Q-OSSEC®

El dispositivo de red **Q-OSSEC**® ("Open Source HIDS [Host Intrusion Detection System] SECurity") de HIDS es un monitor independiente de toda la actividad del sistema 'Nix, incluyendo monitoreo del sistema de archivos, monitoreo de registro, comprobación de rootkit y monitoreo de procesos. El dispositivo de red **Q-OSSEC** también proporciona una detección completa de intrusos basada en host en Windows, Linux, Solaris, AIX, HP-UX, MAC y VMWare ESX. El dispositivo de red **Q-OSSEC** está destinado a complementar los otros dispositivos de seguridad de red de Quantalytics para ayudar a proporcionar una mayor defensa en profundidad de la red. Sin embargo, el dispositivo de red **Q-OSSEC** puede utilizarse de forma autónoma. Es ideal para redes PoS (Point of Sale). El dispositivo de red **Q-OSSEC** puede inspeccionar las redes PoS para el cumplimiento PCI DSS 1.2 / 2.0, así como supervisar las modificaciones no autorizadas del sistema de archivos y los administradores de alertas si se producen. El dispositivo de red **Q-OSSEC** también proporciona análisis de archivos de registro de los productos COTS (comerciales fuera de la plataforma; "Commercial Off-The-Shelf").

A continuación se muestra un breve resumen de cada paquete. Le animamos a ir a nuestro sitio web, www.quantalytics.com, para una explicación más completa de las características de cada paquete

*Especificaciones de Hardware **Q-OSSEC**:*

- 108 mm x 64 mm x 26 mm – 170 gramos (4.25" x 2.50" x 1.125" – 6 oz)
- Consumo de energía a plena carga: 12 watts, 120v-240v
- No hay ventilador ni ninguna pieza móvil. Debe instalarse en un espacio bien ventilado.
- Funciona de 0°C a 70°C (32°F–158°F)

Indicadores LED:

- Energia electrica
- Enlace (conexión física a la red)
- Actividad (tráfico de red)
- Conexión de NIC de 1000 mbps (gigabit)
- WiFi de Banda Dual. (2.4 GHz & 5 GHz)

El **Q-OSSEC** incluye:

- **OSSEC** - **OSSEC** ("Open Source Security") es un sistema de detección de intrusos (IDS) basado en host, que realiza análisis de log, comprobación de integridad de archivos, detección de rootkit y monitoreo de políticas y proporciona alertas en tiempo real. **OSSEC** también incluye funciones de respuesta activa para su uso después de una alerta a través de sus componentes de Información de Seguridad y Gestión de Eventos (SIE / SIM). La alerta se realiza a través del correo electrónico y syslog. Los registros se pueden exportar al **Q-Log**® oa cualquier otro sistema Syslog o SIEM. **OSSEC** proporciona detección de intrusión para sistemas que ejecutan Windows, Mac, Linux, Solaris, AIX, HP-UX, BSD y VMware ESX.

OSSEC también permite a los administradores de red comprobar y certificar el cumplimiento de PCI DSS 1.2 / 2.0, que es esencial para asegurar las redes de puntos de venta (PoS) que aceptan tarjetas de crédito.

- **ntopng – ntopng** ("**ntop next generation**") es la última versión de ntop, que se utiliza para sondear todo el tráfico de red. Algunas de sus características incluyen: mostrar el tráfico de red

Contacto: Richard Avery
+1 646-449-7810
q-ossec@quantalytics.com

Quantalytics. Defensas de la red en profundidad.

en tiempo real y los hosts; crear informes a largo plazo para el rendimiento de la red, aplicaciones y protocolos de aplicación; supervise e informe el rendimiento en vivo, las latencias de red y de las aplicaciones, RTT y estadísticas TCP completas; descubra los protocolos de aplicación (por ejemplo, Facebook, BitTorrent, etc.) aprovechando nDPI (ntop Deep Packet Inspection); caracterizar el tráfico HTTP utilizando los servicios de caracterización proporcionados por Google y HPPT Blacklist; proporcionar mapeo geolocalización de hosts; clasifique todo el tráfico de la red a través de criterios que incluyen la dirección IP, el puerto, el protocolo L7, el rendimiento, los sistemas autónomos (AS); analizar el tráfico de IP y ordenar por fuente y destino; Soporte de IPv6; soporte completo de Capa 2, incluidas las estadísticas ARP; y un motor de alertas para capturar hosts anómalos y sospechosos.

- **Webmin - Webmin** es el principal paquete de GUI Web de código abierto para la configuración y el mantenimiento del servidor. **Webmin** también permite la vinculación de múltiples dispositivos **Q-IDS** para la administración simplificada.
- **HA Proxy – HA Proxy** es el paquete líder de código abierto para la conmutación automática y el equilibrio de carga. Se pueden conectar hasta 32 dispositivos **Q-OSSEC** para la conmutación automática o el equilibrio de carga para la cobertura de redes extremadamente grandes. La administración se realiza a través de una GUI Web.
- **ModSecurity® – ModSecurity®** (**ModSec**) es el principal paquete de protección contra ataques de scripts cruzados de código abierto para endurecer el servidor web Apache de **Q-OSSEC** y prevenir ataques concebibles.
- **Tiny Honeypot (THP) - THP** engaña a los atacantes haciendo que parezca que el ataque está funcionando, mientras que mientras registra la información de ataque. **THP** desperdicia el tiempo de un atacante y crea una oportunidad para detectar la intrusión de red ofreciendo al atacante lo que parece ser miles de servicios.
- **ClamAV®** – **ClamAV®** es el paquete de software antivirus de código abierto líder.

El dispositivo de red **Q-OSSEC** tiene un NIC Gigabit (1000 mbps) y WiFi 802.11 de Doble Banda. (2.4 GHz y 5 GHz). La detección de intrusos se puede configurar en cualquier interfaz de red.

El dispositivo de red **Q-OSSEC** también está disponible como una Máquina Virtual (VM).

El **Q-OSSEC** se administra completamente a través de una GUI Web. Todo el uso del paquete es a través de interfaces Web, lo que abre la sofisticada detección de intrusiones, análisis forense de red y supervisión de red incluso a los administradores de red novatos. No se requiere ninguna habilidad de interfaz de línea de comandos (CLI) o Linux..

Usando el módulo **Webmin** proporcionado, la autenticación de dos factores se puede agregar usando **Google Authenticator** o **Authy**, un servicio comercial con su propia aplicación. **Google Authenticator** se ejecuta en dispositivos Android, IOS y Blackberry y utiliza el protocolo TOTP estándar

Las notificaciones se proporcionan por correo electrónico utilizando **SendMail**, que está configurado con un módulo en **Webmin**, y las entradas de syslog. El dispositivo de red **Q-OSSEC** se puede integrar con **Nagios®** en el **Q-Box®** como otra ruta de notificación. La notificación por SMS está disponible como opción. El dispositivo de red **Q-OSSEC** también se puede integrar con el dispositivo de red **Q-Log®** o cualquier otra solución Syslog o SIEM. (Security Information and Event Management).

Contacto: Richard Avery
+1 646-449-7810
q-ossec@quantalytics.com