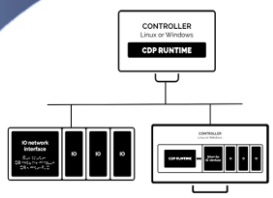

Evaluation

Identification of the System under Consideration (SuC)

This service consists of detailed identification of the system under consideration (SuC). It is the first activity to carry out a cyber risk assessment in the industrial field (OT). It aims to understand how the system was designed, configured, installed, the changes that were introduced since its conception, how it is being operated and how it is being maintained.

RISK MANAGEMENT SYSTEM

Whether it's old dinosaur, modern systems, or a combination of these, industrial control systems once they're installed in your plants tend to stay for decades. Small and successive changes are being introduced over time and different subsystems are being connected (local and/or remote).

Documentary assessment

All documentation available and provided by the user is analyzed in search of changes, undocumented connections and differences with physical reality. All cyber-assets are understood, the current situation, technology and their relationships are analyzed. All the necessary data for each of the cyber-assets are collected for proper treatment and subsequent use. As a result of this service the corresponding documentation will be updated, and the specific data obtained from the different sources are recorded.

Physical evaluation

Physical security and cybersecurity are closely related. The single evaluation of the documentation is not enough, and a physical context visualization is required for each of the cyber-assets that make up the system under consideration (SuC). Distances between these, the way these were installed, how they are being maintained, the processes that are being controlled and the aggressiveness of the physical environment are just some of the aspects to analyze. Various service orders are executed passively.

Traffic assessment

Methods with passive techniques are implemented in industrial networks for the evaluation of existing traffic in order to identify industrial protocols, which devices communicate with each other, which devices have access and what flow of communications are generated in different situations of operation of the plant. All this information is contrasted with documentary information.

Identifying cyber-assets

All cyber-sensitive hardware and software assets of the system under consideration (SuC) are correctly identified and all relevant information required is collected for evaluation. The complete list of cyber-assets and associated information will be required in other subsequent activities. Existing partial listings are reviewed, updated and completed with additional information relevant to cybersecurity.

Identifying vulnerabilities

By means of different methods, techniques and sources of information vulnerabilities in the system under consideration begin to be identified. Contrary to what many professionals believe, the vulnerabilities of control systems are not found solely in technology; but these are also located in the way the systems were designed, how they were built, how they are being operated and how they are maintained. While many vulnerabilities are identified at this stage, other methods and techniques will be required for complete identification.

Through other services in our catalog can be added to identify Vulnerabilities that are still unknown or have not been published. Cyber-assets that are being evaluated may have more vulnerabilities not yet discovered. Especially for those products and systems that don't have any lab certifications, such as: ISASecure.

Public Vulnerabilities
are those vulnerabilities known and/or disclosed by organizations (e.g. ICS-CERT, NVD, CVEs) and those that are informed by the manufacturers themselves of the industrial systems.

Private Vulnerabilities
are those vulnerabilities (non-public) discovered as a result of the use of specific methods and techniques, and all those related to design, configuration, operation and maintenance during a vulnerability assessment of the System under Consideration (SuC).

Zero-Day Vulnerabilities
are those newly discovered new vulnerabilities. We can "propose" Zero-Day vulnerabilities during a "Detailed Industrial Cyber Risk Assessment" (Cyber-PHA) and design the risk output against unrealistic situations.

Identifying threats

In a similar way for each of the cyber-assets we will begin to identify a certain number of potential threats. Without dismissing any of them, the threats are identified as well as their possible actions on the cyber-asset. Additional methods and techniques will be needed at later stages to obtain a complete list of threats. These threats have different natures, different backgrounds, different ways of manifesting themselves and acting.

Complementary services

Other more sophisticated complementary methods and techniques can be used to identify vulnerabilities in cyber-assets with laboratory techniques and penetration testing. Visit our service catalog in the "complementary services" section for more information.

Zones & Conduits Manager it will allow you to manage and manage all cyber-asset information related to security, vulnerabilities (public, private and zero-day), criticality analysis, zone and conduit assignment, detailed cyber risk assessment, security levels (capacity, current, desired) and all associated security recommendations.