Quad Plus®

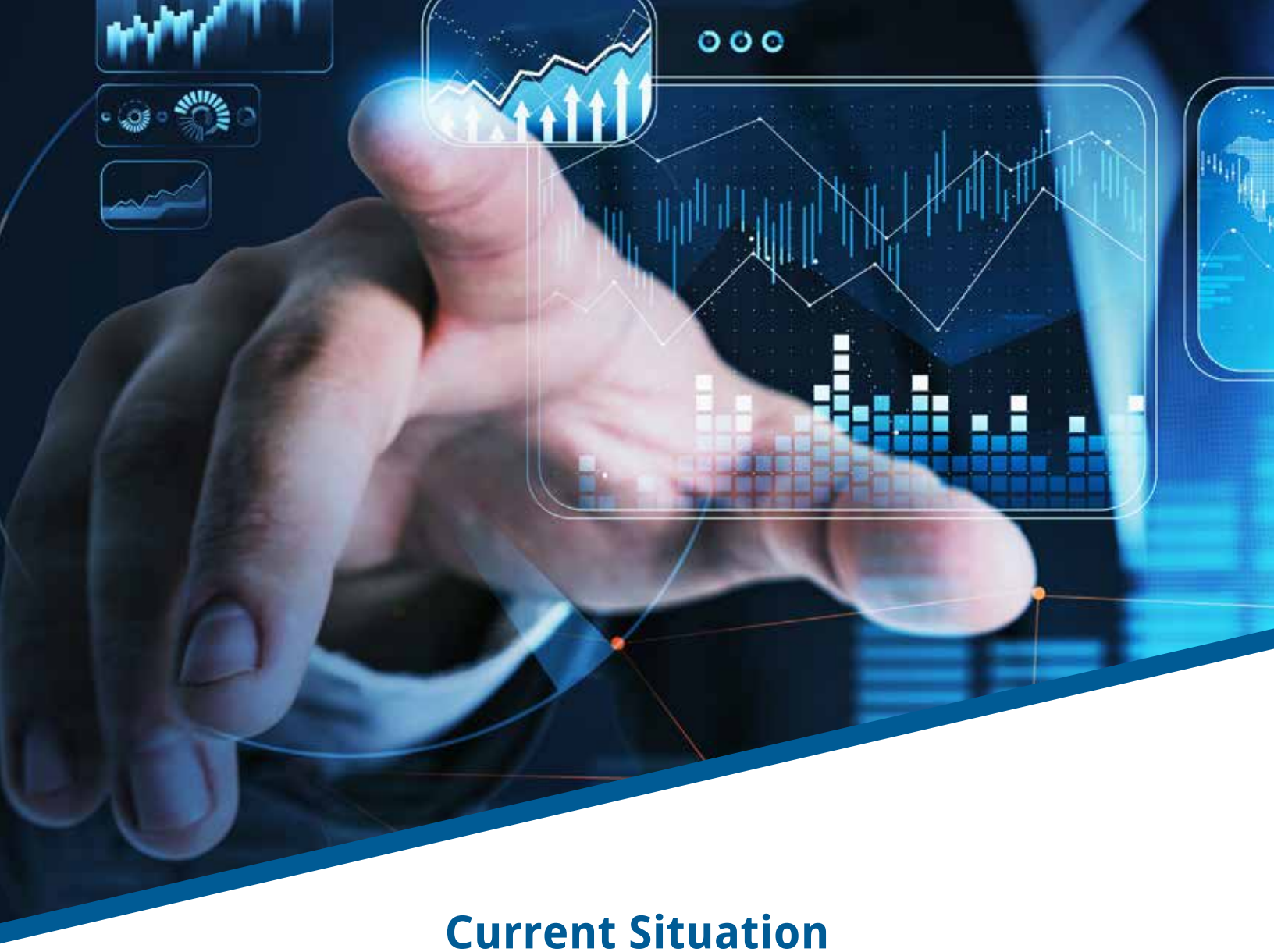
Operation to Enterprise (O2E) MSP

Consultation and Implementation, Backup and Disaster Recovery, Asset Inventory and Life Cycle Management, Firewall and Networking, End Point Security and Active Threat Hunting, Data Encryption and Storage, Controls Systems

Connect with us

www.quadplus.com

(815) 724-2323



Current Situation

Security, both physical and logical, is a critical component to maintaining production on connected systems. Historically, the manufacturing floor was isolated from external threats by keeping it disconnected. This is no longer an option as manufacturing floor data is needed by the front office to make timely or critical decisions promptly. Remote workforces need to be able to make changes and investigate issues. It is no longer practical to maintain isolation on the factory floor. With the requirements of connectivity come certain threats that can be managed and mitigated through a thoughtful and comprehensive approach to cybersecurity.

