+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 02/26/2026

Register

PET Training: Computing on Private Data & FHE

3 days (21 hours)

Overview

Privacy-Enhancing Technologies (PET) and Fully Homomorphic Encryption (FHE) are now an advanced technological response to the security requirements imposed by the NIS2 Directive. These technologies enable calculations to be performed on encrypted data without ever decrypting it, thereby eliminating the critical exposure stage during processing.

In a context where essential entities must demonstrate proportionate technical measures and reduce their attack surface, encryption at rest and in transit is no longer sufficient. Data "in use" becomes the major point of vulnerability.

This training course will enable you to understand and implement computing on private data as a concrete technical remediation measure.

You will study the fundamentals of Fully Homomorphic Encryption, from network-based cryptography to noise management mechanisms, and learn how to use the main industrial libraries such as Zama (TFHE-rs), Microsoft SEAL, and OpenFHE.

At the end of this training course, you will be able to design secure PET-oriented architecture, justify NIS2-compliant technical measures, and integrate homomorphic encryption into a comprehensive cybersecurity strategy.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Master the Privacy-Enhancing Technologies (PET) framework.

- Understand and use Fully Homomorphic Encryption (FHE) to process data without decryption.
- Reduce the attack surface by eliminating the decryption step on computing servers.
- Get to grips with industrial libraries (Zama, Microsoft SEAL, OpenFHE).
- Perform use cases (statistical analysis, AI inference) on encrypted data.
- Justify and document a NIS2-compliant technical remediation measure.

Target audience

- Cyber/Data engineers
- IT architects
- CISO
- DPO

Prerequisites

- Solid knowledge of cybersecurity
- Basic knowledge of cryptography
- Knowledge of IT/cloud architecture and data processing

PET training: Computing on Private Data & FHE

[Day 1 - Morning]

NIS2 governance and executive responsibility

- NIS2 Directive framework and essential entities
- Civil and criminal liability of managers
- Proportionate technical measures required
- ANSSI audit expectations
- Positioning of advanced encryption as a remediation measure
- Practical workshop: Mapping NIS2 obligations for a critical organization.

[Day 1 - Afternoon]

Limitations of traditional encryption in the face of audits

- Encryption at rest vs. encryption in transit
- Vulnerability of data "in use"
- Risk associated with decryption on computing servers
- Exposure in cloud and multi-tenant environments
- Attack surface of outsourced processing
- Hands-on workshop: Analysis of a critical data exposure scenario.

Privacy-enhancing technologies as a strategic response

- Definition of Privacy-Enhancing Technologies (PET)
- Confidential Computing vs. FHE
- Secure Multi-Party Computation
- Zero-Knowledge Proof
- Integration into a Zero Trust Architecture
- Hands-on workshop: Identifying PETs suitable for a regulated environment.

[Day 2 - Morning]

From partial encryption to fully homomorphic encryption

- Partially homomorphic encryption (Paillier)
- Transition to Fully Homomorphic Encryption (FHE)
- Calculating encrypted data without decryption
- Cryptographic noise and bootstrapping
- Lattice-based security
- Hands-on workshop: Performing homomorphic arithmetic operations.

[Day 2 - Afternoon]

Mathematical foundations and security parameters

- Introduction to Euclidean lattices
- Noise management and circuit depth
- Post-quantum security parameters
- CPU/RAM constraints
- Performance/security trade-offs
- Hands-on workshop: Adjusting parameters for optimization.

Industrial libraries and FHE ecosystem

- Presentation of Zama (TFHE-rs) and open source approach
- Microsoft SEAL
- OpenFHE
- Comparison of implementations
- Integration into an existing IT architecture
- Hands-on workshop: Implementing processing via the FHE library.

[Day 3 - Morning]

Use case: statistical analysis of encrypted data

- Calculation of averages and secure aggregations
- Use of an encrypted database

- Confidentiality of identities and results
- Outsourcing of calculations without exposure
- NIS2 regulatory validation
- Hands-on workshop: Statistical analysis on encrypted datasets.

[Day 3 - Afternoon]

Use case: Confidential AI and machine learning

- Inference on encrypted data
- Protection of models and datasets
- Secure AI computing outsourcing
- Latency constraints
- CPU/RAM optimization
- Hands-on workshop: Simulation of homomorphic inference.

Implementation strategy and NIS2 compliance

- PET as a technical remediation measure
- Justification during audits
- Documentation and security governance
- Roadmap for gradual adoption
- Risk reduction measures
- Hands-on workshop: Developing a NIS2-ready implementation plan.

Companies concerned

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific business knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.

Training organization registered under number 11 75 54743 75. This registration does not constitute state approval.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg