Q-IDS®

The **Q-IDS®** is a stand-alone, ultra-small-form-factor, ultra-low powered Intrusion Detection System (IDS) that includes two of the leading open source intrusion detection software packages available today.

Suricata is available for wired IDS, and **Kismet**, for WiFi. Each includes a web GUI. No Linux or Command Line Interface ("CLI") experience is needed to use either of these IDS tools, thereby opening up a deeper level of network protection to businesses and organizations who might otherwise lack the necessary internal skills for successful use of an IDS system, as well as providing a deeper, in-depth level of protection for businesses and organizations already using an Intrusion Detection System.

In addition to Intrusion Detection, the **Q-IDS** includes **Xplico**, a packet capture and forensic analysis tool for suspicious packets, including reconstructing entire messages, chats, etc.

We have also included **DDoS-Deflate** to automatically abate and mitigate DDoS attacks.

Our ultra-compact design permits exceptionally flexible and creative deployment options as well significant electricity and space savings.

Q-IDS 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)

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

Quantalytics. In-depth network defenses.

Quantalytics

Q-IDS®

The **Q-IDS** includes:

- **Suricata – Suricata** is a leading open source enterprise-class Intrusion Detection System (IDS). **Suricata** is a high performance multi-threaded IDS and IPS (Intrusion Prevention System) which uses 2 rule sets, the Specialized Emerging Threats Suricata Ruleset and the VRT Ruleset. It also includes LuaJIT, ("LUA"), a scripting language and engine for additional analysis and functionality, including custom detection rules for items not "seen" by the provided rulesets, and "EVE", a JSON event and alert output tool. **Suricata** is integrated with **Logstash** (see below) for easy log analysis and alerting.

- **Logstash - Logstash** is a leading open source tool for managing events and logs. **Logstash** collects logs, parses them, and stores them for later use via an integrated Web-based search tool. **Logstash** is also integrated with **Suricata** to leverage its usefulness for Network Admins. Logs are much easier to examine for anomalous network behavior when processed by **Logstash.**

- **Kismet - Kismet** is an 802.11 Layer 2 wireless (wifi) network detector, sniffer, and intrusion detection system. **Kismet** can sniff 802.11 a/b/g/n traffic. It also contains a plugin for sniffing other media, including DECT. **Kismet** passively collects network traffic and can detect, given sufficient time and traffic, hidden networks, and can infer the presence of non-beaconing networks from data traffic.

- **Kismon – Kismon** is a gui client for **Kismet**. Using **Kismon**, admins gain the following: a live map of the networks; file import: netxml (kismet), csv (old kismet version), json (kismon); file export: kmz (Google Earth) and all import formats; a signal graph for each wifi network. **Kismon** can connect to multiple **Kismet** servers simultaneously.

- **Xplico - Xplico** is a leading open source package for real time network packet capture and forensic analysis. In the event **Suricata** 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.

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

Quantalytics. In-depth network defenses.

- **DDoS-Deflate – DDoS-Deflate** is an open source tool to mitigate and abate Distributed Denial of Service (DDoS) attacks. IP addresses from attacking servers are blocked for 10 minutes, then automatically unblocked. Likewise, blocking is done by connection state. This automates DDoS abatement for all Level 7 DDoS attacks.

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

- **ClamAV® – ClamAv®** is the leading open source anti-virus 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 –** The leading open source Web GUI package for server configuration and maintenance.
  Webmin also allows for the linkage of multiple **Q-IDS** appliances for simplified administration.

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

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

Quantalytics. In-depth network defenses.

Quantalytics

Q-IDS®

The **Q-IDS** 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.

The **Q-IDS** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.) Intrusion detection can be set up on both network interfaces. Both can be active at the same time.

The **Q-IDS** 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.

Suricata and **Kismet** have been integrated with **Nagios®** in the **Q-Box®** as a notification route. SMS notification is available as an option. The **Q-IDS®** 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-IDS@quantalytics.com

Quantalytics. In-depth network defenses.