Formations Embedded security: Secure Embedded Systems - eLearning et Cours en ligne

Embedded security

Secure Embedded Systems

Secure embedded systems integrate numerous strategies and procedures to perfectly coordinate cybersecurity in the programming and equipment of embedded frameworks. Security segments added to embedded systems can block the usefulness of a framework and affect the constant execution of the missions of the core systems. Framework specialists, engineers and experts need a highly characterized approach to the whole process, while emphasizing the usefulness of embedded frameworks and cyber security. A secure embedded framework can use a security coprocessor to cryptographically guarantee the confidentiality and reliability of the framework while ensuring its usefulness.

Vous pouvez visualiser les descriptifs détaillés des différents cours en utilisant la barre de navigation ci-dessus. Vous pouvez également cliquer sur les références des cours dans les descriptions ci dessous.

oSEC1 - Writing Secure C/C++ code This is a Live Online Training
Lean ways to use C/C++ safely in critical systems and discover the Embedded system features for security

oSEC2 - Advanced Embedded Systems Security This is a Live Online Training
Discover how to protect your programs from malicious user input, Secure System Software and Consideration, Apprehend the context and the use of Hypervisors and System Virtualization and Discover Security checks and Tools

oSEC3 - wolfSSL for Embedded Security The OSEC3 course is designed for software/ Hardware engineers to understand how SSL/TLS Works , establish fundamental knowledge about cryptographic, algorithms, and protocols and Learn how to implement secure authentication with wolfSSL

oSEC4 - Advanced wolfSSL for Embedded Security The OSEC4 course is designed for software/ Hardware engineers. The aim of this course is to discover how encryption works and how to manage secret keys, learn how to implement secure authentication with wolfSSL, building wolfSSH on standard Platforms, secure boot using wolfBoot (with wolfCrypt and WolfSSL)and understand how to build wolfMQTT on standard platforms and use it in an IoT application