SIEMENS

On line-Training II Risk Assessment in ambito OT Cyber Security, IEC 62443-3-2 (IK-SECRISK)

Short Description

In parallel and completing the IK-SEC2 course, this module provides an important study on risk assessment, considered as a key tool for preparing the necessary measures and for the consequent management of cyber risk on industrial plants. Where having deepened the techniques and tools used for attacks, with simulations and examples of attacks, the risk assessment process will be deepened. The first step will be the definition of the business rationale, that is the risk assessment criterion to be used, agreed with the company management. What are the critical business consequences in the event of an attack? What are the various levels? What are the potential critical threats that can carry out an attack. The answer to these questions will be the key element in organizing a good risk assessment process. Downstream of the definition of the criteria (the business rationale), the next step involves the execution of the high-level risk analysis, i.e. the analysis carried out on industrial assets with the aim of understanding where we can have critical consequences and which level and then derive the list of critical assets that will deserve an in-depth analysis with the detailed risk analysis. This analysis, much more in-depth than the previous one, will require a specific analysis on critical assets, in order to evaluate architectures, devices, protocols and vulnerabilities with a dedicated network traffic analysis and therefore understand what attack vectors and scenarios can be. Being a very complex analysis, it can be understood how the high-level analysis essentially has the purpose of skimming the list of critical assets in order to optimize the assessment process and therefore go into detail only where useful to make additional information to evaluate the problems and implement the most appropriate risk containment measures. The final goal of the process will therefore be the determination of a cyber security specification that, starting from a segmentation of the network, will allow us to understand how and where to intervene for risk mitigation.

Objectives

After attending the course you will be able to:
- Set up an industrial cyber security risk assessment process
- Define the criteria and methods for carrying out a risk assessment
- Describe how cyber business risks are assessed and presented
- Understand how threat intelligence is acquired and how credible threat assessment can be done
- Understand what a vulnerability is, how it is categorized and cataloged, how it can be exploited to carry out an attack
- Understand how to carry out a vulnerability analysis, with what purpose and with which tools to carry it out
- Understand how a risk is estimated and assigned a security level and how to get to the zoning and segmentation of the network
- Describe the reference architectures presented in IEC 62443 and understand how to use them within a specific infrastructure
- Understanding how to protect the most critical areas of the plant
- Understand the security requirements organized in IEC 62443-3-3 and how they contribute to the security objectives
- Describe how a cyber security specification is born and its importance

Target Group

For the level of detail implemented, this course is intended for personnel called to carry out risk assessment in the cyber environment within an organization of an end-user or to integrators who will have to carry out risk assessments to demonstrate to the end user the fulfillment of security objectives.

Content

- The assessment process for IEC 62443-2-1 and the contextualization of the criteria and method with reference to IEC 62443-3-2
- The business rationale, as a fundamental criterion and step for determining the impact on the business of a potential attack
- High-level risk analysis and determination of critical assets and credible threats
- Network analysis, active and passive scans, vulnerability analysis, penetration tests, all tools for obtaining valuable information on an industrial network
- Dynamics and simulations of attack, vectors and attack scenarios within the detailed risk assessment.
- Detailed risk analysis, how to use the information from the high-level risk assessment and vulnerability analysis to determine the real risk on plants
- What is the result of the assessment: security level, zoning and determination of the necessary processes and measures
- The link between IEC 62443-3-3 and the result of the risk assessment
- From risk assessment to cyber security specifications and related implementation
- From the security level target to the security level actually reached, how to measure security performance

The course includes examples, developed on real components and systems, albeit in the laboratory.
During the course, group and individual exercises will be carried out to facilitate and verify the learning of the topics described.

Prerequisites

Basic knowledge of automation systems and networks, familiarity with the principles and methods of risk assessment.

Note

No Training Material is provided.

Type

Online-Training

Duration

8 hours

Language

it