Machine Learning Security (MLSEC)

ID MLSEC **Prix** sur demande **Durée** 4 jours

A qui s'adresse cette formation

Python developers working on machine learning systems

Pré-requis

General machine learning and Python development

Objectifs

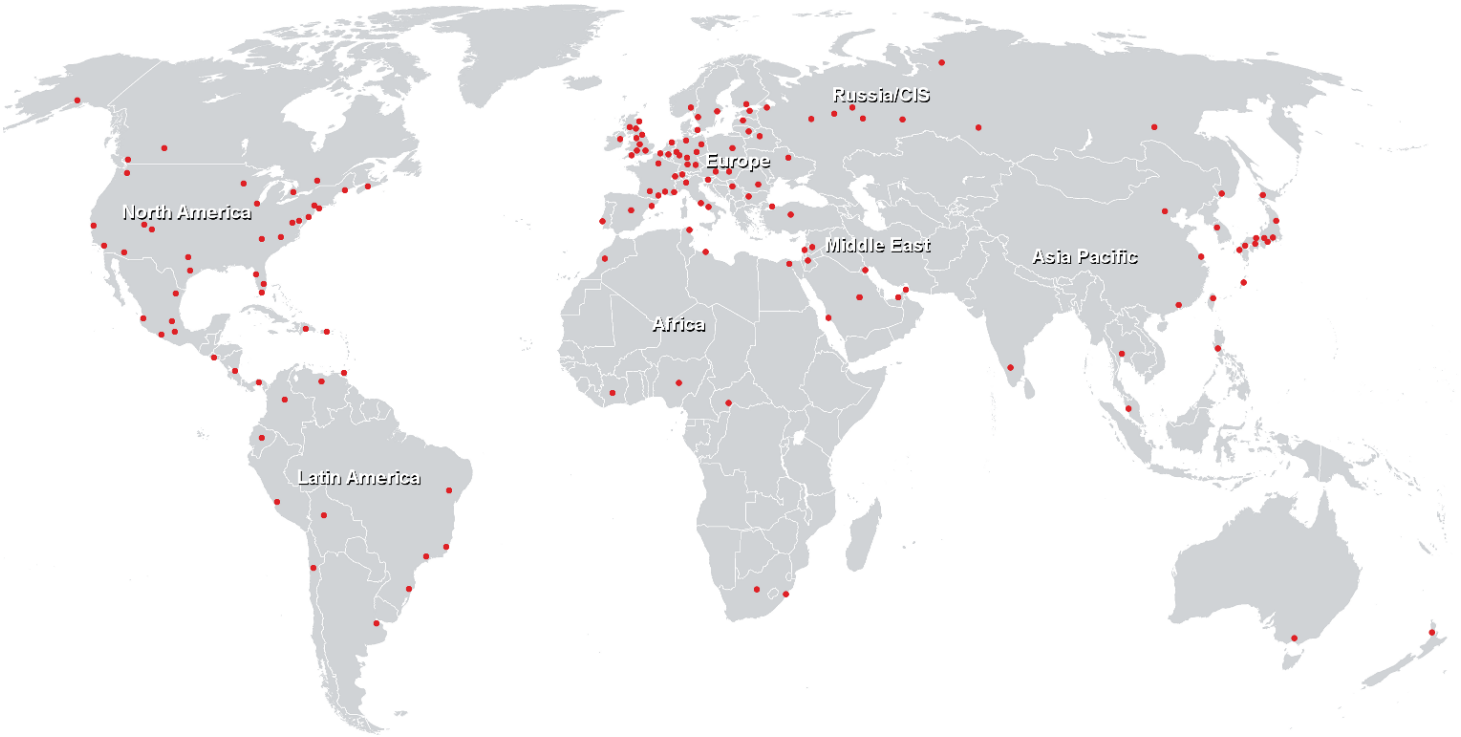
- Getting familiar with essential cyber security concepts
- Learning about various aspects of machine learning security
- Attacks and defense techniques in adversarial machine learning
- Identify vulnerabilities and their consequences
- Learn the security best practices in Python
- Input validation approaches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

Contenu

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

Machine Learning Security (MLSEC)

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

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

info@flane.ch, https://www.flane.ch