Our Mission

We will implement a Defense-in-Depth (DiD) Plan to guard against, mitigate, and recover from malicious attacks. We are committed to mitigating attacks, as much as practical, and when the inevitable breach occurs to minimize the impact and restore continuity of businesses.

O2E Services

- ✓ Consultation and Implementation
- ✓ Backup and Disaster Recovery
- ✓ Asset Inventory and Life Cycle Management
- ✓ Firewall and Networking
- ✓ Data Encryption and Storage
- ✓ Controls Systems
- ✓ End Point Security and Active Threat Hunting
- ✓ Managed Compliance and Governance

Asset Inventory and Life Cycle Management

Knowing what should be on your network and with what it communicates aids in identifying when incursions or malfunctions occur. Itemizing the components and understanding their life expectancy increases uptime by proactively replacing or upgrading prior to failure. Additionally, technology changes at a rapid pace, which means upgrading incrementally as current as practical reduces the gaps to bridge. For example, when a 15-year-old PLC finally fails, there is no direct replacement, which results in an expensive and unplanned outage for a large-scale system redesign and rewrite.

Firewall and Network

The need to share information across systems is unavoidable, but access should be closely monitored and controlled. Unlike IT environments, a failure or loss of connectivity in OT networks may induce a health and safety risk as well as expensive downtime. OT networks need a higher level of reliability, as controls systems control real world equipment. The usage of firewalls and network segmentation not only reduce the risks of incursions, but limit the impact.

Consultation and Implementation

Looking to implement or improve cybersecurity on your operation technology (OT) systems and controls? We can help via consultation, implementation and ongoing support with a wide range of services.

Backup and Disaster Recovery

Cyber criminals are continuously inventing new methods to penetrate security to steal intellectual property, cause damage and/or hold assets for ransom. There is no method to completely secure any system, which has any networking or human interfaces. This is why backup and disaster recovery is paramount to business continuity. Aside from cyber threats, other factors can contribute to disruptions and loss of data, such as power failures or brownouts damaging equipment, routine hardware failure and accidental deletion by employees. Having the ability to recover with acceptable loss and within an acceptable time window is vital to you and your customers.

Quad Plus®

Data Encryption and Storage

When thinking of data encryption, there is a tendency to think it is only for medical or financial data. Encryption should apply to anything which could cause harm, disrupt operations or loss of a competitive advantage. If a cybercriminal can gain physical access to a device, there is little most cybersecurity countermeasures can do to help. Proper encryption will increase the time required to access the information, ideally to the point to which the data loses relevance. Think of a storage dive, laptop or mobile device containing sensitive data being stolen; how long could it take to detected the device was missing.

Controls Systems

Controls systems are often overlooked as part of the cybersecurity posture, though they are also typically the least hardened against cyber threats. Depending on the type of controls, there are various methods and systems designed to aid in backing up the programs. Some systems, such as Allen Bradley PLCs coupled with FactoryTalk AssetCentre even have the capability to track changes and control access using Active Directory integration.

Controls systems have become a prime target for gaining entry to OT and IT Systems, if not targeted for stopping operations for ransom. Hence, they need to be included in the cybersecurity posture including monitoring, life cycle management and disaster recovery.

End Point Security and Active Threat Hunting

Regardless of the security measures taken, there will always be unforeseen intrusion points and zero-day exploits. Some threats gain access and then go dormant awaiting a specific time or trigger to act. End point security is designed to detect and minimize incursions, but it needs to be accompanied with active threat detection to try to root out existing or new sleepers. Think of it like building security; even though the doors and windows are locked with alarms, there is still a need for someone to patrol the building.

Connect with us

www.quadplus.com **(815) 724-2323**