Q-OSSEC®

The **Q-OSSEC**® (Open Source HIDS [Host Intrusion Detection System] SECurity) network appliance is a stand-alone monitor of all 'Nix system activity, including file system monitoring, log monitoring, rootkit checking, and process monitoring. The **Q-OSSEC** network appliance also provides comprehensive host-based intrusion detection across Windows, Linux, Solaris, AIX, HP-UX, MAC, and VMWare ESX.

The **Q-OSSEC** network appliance is intended to complement the other Quantalytics network security appliances to help provide greater in-depth network defense. However, the **Q-OSSEC** network appliance may be used on a stand-alone basis. It is ideal for PoS (Point of Sale) networks.

The **Q-OSSEC** network appliance can inspect PoS networks for PCI DSS 1.2/2.0 compliance, as well as monitor for unauthorized file system modifications and alert administrators if any occur. The **Q-OSSEC** network appliance also provides log file analysis of COTS (Commercial Off-The-Shelf) products.

Q-OSSEC Hardware Specifications:

- 108 mm x 64 mm x 26 mm – 170 grams
  (4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load: 8 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

LED indicators:

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

The **Q-OSSEC** network appliance includes:

- **OSSEC** - **OSSEC** (Open Source Security) is an open source, host-based, intrusion detection system (IDS) which performs log analysis, file integrity checking, rootkit detection, and policy monitoring, and then provides real-time alerts. **OSSEC** also includes active response features for use after an alert through its Security Information and Event Management (SIE/SIM) components.

  Alerting is done through email and syslog. Logs can be exported to the **Q-Log**® or any other syslog or SIEM system. **OSSEC** provides intrusion detection for systems running Windows, Mac, Linux, Solaris, AIX, HP-UX, BSD, and VMware ESX.

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

Quantalytics. In-depth network defenses.

- **OSSEC** also allows network administrators to check for, and certify, PCI DSS 1.2/2.0 compliance, which is essential for securing Point-of-Sales (PoS) networks that accept credit cards.

- **Xplico - Xplicio** is a leading open source package for real time network packet capture and forensic analysis. In the event **OSSEC** shows suspicious activity, network administrators can capture and examine in depth real-time traffic for deeper analysis of suspicious network traffic. In addition to packet inspection, **Xplico** allows for reconstruction of the actual traffic. E.G. E-mails, texts, IM's, pictures, etc.

- **Webmin - Webmin** is used for network appliance housekeeping and network configuration. **Webmin** also allows for the linkage of multiple **Q-OSSEC** appliances for simplified administration.

- **HA Proxy – HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-OSSEC** network appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Administration is done through a web gui.

- **ModSecurity® – ModSecurity** (**ModSec**) is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. **ModSec** is used to harden the **Q-OSSEC** appliance's built-in Apache web server and prevent conceivable attacks.

- **Tiny Honeypot (THP) - THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.

- **ClamAV®** – **ClamAV®** is the leading open source anti-virus package.

The **Q-OSSEC** network appliance has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.)

The **Q-OSSEC** network appliance is also available as a Virtual Machine (VM).

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

Quantalytics. In-depth network defenses.

Q-OSSEC®

The **Q-OSSEC** network appliance is completely administered through a Web GUI. All package usage is via Web interfaces, thereby opening up sophisticated intrusion detection, network forensic analysis, and network monitoring to even novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Authy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured with a module in **Webmin**, and syslog entries. The **Q-OSSEC** network appliance can be integrated with **Nagios**® on the **Q-Box**® as another notification route. SMS notification is available as an option. The **Q-OSSEC** network appliance can also be integrated with the **Q-Log**® network appliance or any other Syslog or SIEM (Security Information and Event Management) solution.

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

Quantalytics. In-depth network defenses.