Quantalytics Cyber Security Recommendations

Developed for
Electric Power
Substations

Quantalytics appliances are designed to be used individually, or can be combined as a synergistic ecosystem to maximize cybersecurity effectiveness. All images and network appliances are subject to change without notice.

Quantalytics

Overview for:
Power Substations
OT (OperationsTechnology)

Control Room Components

Q-Box® The version of Nagios deployed in the Q-Box for monitoring includes the ability to monitor Modbus over TCP/IP. We recommend using 2 Q-Box appliances for failover and load balancing.

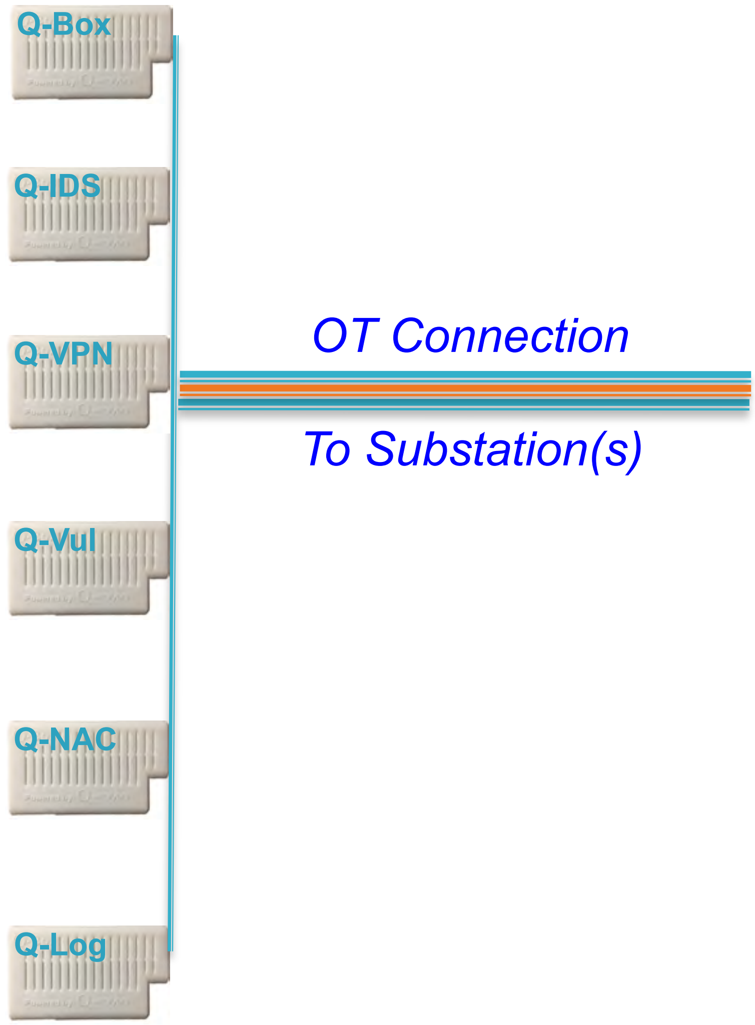
Q-IDS® This intrusion detection and prevention system built using Suricata. We recommend using 2 Q-IDS appliances for failover and load balancing. Suricata uses Snort definitions in addition to heuristics.

Q-VPN® Allows for the creation of VPN-to-VPN networks with extreme granularity of control over the TCP/IP devices at the substation. We recommend using 2 Q-Box appliances for failover and load balancing.

Q-Vul® Recommended to monitor for vulnerabilities in the substations. Even if no patch is available, or deployed, knowledge of security holes is still very valuable. The vulnerabilities can be monitored so as to provide early breach warnings.

Q-NAC® (Network Access Control) provides full control over allowed devices and services. The Q-NAC can thwart a physical penetration of a substation, including providing protection against physical plugbots.

Q-Log® Is a log aggregation and analysis tool running the ELK Stack. (Elasticsearch, Logstash, and Kirbana). It processes log entries and issues alerts. The Q-Log works in conjunction with all Quantalytics appliances plus any device that has a log and can output it, and integrates with any SIEM system. (e.g. Q-OSSEC®. Not shown.)



