SCADA ICS Network Security Challenges

The uncontrolled risk exposure of SCADA ICS environment which has no proper cyber security assurance process in place especially in network management segment is threatening. The nework infrastructure is viewed as the tunnel to access the SCADA ICS environment internally and externally, therefore the security controls should be governed properly. This article covers some of the major challenges that may be found during the cyber security assurance implementation across the SCADA ICS environment. The actual challenges that may be found at each organization may varies one to the other, and the degree of complexity varies as well, but the major challenges can be polarized into several categories, as per covered on this article

SCADA ICS Network Security Challenges

THE COMMON CHALLENGES IN SCADA ICS NETWORK SECURITY MANAGEMENT COMPLIANCE

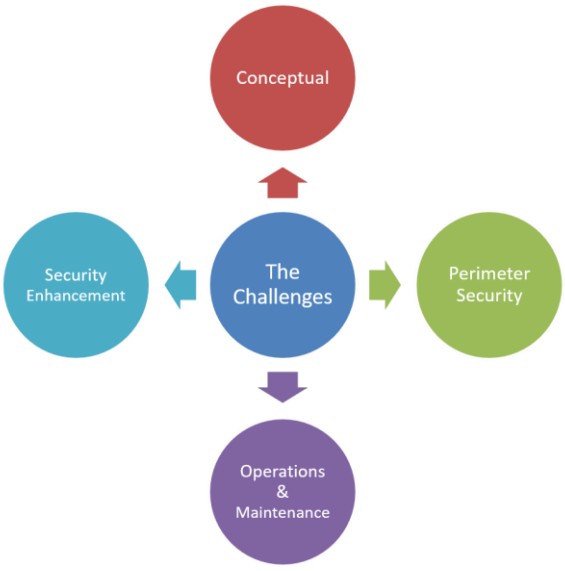
HOW IT HAPPENS AND WHAT ARE THE CHALLENGES

Ideally, the ICS security assurance should be started from the Design and Engineering phase. By having proper design that collaborates cyber security assurance across the entire SCADA ICS environment, it will lead to smoother handover from Project phase into Operations phase. Less major project during the Operations phase due to some essentials requirement of having secure environment already accommodated during the project phase.

But in fact, the adoption of cyber security assurance in SCADA ICS environment usually comes after the Commissioning phase. People just realize that their system contain more vulnerabilities after realizing that some specficiation and architecture that being implemented are not adhering to certain SCADA ICS security standards.

The network management portion also being included on those gap findings, that lead to several prevention mitigation strategies that should be followed up during the Operations phase. Meanwhile the resources to cover such activities are not ready due to lack of professionals in SCADA ICS security assurance, or even lack of corporate mindset and security culture when it comes to deal with SCADA ICS environment.

In general, following diagram depict the core challenges that can be found in the SCADA ICS network management in correlation with its security assurance



Following are the explanation of each challenges on the SCADA ICS network security aspect:

I. Conceptual
- The fundamental philosophy of segregation of Business environment and ICS environment – Internal vs. External
- Absurd in Zoning and Conduit concept
- Blend environment of Business and ICS, improper defense-in-depth and layer filtering concept -> traffic filtering and governance

II. Perimeter Security
- Failed to define proper conceptual basis, lead to perimeter security challenging situation
- Security guard in L3/L4 interconnectivity, loose of proper setup (configuration and management)
- Unclear access philosophy of Business from/to ICS environment, lack of definition that lead to absurd access management

III. Operations Maintenance
- Resources availability – Big gaps of Business vs. ICS -> Network Devices and Security Network Devices operations and management
- Dispute domain on operations and maintenance
- The entity is belong to ICS physically, but the operations and maintenance are belong to Business – lead to operational clash

IV. Security Enhancement

- The Lack of both side review and security assurance (collaboration of both domains, Business and ICS)
- Critical concern on the future improvement and assurance of the security compliance due to improper coordination and partial approach
- Risk assessment and continuous improvement – who to cover, how and what is the framework for current operations and future enhancement

SCADA ICS SECURITY INTEGRATED CYBER SECURITY MANAGEMENT SYSTEM AS A SOLUTION

What is the best way to capture the above challenges from happening at our organization?

One of the best answer is we need to have deep and thorough understanding against what is required to be governed in the pursuance of SCADA ICS security assurance.

As we have the very fundamental standard called Cyber Security Management System, being covered under ISO 27001 standard, then the similar thing should also be governed for SCADA ICS environment to capture all related aspects that have correlation into the cyber security assurance.

By having this kind of approach the challenges that we may face during the Operations phase can be minimized, controlled, governed and actioned from the initial timing of the whole plant life cycle process. Also, the continuous improvement of cyber security assurance across the SCADA ICS environment will also be enhanced in periodic basis.

"The proper SCADA ICS Cyber Security Management System is the key to have cyber security assurance in SCADA ICS environmentd"

Be ready to prepare yourself as the next SCADA ICS Security Professional. Explore more on our SCADA ICS Cyber Security courses – Explore More