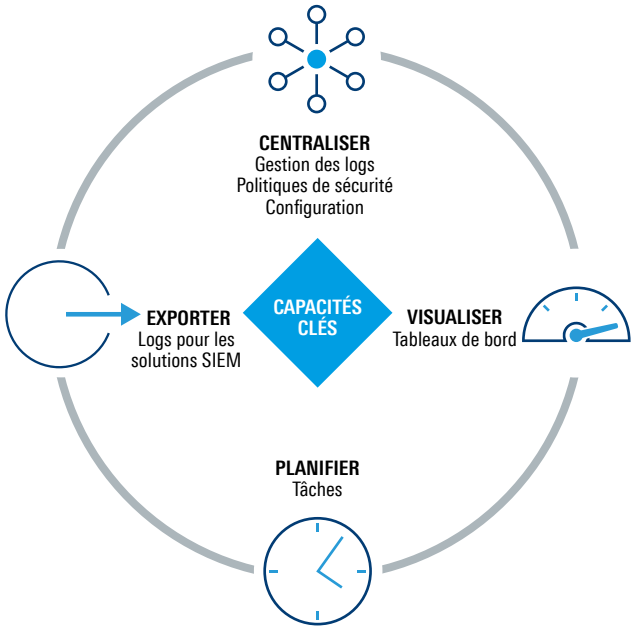
  Le déploiement et la configuration des infrastructures sont automatisés pour aider les utilisateurs à mettre en œuvre des modèles Terraform selon une approche Infrastructure as Code. Les gains de temps sont au rendez-vous par rapport aux méthodes manuelles des équipes IT traditionnelles.

- Administration de toutes les instances

  La console d'administration permet de gérer efficacement les déploiements hybrides (sur site + cloud) grâce à une gestion centralisée de toutes les instances du pare-feu applicatif par les administrateurs. Cette approche permet d'affecter une application à une nouvelle instance en quelques clics (pré-production à production par exemple). D'autre part, chaque instance managée est autonome, ce qui évite les risques associés à un point unique de défaillance (SPOF).

- Gestion des performances des applications en production par une plateforme dédiée à l'administration

  Les fonctions d'administration et de supervision sont dissociées du trafic associé aux applications en production. Cette séparation logique des tâches définit un système robuste qui permet d'assurer que la protection du trafic n'est jamais compromise. La console de gestion gère les opérations qui consomment le plus de ressources, ce qui permet de maximiser les performances des instances en production.



Capacités clés

Visualiser

- Tableau de bord et plate-forme web de reporting personnalisables et avancés

  La console fournit des tableaux de bord complets pour que les administrateurs visualisent rapidement et facilement l'état opérationnel de leurs systèmes. Ces tableaux de bord incluent des informations sur les attaques et le trafic web bloqués, l'identification des sites les plus ciblés, le temps de réponse, les erreurs et les logs d'événements, ce qui permet une gestion avancée de leur niveau de sécurité.

Planifier

- Tâches de gestion répétitives et longues

  La console permet de programmer des tâches automatisées sur les boîtes, telles que l'exportation de logs et l'exécution de sauvegardes vers des systèmes de fichiers externes. Il en résulte un système autonome qui fonctionne avec peu d'intervention manuelle.

Exporter

- Logs vers les solutions SIEM ou visualisation dans la console

  Elle permet d'exporter des logs vers les solutions SIEM afin de répondre aux exigences de leur organisation en matière de sécurité et d'analyse. Cela les aide à détecter les menaces et d'analyser les événements de sécurité critiques en utilisant des capacités avancées.

Rohde&Schwarz Cybersecurity SAS
Parc Tertiaire de Meudon
9-11 Rue Jeanne Braconnier | 92366 Meudon, France
Info: +33 (0)1 46 20 96 00
Email: sales-fr.cybersecurity@rohde-schwarz.com

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Allemagne
www.rohde-schwarz.com/cybersecurity

PD 5214.7270.33 | Version 01.00 | janvier 2021 (sch)
Management Console
Données sans tolérance : sans obligation | Sous réserve de modification

5214727033

5214.7270.33 01.00 PDP 1 fr