Applus⊕ laboratories

Cybersecurity training

Applus+ offers a range of open training services to help customers preempt security problems right from the start of product development.

We offer open training sessions in cibersecurity to help our customers to train their engineers with the required knowledge to face any security feature in their products or systems, during product design and before prototyping.
All our training courses are designed ad-hoc to meet customers' necessities.

ICs
Learn about physical attacks, side channel analysis and perturbation attacks. Review the most important implementation attacks against cryptography. Analyze the most reliable security countermeasures. Learn about the best security practices and keep know-how in the organization.

Platform
Check the implications of platform security guidelines and learn how to protect your TOE while meeting all security requirements.

Mobile Payment Applications
Anticipate security issues by learning about best security practices when developing MPA.

TEE
As an upcoming technology, TEE presents vendors and developers with new security challenges. Applus+ can provide training about the technology, its security boundaries and any related security issue helping vendors being at state of the art know-how of this technology.

Common Criteria
Our Common Criteria experts can provide training about the complexities of Common Criteria evaluations, covering assurance levels, work units, site certificate process, documentation generation and review, security features, and TOE definition. Essential training before facing your first Common Criteria evaluation.

Note: Because Applus+ Laboratories is accredited as a third party laboratory by several evaluation and certification schemes, and in order to guarantee its impartiality, Applus+ engineers are never involved in actual product development or solutions implementation.