QUANN PROTECT

QUANN OPERATIONAL TECHNOLOGY DEFENCE

Protect your operational technology infrastructure 24.7.365

SCADA (Supervisory Control and Data Acquisition) and Industrial Control Systems (ICS) face growing security risks as the infrastructure for Operational Technology (OT) becomes increasingly complex, smarter and IP-enabled for connectivity. Built with efficiency and function in mind, these systems are often not optimised for security, and the traditional approach of air-gapping no longer works because of the easy availability of remote access software. Under these circumstances, organisations often do not have the capabilities in place to monitor and protect their SCADA systems and lack visibility of potential vulnerabilities and threats.

QUANN OPERATIONAL TECHNOLOGY DEFENCE

Quann Operational Technology (OT) Defence is purpose-built appliances that deliver full visibility into your ICS networks and assets to protect your operations technology infrastructure. The appliance passively monitors all network traffic 24.7.365 and provides actionable alerts of security risks, human errors and system failures. The solution is easy to deploy without requiring additional agents or gateways.

It can be connected to Ethernet networks through a mirror/SPAN port of existing equipment or to Fieldbus networks as a new device on the network.

FEATURES

Unified solution for all ICS vendors

- Quann OT Defence is vendor-agnostic and works with whatever system you have deployed, regardless of supplier or protocol.
- It provides full visibility into all ICS equipment and network components, both IP and non-IP based.

Threat detection and management

- The ICS network is monitored for anomalies such as human errors, network failures and malicious activities.
- ICS-specific detection engines combine deep understanding of offensive capabilities with applied knowledge of the ICS domain.
- Information from the entire ICS network is correlated to provide insights into the root cause of incidents and changes.

Forensics and incident response

- Actionable alerts allow for swift and effective response to cyber incidents.
- A detailed forensics trail helps with a full investigation into past and current network behaviour.
- Monitored through Quann Security Operations Centres 24.7.365.

Risk management

- Manages and prioritises risks by automatically generating a risk profile of assets based on their criticality to the operational process and real-time risk indicators from the network.
- Automatically detects and classifies changes to the ICS network and assets.

BENEFITS

Ensures that the entire ICS environment is protected 24.7.365

By providing complete network and communication visibility on all IP and non-IP based assets, Quann OT Defence ensures comprehensive cyber security coverage and protection for your ICS systems. Real-time alerts for malicious activities, based on known and unknown threats and suspicious behavioural anomalies, ensure that you are always kept updated and aware of the latest security status.

Reduces the risk of downtime

By monitoring all risks to network and asset stability, whether caused by human errors, misconfigurations or actual malicious activities, Quann OT Defence helps ensure the availability and integrity of operational processes. Intelligent analysis of risks also enables you to optimise the deployment of scarce security resources – events can be classified so that you are alerted only to the ones that need further investigation.

Saves time and costs involved in operational and compliance tasks

By collecting information and automatically generating reports that comply with ICS regulations and standards, Quann OT Defence helps organisations to save time and costs while fulfilling regulatory or company policy requirements. It also increases operational effectiveness by automatically detecting and classifying changes for more efficient change management.

QUANN
THE ART AND SCIENCE OF BEING CYBER SECURE

For more information, please contact us at **info@quannsecurity.com**
or visit our website at **quannsecurity.com**