Q-DLP®

Le **Q-DLP**® (Data Loss Prevention) est un outil indépendant et dédié de prévention des pertes de données (DLP), utilisant **OpenDLP**, l'un des logiciels les plus avancés de prévention des pertes de données disponibles aujourd'hui. En plus de la prévention des pertes de données, le **Q-DLP** comprend des outils pour tenter de modifier les fichiers. Nous avons également inclus **BRO-IDS**, un outil de détection d'intrusion, et **Brownian**, une interface graphique Web pour **BRO-IDS**. Le **Q-DLP** est destiné à compléter les autres appareils de sécurité du réseau Quantalytics afin de fournir une plus grande défense du réseau en profondeur. Toutefois, le **Q-DLP** peut être utilisé sur une base autonome. Il est idéal pour les réseaux PoS (Point de Vente).

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

*Spécifications matérielles **Q-DLP**:*

- 108 mm x 64 mm x 26 mm – 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 0°C–70°C (32°F–158°F)

Indicateurs LE:

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

Le **Q-DLP** comprend:

- **OpenDLP** - **OpenDLP** (Open Data Loss Prevention) est un outil de prévention de perte de données distribué de manière ouverte et centralisée. Il fonctionne à la fois agent et agent-moins. Avec les informations d'identification Windows, UNIX, MySQL ou MSSQL appropriées, **OpenDLP** peut identifier simultanément des données sensibles au repos sur des centaines, voire des milliers de systèmes Microsoft Windows, des systèmes UNIX ou des bases de données MySQL ou MSSQL. Il utilise une interface de gestion Web centralisée. Les données sensibles peuvent être des numéros de cartes de crédit, des numéros de sécurité sociale ou toute autre donnée sensible à l'utilisateur.

  OpenDLP se compose de deux composants: (1) Une application Web pour gérer les agents Windows plus les scanners sans bases de données Windows et UNIX. (2) Un agent Microsoft Windows pour effectuer des analyses accélérées sur plusieurs milliers de systèmes simultanément.

En raison du jeu de fonctionnalités extraordinairement riche d'**OpenDLP** et de l'interface avec **Q-Log**® pour l'analyse de journal, nous vous recommandons de visiter notre site Web à www.quantalytics.com pour une description beaucoup plus détaillée.

- **Bro-IDS** – **Bro-IDS** est à la fois un paquet d'IDS de signature et d'anomalie. **Bro-IDS** examine tous les événements réseau (par exemple, FTP, HTTP), puis, en utilisant son Interprète de Script de Politique, donne un aperçu de la légitimité des événements. **Bro-**

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

Quantalytics. Défenses de réseau en profondeur.

IDS comprend Bro-Script, son propre outil de script, pour créer des règles et des analyses personnalisées. **Bro-IDS** s'interface avec le **Q-Log®** pour la surveillance et l'analyse de ses journaux de détection d'intrusion.

- **Brownian** – **Brownian** est l'interface Web de **Bro-IDS**.
- **Xplico** - **Xplico** est un paquetage open source leader pour la capture en paquets en réseau en temps réel et forensicune analyse. Dans le cas où **Bro-IDS** montre une activité suspecte, les administrateurs réseau peuvent capturer et examiner en profondeur le 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. PAR EXEMPLE: E-mails, textes, IM, images, etc.
- **Webmin - Webmin** est utilisé pour l'entretien ménager des réseaux et la configuration du réseau. **Webmin** permet également le couplage de plusieurs appliances **Q-DLP** 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 serveurs **Q-DLP** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement grands. L'installation et l'administration se font via **Webmin**.
- **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-DLP** pour éviter les attaques concevables.
- **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 anti-virus open source.

Le **Q-DLP** dispose à la fois d'une NIC Gigabit (1000 Mbits/s) 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.

Il est également disponible en tant que Machine Virtuelle (VM).

Le **Q-DLP** est complètement 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 forensale 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. L'appliance de réseau **Q-DLP** 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-DLP** peut également être intégré au **Q-Log®** ou à toute autre solution Syslog ou SIEM (Security Information and Event Management).

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