Quantalytics

Q-Box®

Le **Q-Box®** est une amalgame d'un certain nombre de logiciels open source fonctionnant sur un facteur de forme extrêmement petit, un serveur à faible consommation d'énergie. Il fournit la sécurité du système grâce à la surveillance des périphériques réseau et des services, combinée à la détection et à la prévention des intrusions - création dans un seul périphérique, ce qui est généralement fourni avec deux serveurs "pizza box" de 1U. Ce design ultra compact permet des options de déploiement exceptionnellement flexibles et créatives, ainsi que d'importantes économies d'électricité et d'espace.

Q-Box Characteristiques:

- 108 mm x 64 mm x 26 mm – 170 grammes (4.25" x 2.50" x 1.125" – 6 oz)
- Consommation maximale en pleine charge: 12 watts, 120v-240v
- Pas de ventilateur ou de pièces mobiles. Doit être installé dans un espace bien ventilé.
- Fonctionne 0°C–70°C (32°F–158°F)

LED indicators:

- Pouvoir électrique
- Lien (connection physique au réseau)
- Activité (traffic réseau)
- 1000 mbps (gigabit) NIC connexion
- WiFi Double Bande. (2.4 GHz & 5 GHz)

Le **Q-Box** comprend:

- **Snort® – Snort®** est la principale solution open source, de classe enterprise, système de détection et de prévention des intrusions réseau (IDS/IPS). **Snort** est surveillé par **Nagios**. Une solution Syslog ou SEIM peut également être utilisée pour la surveillance.
- **Nagios® – Nagios®** est la principale solution open source, de classe d'enterprise, de surveillance de réseau et d'alerte. L'implémentation de **Nagios** inclut la surveillance **ModBus** et l'alerte pour les périphériques IoT prenant en charge **ModBus**.
- **NagiosQL® – NagiosQL®** est la principale solution open source, de classe enterprise, ensemble de configuration Web GUI pour **Nagios**. NagiosQL prend en charge toutes les définitions d'objet Nagios connues, ce qui permet aux administrateurs de personnaliser facilement Nagios pour leurs réseaux.
- **Nagios Bulk Import («NBI») – NBI** est le package le chef d'open source, qui, combiné avec **NMap**, automatise l'inventaire complet des objets réseau, y compris les périphériques réseau et les services. Le **NBI** est accessible en utilisant **Webmin**.
- **NMap – NMap** est le principal package de cartographie réseau open source pour l'inventaire des réseaux et l'audit de sécurité.
- **Xplico – Xplico** est la principale solution open source pour la capture de pacquets en réseau en temps réel et l'analyse médico-légate. Dans le cas où **Snort** affiche une activité suspecte, les administrateurs réseau peuvent capturer et examiner en profondeur du trafic en temps réel pour une analyse plus approfondie du trafic réseau suspect. En plus de l'inspection des paquets, **Xplico** permet la reconstruction du trafic réel. E.G. E-mails, texts, IM's, pictures, etc.
- **ntop-ng** – **ntop-ng** ("**ntop next generation**") est la dernière itération de ntop, utilisée pour sonder tout le trafic réseau. Certaines de ses caractéristiques comprennent le trafic réseau en temps réel et les hôtes; créer des rapports à long terme pour le débit du réseau, les protocoles d'application et d'application; surveiller et signaler le débit en direct, les latences de réseau et d'application, le RTT et les statistiques TCP complètes; découvrir les

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

Quantalytics. Défenses de réseau en profondeur.

protocoles d'application (par exemple Facebook, BitTorrent, etc.) en exploitant nDPI (ntop Deep Packet Inspection); caractériser le trafic HTTP en utilisant les services de caractérisation fournis par Google et HPPT Blacklist; fournir une cartographie de géolocalisation des hôtes; trier tout le trafic réseau via des critères incluant l'adresse IP, le port, le protocole L7, le débit, les systèmes autonomes (AS); analyser le trafic IP et trier par source et destination; Support 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.

- **ModSecurity® – ModSecurity®** («**ModSec**») est le principal pare-feu d'applications Web («WAF») open source pour la protection contre les attaques par script croisé. Nous avons durci le serveur Web Apache intégré du **Q-Box** pour éviter les attaques.
- **ClamAV® – ClamAV®** est le principal logiciel antivirus open source.
- **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.
- **Webmin – Webmin** est le premier paquet GUI Web open source pour la configuration et la maintenance du serveur. **Webmin** permet également la liaison de plusieurs appareils **Q-Box** pour une administration simplifiée.
- **HA Proxy – HA Proxy** est le premier fournisseur open source pour le basculement automatique et l'équilibrage de charge. Jusqu'à 32 appareils **Q-Box** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement grands. L'administration se fait via une interface graphique Web.

Le **Q-Box** possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Dual Band 802.11. (2.4 GHz et 5 GHz.) La détection d'intrusion peut être configurée sur l'une ou l'autre des interfaces réseau.

Le **Q-Box** est également disponible en tant que Machine Virtuelle (VM).

Le **Q-Box** est entièrement administré via une interface graphique Web. L'utilisation de tous les packages se fait via des interfaces Web, ouvrant ainsi une détection sophistiquée des intrusions, une analyse légal du réseau et une surveillance du 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. **Snort** a été intégré à **Nagios®** dans le **Q-Box** comme un itinéraire de notification. La notification par SMS est disponible en option. Le **Q-Box** peut également être intégré à l'appliance réseau **Q-Log®** ou à toute autre solution Syslog ou SIEM ("Security Information and Event Management").

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