

## Machine learning security (Python) (MLSEC-P)

ID MLSEC-P Price on request Duration 4 days

### Who should attend

Python developers working on machine learning systems

### Course Objectives

- Getting familiar with essential cyber security concepts
- Learning about various aspects of machine learning security
- Attacks and defense techniques in adversarial machine learning
- Input validation approaches and principles
- Identify vulnerabilities and their consequences
- Learn the security best practices in Python
- Managing vulnerabilities in third party components
- Understanding how cryptography supports security
- Learning how to use cryptographic APIs correctly in Python

### Course Content

- Cyber security basics
- Machine learning security
- Input validation
- Security features
- Time and state
- Errors
- Using vulnerable components
- Cryptography for developers
- Wrap up

## Machine learning security (Python) (MLSEC-P)

---

### Training Centres worldwide



### Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3  
CH-8304 Wallisellen  
Tel. +41 44 832 50 80

[info@flane.ch](mailto:info@flane.ch), <https://www.flane.ch>