Overview for:
Power Generation & Transmission
IT (Information Technology)

Q-Box provides network monitoring and alerting, intrusion detection, a Web Application Firewall (WAF) for self-protection, and real time network packet capture and forensic analysis. The second unit provides fail-over and load balancing.

Q-Hpot honeypot is a decoy server used for network obfuscation, denying the attacker access to actual network data while giving the attacker 1,000's of false attack surfaces on the number and types of systems and services on the network.

Q-NAC is a comprehensive Network Access Control (NAC) appliance that provides authentication, compliance, IDS, device management, profiling and fingerprinting.

Q-Vul (Vulnerability Testing and Reporting) a scanning tool that can find and identify more than 47,000 security vulnerabilities in Windows, IOS, and Linux. It also can identify vulnerabilities in various network appliances, including routers, smart switches, and IoT devices.

Q-Log appliance provides full log collection and automated analysis for all devices and services on a network. It has 160 different log connectors and data transformation tools so that logs from all kinds of hardware and services can be aggregated, analyzed and reported.

Quantalytics appliances are designed to be used independently, or can be combined in packages to maximize cybersecurity effectiveness.
All images and controls are subject to change without notice.

IT Networks Cybersecurity for Power Generation and Transmission

Information Technology (IT) Networks in The Power Generation and Transmission industries are a special class of IT networks. They must be reliable, and ideally, un-hackable. Security is therefore paramount.

The disclosure in Wikileaks of the CIA's "Vault 7" on March 7, 2017, revealed that the CIA's entire hacking and data exfiltration tool collection had been stolen. Among the tools, beyond a wide number of 0 Day (Zero Day) exploits, are programs such as "Hammer Drill", which are designed to infect software distributed on CDs, DVDs, and USB thumb drives, which are some of the vehicles used to perform software and firmware upgrades for devices on IT networks.

As in our OT network protection, our guiding design philosophy is summed up as "Trust no one. Verify everything." We believe in providing transparency, and we believe in keeping a very close eye on everything in an IT Network.

To do this, we recommend the following Quantalytics appliances be used for IT networks:

Q-Box. The Q-Box provides monitoring of devices on the IT network, via Nagios, and intrusion detection via Snort. In the event a suspected intrusion is detected, the Q-Box has both xplico and ntop-ng for real time packet capture and forensic analysis.

Because of the critical importance of monitoring and intrusion detection, we recommend using two (2) Q-Boxes for auto-failover, and for load balancing as needed.

Q-Hpot. The Q-Hpot is a honeypot solution specifically for IT networks. A basic tenant of defense in depth is to camouflage the IT network assets so as to hide them from the attacker ("Network Obfuscation"). The Q-Hpot can create thousands of clones of objects in an IT network. The Q-Hpot mimics human activity. The only constraint is purely the number of IP addresses available to assign to each attack surface. By camouflaging and hiding the IT network assets, one shifts the odds in favor of the defender, as opposed to not camouflaging the IT network assets.

646-449-7810
info@quantalytics.com

Q-Vul. The Q-Vul is a vulnerability scanner built using OpenVAS. Even if there is no patch available, or worse, a patch but no time window available to apply it, the Q-Vul will let the IT Network's managers watch extra-carefully the vulnerable device or network service. While this can not prevent an attack, it provides a means to try to find work-arounds to block one, as well as knowledge of security weaknesses that management can use to press manufacturers to provide a fix.

Q-Log. The Q-Log is a log aggregation and reporting tool built using the ELK Stack (Elastic, Logstash, and Kirbana). Everything generates logs. The key is to isolate and report the critical issues quickly, and then to probe deeper as needed. The Q-Log makes it possible to process log data, and render alerts quickly when there is anomalous activity.

Q-NAC (Network Access Control). The Q-NAC, built with PacketFence, provides highly granular access control to the IT Network, and within it, to the various devices and network services. The Q-NAC provides complete audit trails in order to help quickly identify devices that have gone rogue, or are not allowed at all, such as a plugbot. (A plugbot is a small device plugged into a network, or wirelessly, connected, that creates a Command & Control ("C&C") back door.)

A device that has gone rogue means that it has been compromised, and is being controlled and used by the hackers. Most devices on IT Networks have no internal defenses whatsoever against being compromised. Compared to the power of today's hacking tools, the lack of internal defenses makes them very, very easy to compromise. These devices include, for example, All-in-One printers, and a huge variety of IoT devices that are found on IT networks such as IP Cameras and DVRs used in surveillance systems.

All Quantalytics appliances are internally hardened against hackers as an additional precaution. Among the steps we have taken are deploying ModSecurty, a Web Application Firewall, TinyHoneyPot for internal obfuscation, Fail2ban to block brute force login attempts, IPTables, and ClamAV for anti-virus protection. Two-factor authentication is available as an option.

646-449-7810
info@quantalytics.com