

# Sécurité de l'Active Directory

Éligible au CPF: Non

Action collective: Non

## INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

**Domaine:** Systèmes et Réseaux

Filière: Systèmes et réseaux Microsoft

Rubrique : Sécurité des systèmes

Code de formation : SYR630B

#### **€** Tarifs

Prix public : 2130 €

#### Tarif & financement:

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.

Le dispositif FNE-Formation.

**L'OPCO** (opérateurs de compétences) de votre entreprise.

**France Travail:** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

**CPF** -MonCompteFormation

Contactez nous pour plus d'information : contact@aston-institut.com

## **PRÉSENTATION**

## **Objectifs & compétences**

- o Décrire les mécanismes internes Active Directory
- o Identifier les fonctionnalités de sécurité
- o Concevoir une architecture robuste
- o Identifier les attaques et principales exploitations dans un système existant
- Mettre en œuvre les contre-mesures

#### Public visé

Architectes et administrateurs systèmes, ingénieurs sécurité.

#### Pré-requis

Avoir de bonnes connaissances dans l'administration Windows Server 2012 R2 / 2016 / 2019 ainsi que dans les rôles Active Directory.

## Lieux & Horaires

Durée: 21 heures

**Délai d'accès :** Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

#### **PROGRAMME**

#### 1. Les fondamentaux en sécurité

- Comprendre une architecture Active Directory typique
- Revue de l'authentification / autorisation
- Tour d'horizon des différents protocoles
- Comprendre les recommandations et bonnes pratiques associées

#### 2. Comprendre les risques et les attaques

- Vue d'ensemble des méthodes de gestion des risques SI
- Comprendre les différentes étapes d'une attaque
- Simuler des attaques et analyser les contre-mesures
- Détecter les failles de sécurité
- Vue d'ensemble des outils associés

#### 3. Durcissement de l'infrastructure AD

- Concevoir un plan de durcissement
- Déployer les directives associées
- Savoir auditer une infrastructure
- Collecter les évènements au niveau de l'entreprise
- Mettre en œuvre :
- Les directives préconisées
- Les nouveautés de durcissement (PAM, JIT / JEA...)

#### 4. Comprendre les modèles d'administration

#### # Prochaines sessions

Consultez-nous pour les prochaines sessions



- Connaître les différents modèles d'administration (EAM, Tier)
- Intérêt et limites du concept de forêt d'administration
- Mise en œuvre d'une forêt d'administration
- Vue d'ensemble des bonnes pratiques

#### 5. L'identité dans le Cloud

- Vue d'ensemble de la sécurisation via les outils Cloud
- Concevoir une architecture hybride
- Vue d'ensemble des outils :
- o Azure AD Password Protection
- Secure Score
- o Defender for Identity

#### 6. Mise en œuvre d'un durcissement complémentaire Active Directory

- Déployer une infrastructure PKI afin de porter les fonctionnalités de durcissement
- Durcissement de la fédération avec AD FS
- Durcissement Azure AD Connect

#### 7. Mise en oeuvre d'un PCA / PRA

- Concevoir une architecture PCA / PRA sur le socle Authentification
- Planifier des tests de PCA / PRA
- Comprendre les outils et méthodes pour tester un PCA / PRA
- Mettre en œuvre la sauvegarde et restauration

#### 8. Surveiller et auditer

- Vue d'ensemble des niveaux d'audit
- Gestion du cycle de vie des audits
- Centralisation des logs
- Bonnes pratiques et indicateurs

## **MODALITÉS**

#### Modalités

**Modalités :** en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

**Pédagogie :** essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques. **Ressources techniques et pédagogiques :** Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Toom

**Pendant la formation :** mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

#### Méthode

Fin de formation : entretien individuel.

Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.

Assiduité : certificat de réalisation.

**Validations des acquis** : grille d'evalution des acquis établie par le formateur en fin de formation.