

## [Formation certifiante] Architecture en cybersécurité

### OBJECTIFS

- Promouvoir des mesures méthodologiques, techniques et organisationnelles de sécurité
- Définir, déployer et gérer une architecture de sécurité dans différents contextes professionnels
- Identifier les éléments techniques de sécurité ainsi que les outils à mettre en oeuvre selon les besoins
- Réaliser une analyse de risque, un audit de vulnérabilités et de politique de sécurité
- Analyser les outils du marché les mieux adaptés à la protection du SI et des réseaux
- Évaluer une situation de crise et prendre les bonnes décisions
- Maîtriser les techniques et les outils de gestions d'identité et d'autorisation
- Présenter les risques pour la sécurité du Cloud
- Appliquer les technologies d'IA pour renforcer les mesures de cybersécurité et comment appréhender les risques potentiels qui y sont associés

### PROGRAMME

#### Introduction

#### Conception d'architectures de sécurité

- Conception d'architecture de sécurité et aperçu du marché en solutions de cybersécurité
- Attaques réseaux
- Firewall, routeur, IDS/IPS, VPN
- Cryptographie, fonction de hachage et signature numérique
- Infrastructure de confiance

#### Normes et règlementations

- Standards 27001 et 27002 pour l'établissement et la gestion du SMSI



### DATES ET LIEUX

Du 09/03/2026 au 11/09/2026 à Paris

### PUBLIC / PREREQUIS

Techniciens ou ingénieurs avec bonne expérience en systèmes d'information et en réseaux informatiques avec des connaissances de base en cybersécurité.

### COORDINATEURS

#### Maya BADR

Enseignante et responsable pédagogique en cybersécurité et technologies du numérique à Télécom Paris Executive Education. Elle a obtenu son diplôme de doctorat en communications numériques de Télécom Paris.

- Aspects juridiques
- Protection des données RGPD
- Certification critères communs et CSPN

## Analyse et gestion de risques

### Audit de sécurité

- Audit de vulnérabilités
- Audit de politique de sécurité
- Gestion de crise et reprise d'activité (PRA) : incidences d'une crise cyber sur l'organisation ou l'entreprise
- Plan de continuité d'activité (PCA) et protection contre la fuite des données sensibles

## Outils de supervision, SOC, SIEM

### Authentification, Identity & Access Management

- Gestion et fédération des identités : SSO interne et web SSO, OpenID et SAML
- Gestion de rôles : Role Mining, réconciliation de rôles
- Gestion des autorisations : provisioning, gestion des exceptions, reporting
- Aperçu de l'offre commerciale : retour d'expérience et limites de l'offre

## IA et cybersécurité

### Introduction à l'informatique quantique et la cryptographie post-quantique

### Architecture Blockchain

- Fondements et infrastructure de la Blockchain
- Domaines d'exploitation

## Sécurité du Cloud

- Typologie des environnements de Cloud, impact pour la sécurité
- Virtualisation et sécurité : menaces et vulnérabilités, solutions de sécurité
- Sécurité des données externalisées
- Référentiels de sécurité Cloud
- Détection et exploitation de vulnérabilités dans le Cloud

## DevSecOps

- Outils du DevOps
- Principes et best-practices du Secure Design
- l'intégration de la sécurité dans le cycle de vie du

développement logiciel  
- Collaboration et communication dans le DevSecOps

## Synthèse et conclusion

Appelez le 01 75 31 95 90  
International : +33 (0)1 75 31 95 90

[contact.exed@telecom-paris.fr](mailto:contact.exed@telecom-paris.fr) / [executive-education.telecom-paris.fr](http://executive-education.telecom-paris.fr)