Quantalytics

Q-SOAR®

The **Q-SOAR®** **(Security Orchestration, Automation, and Response)** is an amalgamation of a number of open source software packages, listed below, running on an extremely small form factor, low-power-consumption server. The **Q-SOAR**, through its web gui, provides Security Orchestration, Automation, and Response (SOAR), which is the process of automating detection and response to security breaches, using **The HIVE**, a highly scalable, 4-in-1 open source Security Incident Response Platform. **The HIVE** seamlessly integrates with **MISP** (Malware Information Sharing Platform), the leading Threat Intelligence (TI) sharing platform. **The HIVE** also fully integrated with **CORTEX**, the open source and largest incident response community with over 13,642 members. **CORTEX** provides playbooks so **The HIVE** can automatically respond to cyber security incidents, including patching or shutting down infected network devices. There are literally thousands of open source off-the-shelf playbooks and incident responses available. **CORTEX** also includes the ability to create custom playbooks and automated incident responses.

- ***Q-SOAR 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:
  12 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-SOAR** includes:

- **The HIVE – The HIVE** is a Security Orchestration, Automation and Response (SOAR) system that aggregates a wide variety of inputs, including logs and warnings from SIEM systems, and through the use of pre-defined playbooks, can automatically take steps to contain and/or terminate the cyber security event. **The HIVE** can be synchronized with **MISP** seamlessly to start investigations from **MISP** events, or export to **MISP** to enable the MISP community to look at the investigation. **The HIVE** fully supports **CORTEX®** (see below), including all pre-defined response playbooks. When used with **CORTEX®**, **The HIVE** can analyze hundreds of observations simultaneously and automatically contain or remove malware far faster than any possible human intervention.
- **CORTEX® – CORTEX®** enables automatic alerting and through the use of either off-the-shelf or custom-designed playbooks, completely automate security responses throughout the enterprise. **CORTEX** enables **THE HIVE** to completely triage and ameliorate security threats, especially when integrated with **MISP** (Malware Intelligence Sharing Platform). For vetted customers, Quantalytics can provide a MISP feed from **CIRCL**, the EU's equivalent to the US's CISA and CERT. Please

inquire for subscription details.

- **ModSecurity® – ModSecurity®** ("**ModSec**") is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-Box**'s built-in Apache web server to prevent conceivable attacks.
- **ClamAV® – ClamAV®** is the leading open source anti-virus software package.
- **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.
- **Webmin – Webmin** is the leading open source Web GUI package for server configuration and maintenance. **Webmin** also allows for the linkage of multiple **Q-SOAR** appliances for simplified administration.
- **HA Proxy** – **HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-SOAR** appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Administration is done through a Web GUI.

The **Q-SOAR** is completely administered through a Web GUI. All package usage is via Web interfaces, thereby opening up sophisticated, automated cyber security analysis and remediation to even novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

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

The **Q-SOAR** is also available as a Virtual Machine (VM).

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. SMS notification is available as an option. The **Q-SOAR** can also be integrated with the **Q-Log**® network appliance or any other Syslog or SIEM (Security Information and Event Management) solution, including the **Q-OSSEC**®.

***Q-SOAR*®** *and all registered trademarks above are property of their respective owner(s).*

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