Overview for Power: Generation & Transmission OT (Operations Technology)

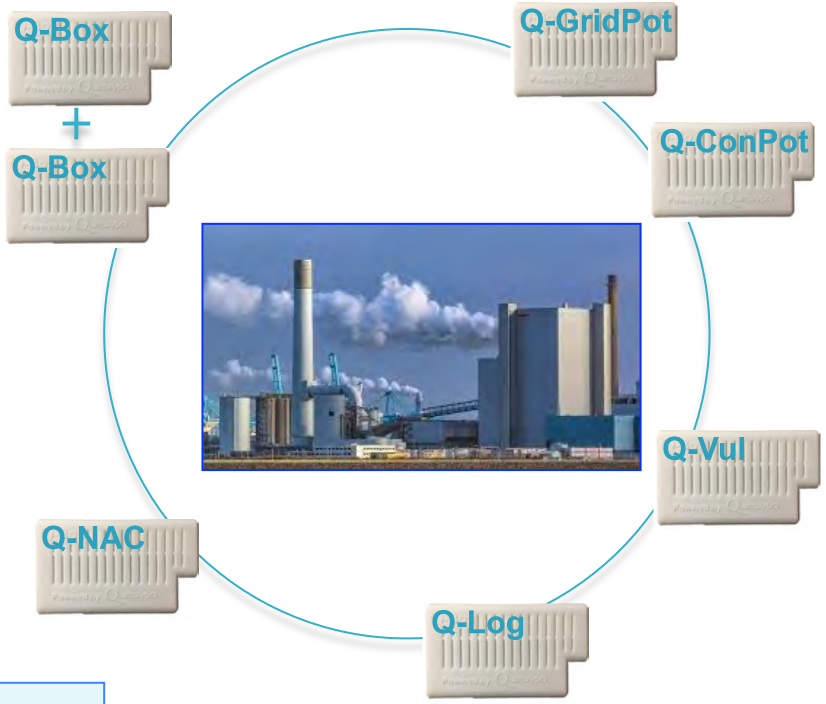
(For Power Transmission)*

Q-GridPot is a decoy which can present 1,000's of false attack surfaces. The Q-GridPot is a network appliance specifically designed for the power transmission industry. It mimics the actual operational appearance of a human operating the power grid.

(For Power Generation)*

Q-ConPot (Control System HoneyPot) is a decoy which can present 1,000's of false attack surfaces. The Q-ConPot is specifically designed to be used to protect Industrial Control Systems (ICS) and SCADA systems. It mimics the actual operational appearance of a human operating the power facility. These are used to monitor and control a plant and its equipment.

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

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

*Product packages for Transmission and Generation are identical with the exception of the use of Q-GridPot or Q-ConPot

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.

OT Networks Cybersecurity for Power Generation & Transmission

Operational Technology Networks in power plants are a special class of Internet of Things (IoT) networks. They must be reliable, and ideally, un-hackable. Keeping them air-gapped is, unfortunately, only a partial solution towards protecting them from being hacked. Security is therefore paramount.

There is always room for human error, and human malevolence.

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, the vehicles used to perform software and firmware upgrades for devices on OT networks.

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

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

Q-Box. The Q-Box provides monitoring of devices on the OT network, including ModBus, via Nagios, and intrusion detection via Snort. In the event a suspected intrusion is detected, the Q-Box has 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 load balancing as needed.

Q-ConPot. (For Power Generation Facilities) The Q-ConPot is a honeypot solution specifically for OT networks. A basic tenant of defense in depth is to camouflage the OT network assets from the attacker ("Network Obfuscation"). The Q-ConPot can create thousands of clones of the OT network, including HIDs (Human Interface Devices) for complete verisimilitude. The only constraint is purely the number of IP addresses available to assign to each attach surface. The Q-ConPot mimics human activity. By camouflaging and hiding the OT Network assets, one shifts the odds in favor of the defender, as opposed to not camouflaging the OT Network assets.

Q-GridPot. (For Power Transmission use) This network appliance is a highly specialized, low impact honeypot appliance specifically for electric power grids using ICS and SCADA. Network honeypots provide network obfuscation (hiding in plain sight) and denies the hacker easy network reconnaissance, while greatly increasing the likelihood of detecting a network breach. The Q-GridPot uses GridPot, an open source software package that has built-in IEC 61850 protocols for imitating large-scale electric power grids. This allows administrators to create attack surfaces that mimic their actual power grid environment, and/or portray a very complex and fictional power grid infrastructure. The Q-GridPot also mimics human activity. The number of deployed decoy attack surfaces is only limited by the number of available LAN IP addresses.

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 OT 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 OT 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, defeating air-gapping an OT Network.)

A device that has gone rogue means that it has been compromised, and is being controlled and used by the hackers. Most devices on OT 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.