MonSoteria Industrial Controls Practice

Securing Industrial Control systems from cyber threats

Going beyond mere network segmentation to protect Industrial Control systems.

Cybersecurity of most Industrial Control systems is an after thought and rarely effective.

> **"MonSoteria helped us build resilience around our Industrial Control systems."**
>
> **- VP Operations, Public Company**

The cyber world becomes real through industrial control systems and losing control over these can have real world ramifications.

The Stuxnet virus showed that it is possible for hackers to do real world damage. It also provides a ready framework for hackers to emulate and it shows that even air-gapped systems can be attacked.

A key element of protecting Industrial Control systems is to not view them as one homogenous entity. Instead it is important to understand the "Crown Jewels" within them and take special measures to protect these. Our practice will show you how to get this done. You begin with an assessment that identifies the Crown Jewels and maps your existing network and defenses and provides a roadmap to defend the most critical elements. This is done by bringing together three elements: Isolation, Simplification, and Active Monitoring.

In the post-Stuxnet world it has become imperative to not merely rely on network segmentation for the cybersecurity of the Industrial Control Systems. Call us now and leverage our expertise in defending these systems.

MonSoteria Cyber Security Solutions LLC
http://monsoteria.com
Call now: 1-877-494-7133