Using Automated Network Micro-Segmentation to Manage Cyber Risk in Your OT Environments

As cyber risks including ransomware attacks continue to increase on Industrial Companies, regulators, insurance companies, and outside auditors are recommending and often mandating that industrial companies invest in better managing their OT network attack surface.

Micro-network segmentation benefits

- Reduce the Attack Surface of the OT Network
- Better Visibility and Management of OT Network Operations
- Minimize the number of users in specific zones
- Limit the ability of adversaries to get command and control during a ransomware attack
- Provides asset visibility on what is on the network
- Stay compliant with cyber insurance policies
- Aligns with NIST CSF and other Cyber Standards
- Delivers a Zero Trust Framework

How does micro-segmentation work

In a typical segmentation project, devices at different layers in the plant or different sections are broken up by physically or virtually segmenting the network. This requires a redesign of the network, along with implementation and continuous monitoring of configuration rules. A micro-segmented network creates a firewall for every device on the network by restricting communications to that device from anywhere except known safe traffic. Changes to the network do not compromise the segmentation strategy, reducing cost and complexity.

How does this fit in with a defense-in-depth strategy

There are two main strategies that are part of a defense in depth approach to cyber security: proactive and reactive. Reactive approaches focus on scanning assets and network traffic for changes that indicate a bad actor has infiltrated your network. Proactive security focuses on guarding assets from initial infiltration. Micro segmentation is a fundamental part of a defense in depth strategy and is very effective in preventing bad actors access to your assets, network, and intellectual property.