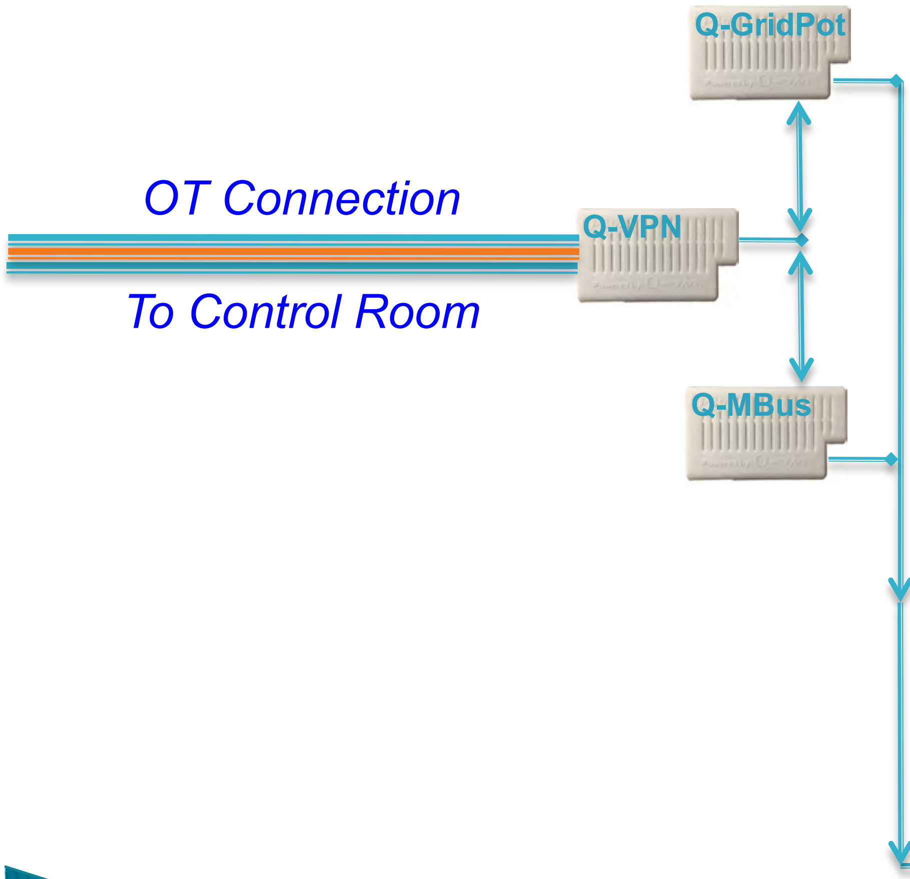
OT Connection

To Substation(s)

Quantalytics appliances are designed to be used individually,
or can be combined as a synergistic ecosystem to maximize cybersecurity effectiveness.
All images and network appliances are subject to change without notice.

Overview for:
Power Substations
OT (OperationsTechnology)

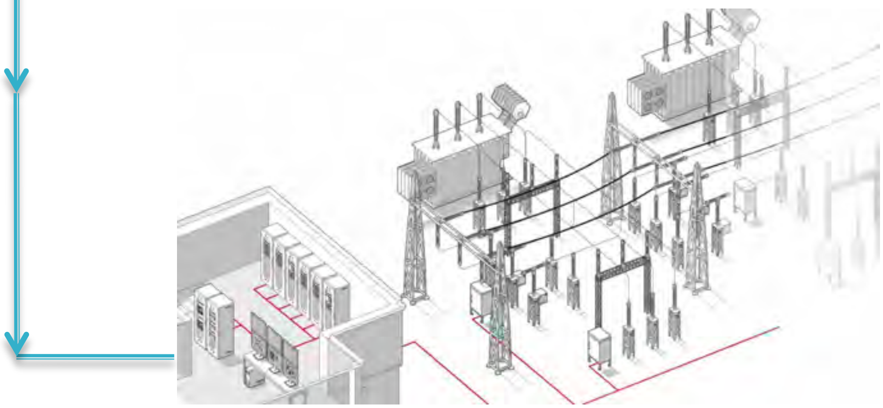
Substation Components



Q-GridPot® Is a honeypot appliance that mimics electric grids, including substations. It is built on top of Conpot, and is specifically for electric grids, including imitating HIDs. In the event of a breech, this will help deny the attacker an accurate surveillance of the subsystem infrastructure, and serve as a tripwire if the hackers manage to bypass the other precautions. The number of attack surfaces is only limited by the number of available IP addresses on each substation's VLAN segment.

Q-VPN® Allows for the creation of VPN-to-VPN networks with extreme granularity of control over the TCP/IP devices at the substation.

Q-MBus® Is the Quantalytics appliance that converts a serial Modbus connection to TCP/IP. This allows Modbus data to run over a VPN.



Quantalytics appliances are designed to be used individually, or can be combined as a synergistic ecosystem to maximize cybersecurity effectiveness.
All images and network appliances are subject to change without notice

Quantalytics

For more information please visit our web site:
www.quantalytics.com

We thank you for your interest and
look forward to your questions and comments.

Contact:
616.449.7810 x 1
info@quantalytics.com

Quantalytics appliances are designed to be used individually, or can be combined as a synergistic ecosystem to maximize cybersecurity effectiveness.
All images and network appliances are subject to change without notice.