Embedded security

Embedded security

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.

You can see detailed course descriptions of the various trainings by using the above navigation bar. You can also click on course identifiers in the following course briefs hereafter.

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/ Hardwa