Q-OSSEC®

L'appliance réseau **Q-OSSEC**® (Open Source HIDS [Système de détection d'intrusion hôte] SECURE) est un moniteur autonome de toutes les activités du système 'Nix, y compris la surveillance du système de fichiers, la surveillance du journal, la vérification des traitements et la surveillance des processus. L'appliance de réseau **Q-OSSEC** fournit également une détection complète d'intrusion basée sur l'hôte dans Windows, Linux, Solaris, AIX, HP-UX, MAC et VMWare ESX. L'appliance de réseau **Q-OSSEC** est destinée à compléter les autres appareils de sécurité réseau de Quantalytics afin de fournir une meilleure défense en profondeur du réseau. Cependant, l'appliance réseau Q-OSSEC peut être utilisée de manière autonome. Il est idéal pour les réseaux PoS (point de vente). L'appliance réseau **Q-OSSEC** peut inspecter les réseaux PoS pour la conformité PCI DSS 1.2 / 2.0, ainsi que surveiller les modifications non autorisées du système de fichiers et alerter les administrateurs s'il en existe. L'appliance de réseau Q-OSSEC fournit également une analyse des fichiers journaux des produits COTS («Commercial Off-The-Shelf»).

Un bref résumé de chaque colis est ci-dessous. Nous vous encourageons à consulter notre site Web, www.quantalytics.com, pour obtenir une explication plus complète des fonctionnalités de chaque paquet.

Spécifications matérielles Q-OSSEC:

- 108mm x 64mm x 26mm – 170 grammes (4.25" x 2.50" x 1.125" – 6 oz)
- Consommation électrique à pleine charge: 8 watts, 120v-240v
- Pas de ventilateur ou de pièces mobiles. Doit être installé dans un espace bien ventilé.
- Fonctionne de 0°C à 70°C (32°F−158°F)

Indicateurs LED:

- Pouvoir électrique
- Lien (connexion physique au réseau)
- Activité (trafic réseau)
- 1000 mbps (gigabit) NIC connexion
- WiFi Bi-Bande. (2.4 GHz et 5 GHz)

Le système de réseau **Q-OSSEC** comprend:

- **OSSEC** - **OSSEC** («**O**pen **S**ource **Sec**urity») est un système de détection d'intrusion («IDS») open source, basé sur l'hôte, qui effectue l'analyse du journal, la vérification de l'intégrité du fichier, la détection des rootkits et la surveillance des politiques, puis fournit des alertes en temps réel. **OSSEC** comprend également des fonctions de réponse active pour une utilisation après une alerte grâce à ses composants de sécurité et de gestion des événements (SIE / SIM). L'alerte se fait par courrier électronique et syslog. Les journaux peuvent être exportés vers le **Q-Log**® ou tout autre système syslog ou SIEM. OSSEC fournit une détection d'intrusion pour les systèmes exécutant Windows, Mac, Linux, Solaris, AIX, HP-UX, BSD et VMware ESX.

OSSEC permet également aux administrateurs de réseau de vérifier et de certifier la conformité PCI DSS 1.2 / 2.0, ce qui est essentiel pour sécuriser les réseaux de point de vente («PoS») qui acceptent les cartes de crédit.

- **ntopng – ntopng** ("**ntop next generation**") est la dernière itération de ntop, utilisée pour sonder tout le trafic réseau. Certaines de ses fonctionnalités comprennent: afficher le trafic réseau en temps réel et les hôtes; créer des rapports à long terme pour le débit réseau, les applications et les protocoles d'application; surveiller et consigner le débit en temps réel, les latences du réseau et des applications, les RTT et les statistiques TCP complètes; découvrir les protocoles d'application

Contact: Richard Avery
+1 646-449-7810
Q-OSSEC@quantalytics.com

Quantalytics. Défenses de réseau en profondeur.

(Facebook, BitTorrent, etc.) en utilisant nDPI (ntop Deep Packet Inspection); caractériser le trafic HTTP à l'aide des services de caractérisation fournis par Google et la liste noire HPPT; fournir une cartographie de géolocalisation des hôtes; triez tout le trafic réseau selon des critères tels que l'adresse IP, le port, le protocole L7, le débit, les systèmes autonomes (AS); analyser le trafic IP et trier par source et destination; Prise en charge IPv6; prise en charge complète de la couche 2, y compris les statistiques ARP; et un moteur d'alertes pour capturer les hôtes anormaux et suspects.

- **Webmin - Webmin** est utilisé pour l'entretien ménager des réseaux et la configuration du réseau.
- **HA Proxy – HA Proxy** est le premier fournisseur open source pour le basculement automatique et l'équilibrage de charge. Jusqu'à 32 appareils de réseau **Q-OSSEC** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement grands. L'administration se fait via un web gui.
- **ModSecurity® – ModSecurity®** («**ModSec**») est le premier package de protection contre les attaques du serveur Web Apache. **ModSec** est utilisé pour endurer le serveur web Apache intégré de l'appliance **Q-OSSEC** et éviter les attaques imaginables.
- **Tiny Honeypot («THP») - THP** trompe les attaquants en faisant apparaître que l'attaque fonctionne, tout en enregistrant les informations d'attaque. **THP** gaspille le temps d'un attaquant et crée l'opportunité de détecter l'intrusion du réseau en offrant à l'attaquant ce qui semble être des milliers de services.
- **ClamAV®** – **ClamAv®** est le premier package antivirus open source.

L'appliance de réseau **Q-OSSEC** possède possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Dual Band 802.11 (2.4 GHz & 5 GHz). La détection d'intrusion peut être configurée sur les deux interfaces réseau.

L'appliance réseau **Q-OSSEC** est également disponible en tant que Machine Virtuelle («VM»).

L'appliance réseau **Q-OSSEC** est complètement administrée via une interface graphique Web. L'utilisation de tous les packages se fait via des interfaces Web, ouvrant ainsi une détection d'intrusion sophistiquée, une analyse légale en réseau et une surveillance de réseau même aux administrateurs réseau novateurs. Aucune interface de ligne de commande («CLI») ou Linux n'est requise.

En utilisant le module **Webmin** fourni, l'authentification à deux facteurs peut être ajoutée à l'aide de **Google Authenticator** ou **Authy**, un service commercial avec sa propre application. **Google Authenticator** s'exécute sur les appareils Android, IOS et Blackberry, et utilise le protocole standard de TOTP.

Les notifications sont fournies par e-mail à l'aide de **SendMail**, qui est configuré avec un module dans **Webmin** et les entrées syslog. L'appliance de réseau **Q-OSSEC** peut être intégré à **Nagios®** sur le **Q-Box®** comme autre voie de notification. La notification par SMS est disponible en option. L'appliance de réseau **Q-OSSEC** peut également être intégré au **Q-Log®** ou à toute autre solution Syslog ou SIEM.

Contact: Richard Avery
+1 646-449-7810
Q-OSSEC@quantalytics.com