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

Mis à jour le 26/02/2026

S'inscrire

Formation PET : Computing on Private Data & FHE

3 jours (21 heures)

Présentation

Privacy-Enhancing Technologies (PET) et Fully Homomorphic Encryption (FHE) constituent aujourd'hui une réponse technologique avancée aux exigences de sécurité imposées par la Directive NIS2. Ces technologies permettent d'effectuer des calculs sur des données chiffrées sans jamais les déchiffrer, supprimant ainsi l'étape critique d'exposition lors des traitements.

Dans un contexte où les entités essentielles doivent démontrer des mesures techniques proportionnées et réduire leur surface d'attaque, le chiffrement au repos et en transit ne suffit plus. La donnée "in use" devient le point de vulnérabilité majeur.

Cette formation vous permet de comprendre et d'implémenter le computing on private data comme mesure concrète de remédiation technique.

Vous étudierez les fondements du Fully Homomorphic Encryption, de la cryptographie basée sur les réseaux aux mécanismes de gestion du bruit, et prendrez en main les principales bibliothèques industrielles telles que Zama (TFHE-rs), Microsoft SEAL et OpenFHE.

À l'issue de cette formation, vous serez en mesure de concevoir une architecture sécurisée orientée PET, de justifier une mesure technique conforme NIS2 et d'intégrer le chiffrement homomorphe dans une stratégie globale de cybersécurité.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Maîtriser le cadre des Privacy-Enhancing Technologies (PET).

- Comprendre et utiliser le Fully Homomorphic Encryption (FHE) pour traiter des données sans déchiffrement.
- Réduire la surface d’attaque en supprimant l’étape de déchiffrement sur les serveurs de calcul.
- Prendre en main les bibliothèques industrielles (Zama, Microsoft SEAL, OpenFHE).
- Réaliser des cas d’usage (analyse statistique, inférence IA) sur données chiffrées.
- Justifier et documenter une mesure technique de remédiation conforme NIS2.

Public visé

- Ingénieurs Cyber/Data
- Architectes IT
- RSSI
- DPO

Pré-requis

- Connaissances solides en cybersécurité
- Notions de cryptographie
- Culture architecture SI / cloud et traitement de données

Formation PET : Computing on Private Data & FHE

[Jour 1 - Matin]

Gouvernance NIS2 et responsabilité des dirigeants

- Cadre de la Directive NIS2 et entités essentielles
- Responsabilité civile et pénale des dirigeants
- Mesures techniques proportionnées exigées
- Attentes des audits ANSSI
- Positionnement du chiffrement avancé comme mesure de remédiation
- Atelier pratique : Cartographie des obligations NIS2 pour une organisation critique.

[Jour 1 - Après-midi]

Limites du chiffrement traditionnel face aux audits

- Chiffrement au repos vs en transit
- Vulnérabilité de la donnée “in use”
- Risque lié au déchiffrement sur serveurs de calcul
- Exposition en environnement cloud et multi-tenant
- Surface d’attaque des traitements externalisés
- Atelier pratique : Analyse d’un scénario d’exposition de données critiques.

Privacy-Enhancing Technologies comme réponse stratégique

- Définition des Privacy-Enhancing Technologies (PET)
- Confidential Computing vs FHE
- Secure Multi-Party Computation
- Zero-Knowledge Proof
- Intégration dans une architecture Zero Trust
- Atelier pratique : Identification des PET adaptés à un contexte réglementé.

[Jour 2 - Matin]

Du chiffrement partiel au Fully Homomorphic Encryption

- Chiffrement partiellement homomorphe (Paillier)
- Passage au Fully Homomorphic Encryption (FHE)
- Calcul sur données chiffrées sans déchiffrement
- Bruit cryptographique et bootstrapping
- Sécurité basée sur les lattices
- Atelier pratique : Réalisation d’opérations arithmétiques homomorphes.

[Jour 2 - Après-midi]

Fondements mathématiques et paramètres de sécurité

- Introduction aux réseaux euclidiens (Lattices)
- Gestion du bruit et profondeur de circuit
- Paramètres de sécurité post-quantique
- Contraintes CPU / RAM
- Arbitrage performance / sécurité
- Atelier pratique : Ajustement des paramètres pour optimisation.

Bibliothèques industrielles et écosystème FHE

- Présentation de Zama (TFHE-rs) et approche open source
- Microsoft SEAL
- OpenFHE
- Comparatif des implémentations
- Intégration dans une architecture IT existante
- Atelier pratique : Mise en œuvre d’un traitement via bibliothèque FHE.

[Jour 3 - Matin]

Cas d’usage : analyse statistique sur données chiffrées

- Calcul de moyennes et agrégations sécurisées
- Exploitation d’une base de données chiffrée

- Confidentialité des identités et des résultats
- Externalisation de calcul sans exposition
- Validation réglementaire NIS2
- Atelier pratique : Analyse statistique sur dataset chiffré.

[Jour 3 - Après-midi]

Cas d’usage : IA et Machine Learning confidentiel

- Inférence sur données chiffrées
- Protection des modèles et des datasets
- Externalisation de calcul IA sécurisée
- Contraintes de latence
- Optimisation CPU / RAM
- Atelier pratique : Simulation d’une inférence homomorphe.

Stratégie d’implémentation et conformité NIS2

- PET comme mesure technique de remédiation
- Justification lors d’audit
- Documentation et gouvernance sécurité
- Roadmap d’adoption progressive
- Mesure de réduction de risque
- Atelier pratique : Élaboration d’un plan d’implémentation NIS2-ready.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.