CERTIFICATION

ARCHITECTURE EN CYBERSÉCURITÉ

FFCCERTTERXCS02	PRIX : 13 200 €	DURÉE : 29 JOURS	ÉLIGIBLE CPF

Pauses et déjeuners offerts

L'architecte en cybersécurité joue un rôle central dans la conception, l'évolution et la résilience des systèmes d'information. Elle ou il est responsable de l'intégration de solutions de sécurité adaptées aux besoins métiers, de l'évaluation des situations de crise, de la prise de décision stratégique ainsi que du pilotage du reporting auprès des parties prenantes.

Dans un contexte de transformation numérique accélérée, marqué par l'essor de l'intelligence artificielle, la montée en puissance des architectures distribuées (cloud, edge, zero trust) et l'émergence des risques liés au calcul quantique, l'architecte doit désormais adopter une approche systémique, anticipative et souveraine de la cybersécurité.

Cette formation certifiante, labellisée SecNumEdu FC par l'ANSSI, forme des experts capables de concevoir et piloter des architectures de sécurité robustes, alignées avec les référentiels de sécurité et les bonnes pratiques de l'ANSSI.

VOUS ÊTES

Techniciens ou ingénieurs avec une bonne expérience en systèmes d'information et en réseaux avec des connaissances de base 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 œuvre selon les besoins
- Réaliser une analyse de risque, un audit de vulnérabilités et de politique de sécurité
- Analyser les outils de sécurité du marché les mieux adaptés à la protection du SI et des réseaux
- Évaluer une situation de crise et prendre les bonnes décisions
- Utiliser les techniques et les outils de gestion d'identité et d'autorisation
- Analyser les impacts des évolutions technologiques, notamment liés à l'IA et aux technologies quantiques
- Appliquer les technologies d'IA pour renforcer les mesures de cybersécurité et appréhender les risques potentiels qui y sont associés

ÉVALUATION ET CERTIFICATION

- Évaluation des compétences acquises
- Ateliers de mise en oeuvre et de simulation de cas pratiques concrets
- Évaluation du mémoire professionnel basé sur un projet individuel soutenu devant un jury d'experts

Les participants ayant suivi le parcours avec succès obtiennent la certification des blocs 3 et 4 du RNCP38140 délivrée par Télécom Paris.

PROGRAMME

Introduction
- Objectifs de sécurité
- Domaines d'application
- Différents besoins en sécurité
- Tendances récentes et menaces émergentes

Conception d'architectures de sécurité
- Conception d'architectures 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

IA et cybersécurité
- Principes de l'intelligence artificielle et de l'apprentissage statistique
- Mise en œuvre et évaluation de méthodes d'apprentissage dans le cas de problématique de cybersécurité

Normes et réglementations
- Standards 27001 et 27002 pour l'établissement et la gestion du SMSI
- Aspects juridiques
- Protection des données RGPD
- Directive NIS2
- Certification, critères communs et CSPN

Analyse et gestion de risques
- Principales méthodes : ISO 27005, EBIOS RM

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

L'IA pour la gestion des risques et l'automatisation des audits

Outils de supervision, SOC, SIEM
- Méthodologies d'implémentation, d'exploitation et de traitement
- Étude de cas concret de gestion d'un SOC
- Le SOC augmenté par l'IA

Authentification et Gestion des identités et des accès
- 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

Introduction à l'informatique quantique et à 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
- Intégration de la sécurité dans le cycle de vie du développement logiciel
- Collaboration et communication dans le DevSecOps

Synthèse et conclusion

ATELIER

RÉALISABLE EN ANGLAIS

FAISABLE À DISTANCE

RESPONSABLE(S)

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.

LABEL

SecNumedu
Formation continue
ANSSI

CERTIFICATION DÉLIVRÉE PAR

TELECOM Paris
IP PARIS