MAINTAIN

EN99 – Alerts Manager

Handling and Management of Industrial Cybersecurity Alerts Applying the ISA/IEC-62443 Standard

Cyber security requires monitoring, detecting, watching, and alerting based on a large number of cybersecurity events that occur in control systems. This activity, necessary to accompany the safe operation of the plant, requires a series of fundamental activities that must be correctly executed prior to its implementation.

The generation of security alerts is followed by assertive, immediate and non-tolerance cyber incident management. Alerts should be classified and categorized according to a realistic risk possibility and in context with the industrial process, with no false positives. Responses must be specific and rapid to ensure that the occurrence of potential consequences is preventively, effectively and efficiently avoided.

The generation of cyber security alerts (cyber incidents) may or may not correlate with process disturbances and alarms and ultimately the occurrence of potential consequences. Developing the ability to anticipate physical facts about the plant requires specific knowledge that can only be achieved with specific knowledge of the plant.

It is crucial to design and implement surveillance, warning and incident management systems – without false alerts – through a process of streamlining security alerts, based on specific knowledge and the result of detailed cyber risk assessment.

Additionally, when you're monitoring, alerting, and responding to cybersecurity incidents, it's significantly different to do it on a system that has all of its risks mitigated than it is to do it on a system that doesn't.

At the end of the EN99 course you will be in a position to:

The objective of the course is to know the main activities and requirements of the Life Cycle of Security Alert Management according to ISA/IEC-62443 and ANSI/ISA-18.2-2016, for the development, design, installation and administration of a Cyber Security Alert System in industrial processes.

To meet this objective, the concepts, models and conceptualization for the handling and management of alerts will be presented, and the application of these criteria for the development of the alert philosophy, alert rationalization, basic alert design, advanced alerting techniques, HMI design for alerts, monitoring evaluation, detection and response actions.

Participants will learn the activities of the alert management lifecycle with reference to the ISA/IEC-62443 and ISA/18.2 standards and how to address common problems of security alert management systems and process alarms. Key benefits of attending this course include:

- Learn best practices to improve the performance of the alert system.
- Learning methods to solve common alert management problems.
- Learn about the best practices for an affective and successful implementation of the alert management system.
- Avoid generating false security alerts that don't lead to any action or distractions.
- Design responses to security alerts before they happen with fast, accurate responses.
- Learn the metrics to measure success in alert management and continuous improvement.

Upon completion of the EN99 course, participants will be able to:

- Develop an alert management philosophy.
- Identify alerts.
- Streamline alerts, including triage and prioritization.
- Design basic alerts, their monitoring, detection and notification.
- Determine when advanced alerting techniques should be used.
- Document alerts for operations.
- Design reports to monitor and evaluate the performance of the alerting system.
- Manage changes in alerting systems.

Recognitions:

All participants who meet the course requirements and who successfully pass the final exam with a good grade will be awarded a Digital Badge. The Digital Badge certifies that the participant has attended the EN99 training course and has executed the final assessment test with a good grade, verifying that the participant has assimilated the new knowledge in a reasonable way.

Requirements:

It has no specific requirements. It is recommended that the professional has knowledge of some of the following: Industrial Process Alarm Management Standard, ISA/18.2, International Cybersecurity Standards by Industry Consensus ISA/IEC-62443, ISO-27000 Corporate Cybersecurity or Information Security Standards, Industrial Risk Management Standards such as ISA/IEC-61511, Functional Security, Regulations and/or National Standards such as NIST, NERC, and others; Experience in corporate project management and cultural change management, Other industrial risk management standards (worker safety, environmental safety, etc.).

At WiseCourses we are inspired by innovation in education to create training processes that are representative of the world we live in today. Create and support new systems by empowering educators and practitioners who gain the expertise.