

# Sécurité des applications et des serveurs web

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Éligible au CPF :** Non

**Domaine :** Cybersécurité - sécurité informatique

**Action collective :** Non

**Filière :** Sécurité défensive

**Rubrique :** Qualité et sécurité des infrastructures

**Code de formation :** AS604

## € Tarifs

**Prix public :** 2649 €

### 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](mailto:contact@aston-institut.com)

## PRÉSENTATION

### Objectifs & compétences

- Évaluer les risques internes et externes liés à l'utilisation d'Internet
- Identifier les différentes solutions pour mettre en oeuvre la sécurité d'un serveur Web
- Comprendre comment garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes
- Être capable de mettre en oeuvre une politique de sécurité fiable sur un serveur Apache ou IIS

### Public visé

Responsable sécurité Chef de projets Développeur Web Administrateur de serveur Web

### Pré-requis

Connaissance en administration Unix Connaissance des réseaux et protocoles TCP/IP

## Lieux & Horaires

**Durée :** 21 heures

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

## PROGRAMME

### INTRODUCTION AU PROTOCOLE HTTP

Format des requêtes Mécanismes d'authentification HTTP Génération de requêtes HTTP Découverte passive d'informations HTTP : protocole de transport

### INTRODUCTION AU PROTOCOLE HTTPS

Généralités Authentification par certificats X.509 Méthodes d'audit HTTPS Historique des failles de sécurité

### QUALITÉ DES DÉVELOPPEMENTS WEB

Erreurs classiques Classification OWASP : exemples, démonstrations Injections : exemple avec SQL XSS (Injection croisée de code)

### APACHE

Présentation du serveur phare du marché Web Sécurisation d'un serveur Apache Mettre en place https avec mod\_ssl Apache en relais-inverse Relayage applicatif avec mod\_proxy/mod\_rewrite Filtrage applicatif avec mod\_security Application à l'intégration Apache / Tomcat

### INTERNET INFORMATION SERVICES (IIS)

Architecture Installation Sécurisation Outils HTTPS

## Prochaines sessions

Consultez-nous pour les prochaines sessions.

## 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 / Zoom.

**Pendant la formation :** mises en situation, autodiagnosics, 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'évaluation des acquis établie par le formateur en fin de formation.