Q-IDS®

Le **Q-IDS®** est un système de détection d'intrusion ultra-faible (IDS) autonome et ultramoderne qui comprend deux des principaux logiciels de détection d'intrusion disponibles aujourd'hui. **Suricata** est disponible pour IDS filaire, et **Kismet**, pour WiFi. Chacun inclut une interface graphique Web. Aucune expérience Linux ou Command Line Interface ("CLI") n'est nécessaire pour utiliser l'un de ces outils IDS, ce qui permet d'ouvrir un niveau plus large de protection du réseau aux entreprises et aux organisations qui, autrement, ne disposeraient pas des compétences internes nécessaires à l'utilisation réussie d'un système IDS, ainsi que fournir un niveau de protection plus profond et plus approfondi pour les entreprises et les organisations qui utilisent déjà un système de détection d'intrusion.

En plus de la détection d'intrusion, le **Q-IDS** inclut **Xplico**, une capture de paquets et un outil d'analyse forensique pour les paquets suspects, y compris la reconstruction de messages complets, des chats, etc.

Nous avons également inclus **DDoS-Deflate** pour réduire automatiquement et atténuer les attaques DDoS.

Notre conception ultra compacte permet des options de déploiement exceptionnellement flexibles et créatives, ainsi que des économies importantes d'électricité et d'espace.

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.

***Q-IDS** Spécifications matérielles:*

- 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: 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)

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 **Q-IDS** inclut:

- **Suricata** – **Suricata** est un système de détection d'intrusion (IDS) de classe entreprise open source. **Suricata** est un IDS multi-thread et IPS haute performance (Système de Prévention des Intrusions «Intrusion Detection System» qui utilise 2 ensembles de règles, le jeu de règles Suricata de menaces émergentes spécialisées et le jeu de règles VRT. Il comprend également LuaJIT ("LUA"), un langage de script et un moteur pour une analyse et une fonctionnalité supplémentaires, y compris des règles de détection personnalisées pour les éléments qui ne sont pas «vus» par les jeux de règles fournis et «EVE», un événement JSON et un outil de sortie d'alerte. Il est intégré à **Logstash** (voir ci-dessous) pour faciliter l'analyse et l'alerte des journaux.
- **Logstash** - **Logstash** est un outil open source leader pour gérer les événements et les journaux. **Logstash** collecte des journaux, les analyse et les stocke pour une utilisation ultérieure via un outil de recherche Web intégré. **Logstash** est également intégré avec **Suricata** pour tirer parti de son utilité pour les administrateurs réseau. Les journaux sont beaucoup plus faciles à examiner pour un comportement de réseau anormal lorsqu'il est traité par **Logstash**.
- **Kismet** - **Kismet** est un détecteur de réseau 802.11 Layer 2 sans fil (wifi), un détecteur de sniffer et un système de détection d'intrusion. **Kismet** peut renifler le trafic 802.11 a / b / g / n. Il contient également un plugin pour renifler d'autres médias, y compris DECT. Kismet recueille passivement le trafic réseau et peut détecter, compte tenu du temps et de la circulation suffisants, des réseaux cachés et peut déduire la présence de réseaux de non-balisage à partir du trafic de données.

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

Quantalytics. Défenses de réseau en profondeur.

- **Kismon** – **Kismon** est un client de gui pour Kismet. En utilisant **Kismon**, les administrateurs obtiennent ce qui suit: une carte en direct des réseaux; Importation de fichier: netxml (**Kismet**), csv (ancienne version de **Kismet**), json (kismon); Export de fichiers: kmz (Google Earth) et tous les formats d'importation; Un graphe de signal pour chaque réseau wifi. **Kismon** peut se connecter simultanément à plusieurs serveurs **Kismet**.
- **Xplico - Xplico** est un package open source leader pour la capture de paquets en réseau en temps réel et l'analyse médico-légale. Dans le cas où **Suricata** montre 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. Par Exemple: E-mails, textes, IM, images, etc.
- **DDoS-Deflate** – **DDoS-Deflate** est un outil open source pour atténuer et réduire les attaques de déni de service distribué (DDoS). Les adresses IP des serveurs d'attaque sont bloquées pendant 10 minutes, puis automatiquement débloquées. De même, le blocage se fait par état de connexion. Ceci automatise la réduction de DDoS pour toutes les attaques DDoS de Niveau 7 (Level 7).
- **ModSecurity®** – **ModSecurity (ModSec)** est est le principal Pare-Feu Applicatif Web (WAF) open source pour la protection contre les attaques par script croisé. Nous avons durci le serveur Web Apache intégré du **Q-IDS** pour éviter les attaques concevables.
- **ClamAV®** – **ClamAv** est le premier package 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 fournisseur open source pour la configuration et la maintenance du serveur. Il utilise un web gui. **Webmin** permet également la liaison de plusieurs appareils **Q-IDS** 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-IDS** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement importants. L'administration se fait via un web gui.

Le **Q-IDS** 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.

Le **Q-IDS** possède possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Bi-Bande 802.11 (2.4 GHz & 5 GHz). La détection d'intrusion peut être configurée sur les deux interfaces réseau. Les deux peuvent être actifs en même temps.

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

Le **Q-IDS** 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-IDS** 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-IDS@quantalytics.com

Quantalytics. Défenses de réseau en profondeur.