Security Development Lifecycle Training

exida Can Show you the Way

Training Course: Security Development Lifecycle Training

for developers of industrial control system products

Course Description:

There are well established strategies and techniques that automation suppliers can employ to discover and mitigate security vulnerabilities and improve the inherent security of their products. Learning and adopting these strategies will allow suppliers to better serve their customers and, at the same time, stay ahead of security researchers who aim to expose their flaws.

Software Security Assurance (SSA) is the process of ensuring that software is designed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects. SSA is best achieved by integrating security into the software development life cycle (SDLC).

For over a decade, exida has helped hundreds of companies integrate functional safety into their industrial automation products and achieve IEC 61508 (SIL) certification. We are now pleased to offer a training course dedicated to helping companies integrate security into their industrial automation products.

This course was created specifically for developers of industrial control system products with a particular focus on network-enabled embedded control system products such as PLCs, DCSs, SISs, RTUs, VFDs, etc. It was designed by and is instructed by security certified engineers with over 25 years experience in developing and assessing embedded industrial control and safety system products.

The objective of this course is to train R&D teams, through a combination of lecture and workshop, on how to properly and effectively integrate software security assurance practices and techniques into their existing software development lifecycle.

The training covers all 12 phases of the ISASecure™ Software Development Security Assurance (SDSA) certification program. Course materials are provided including valuable templates and examples.

Background:

Due to recent events, such as the discovery of the Stuxnet virus, owners and operators of industrial facilities have become far more aware and concerned about the risk that cyber events present to their operations. In response, many of these companies are anxiously seeking assurance from their automation suppliers that their products and systems meet an industry recognized baseline for cyber security.

The same events have aroused the "security researcher" community causing them to turn their attention from commercial IT products to industrial automation and control systems. While their motives may vary, the end result is that there are suddenly a lot of very smart people actively looking to expose the fragility and insecurity in industrial control system products.

Responding to this sudden market demand for inherently secure products can be extremely challenging for most automation suppliers. Most products on the market today were developed at a time when security was not even identified as a requirement.

Skills You Will Learn:

- How to identify security vulnerabilities in existing products
- How to use techniques such as threat modeling to identify vulnerabilities in designs
- Test techniques, such as fuzz and abuse case testing, to uncover hidden weaknesses
- Tools and techniques to mitigate vulnerabilities
- How to integrate security into your organization's existing software development lifecycle
- How to specify security requirements
- How to architect security into new designs
- Best practices for writing and reviewing secure code
- How to test and validate security
- How to best manage security vulnerabilities in third-party code
- How to best respond to security vulnerabilities discovered in the field

Who Should Attend:

- R&D managers
- System architects
- Software engineers
- Test engineers
- Quality assurance managers

Course Length: 4 Days

Cost:

Pricing varies with the number of students and the location.

Please call (+1 215-453-1720) or email (info@exida.com) for a quotation.