Zero Trust ICS

Network Assessment Services

As industrial control systems (ICS) and process control network (PCN) environments become more connected, “security by obscurity” is no longer an adequate strategy. Sophisticated adversaries have taken notice of vulnerabilities found in today’s operational environments. Driven by the sophisticated nature of the adversary, the legacy concepts of trusted and untrusted are blurred which necessitates the concept of Zero Trust throughout ICS networks. The Zero Trust ICS assessment is designed to evaluate technology decisions and network defense architectures to measure the effectiveness of access and network controls withing ICS and PCN environment, identify improvement opportunities, and help enhance overall control system segmentation and security. The Zero Trust ICS assessment can be leveraged in conjunction with Capgemini’s leading-edge Industrial Control Systems and Process Control Networks Cybersecurity Assessment or as a standalone service.

Features and Benefits

1. **Outlines current network security posture plan identified gaps**
2. **Detailed network analysis, Network and access control remediation plan**
3. **(Optional) Program Management and Implementation of a Zero Trust network**

The Zero Trust ICS assessment is a tailored technical evaluation of operational technology (OT) environments including Process Control Networks (PCN), Supervisory Control and Data Acquisition (SCADA), and Distributed Control Systems (DCS) network security implementations. The purpose of the assessment is to define opportunities for improvement to the overall security posture of the OT environment. Designed to evaluate the current deployment of the ICS network and access controls, the Zero Trust ICS assessment can be used to identify the current implementation, verify the level of security controls, recommend process and technology improvements and prioritize additional cyber-security investments.

What does the engagement entail?

Capgemini's advanced cybersecurity team initiates the Zero Trust assessment with a kickoff meeting to introduce the team, review and refine scope, describe the process and brief the client on the final deliverables of the engagement.

The Zero Trust ICS assessment includes a review of OT network schematics, supporting infrastructure, onsite discovery interviews with OT application owners; and examination of internal processes. ICS Security network architecture decisions are then analyzed against the 8 domains of the Zero Trust ICS assessment framework via documentation reviews and onsite questionnaire based workshops.

What is the deliverable?

Zero Trust ICS assessment: This service provides a detailed assessment of the network segmentation and access controls within your ICS environment. This detailed report documents findings and provides ICS-specific recommendations including a prioritized list of gap mitigation steps with an estimated level of effort to execute and the benefits to the organization.

Why partner with Capgemini?

Capgemini's broad capabilities in network architecture design, security technology deployments, and managed services can assist you in achieving your Zero Trust network goals. Safely executed in production environments by highly skilled technicians and analysts experienced in working in operational environments, our technical assessments and security deployments are designed to be accomplished without causing downtime or mishaps. Our deep understanding of the cyber-threat landscape, operational technology environments, and business needs enables the delivery of realistic and actionable recommendations. Additionally, the breadth and depth of our cyber implementation professionals will convert the recommendations to a plan and execute it.

For further information, please contact:
infra.global@capgemini.com

People matter, results count.

8 Domains

1. Security Frameworks and Governance Model
2. Network Segmentation
3. Network Infrastructure Hardening
4. Access Control Layers
5. Visibility and Monitoring
6. User Authentication and Authorization
7. Network Services Isolation
8. Operational Support

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Learn more about us at

www.capgemini.com/cybersecurity

CSNA.19.05.06.L007.R04