

# SALT SECURITY : LA PROTECTION DES APIS

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Éligible au CPF :** Non

**Domaine :** Développement

**Action collective :** Non

**Filière :** DevOps

**Rubrique :** Outils

**Code de formation :** S-APIS

## € Tarifs

**Prix public :** 1 600 €

### 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

Comprendre les concepts de sécurité de Salt Security  
Savoir effectuer des tests de sécurité  
Être capable de protéger ses API  
Savoir utiliser les fonctionnalités de Salt Security

### Public visé

Ingénieurs sécurité  
DevOps  
Développeurs  
Architectes

### Pré-requis

Connaissance de base en sécurité informatique.

## 📍 Lieux & Horaires

**Durée :** 14 heures

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

## PROGRAMME

### Conception et développement sécurisés

Qu'est-ce que Salt Security ?  
S'assurer de l'intégration des APIs  
Rationaliser la modélisation des menaces liées aux APIs  
La logique d'entreprise dans les révisions de conception  
Les orientations normatives des équipes d'ingénieurs

### Découverte et catalogage des API

Découverte des environnements de non-production  
Baliser et d'étiqueter les actifs  
Inclusion des dépendances de vos API  
Utilisation de sources de données pour établir un inventaire de base

### Tests de sécurité

Réutiliser l'analyse des vulnérabilités pour identifier l'infrastructure des API  
Analyser automatiquement le code de l'API dans la mesure du possible  
Exécuter des tests de fuzzing et des tests dynamiques sur les API déployées  
Vérifier les dépendances de code vulnérables connues  
Tester les API périodiquement ou conformément aux réglementations en vigueur  
Augmentez les tests avec des primes aux bogues

### Sécurité front-end

Limitation des données stockées côté client  
Examiner les options de protection côté client à la suite du côté serveur  
Fournir des exigences de sécurité pour les front-end  
Anticiper le code et les dispositifs du client compromis

### Journalisation et surveillance

Incorporer des exigences de journalisation non liées à la sécurité  
Adopter l'automatisation pour la configuration de la journalisation

## 📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

Adopter la technologie cloud

**Sécurité des réseaux**

Utilisez le transport crypté pour protéger les données transmises par vos API

Établir des listes d'autorisation et de refus d'adresse IP pour un nombre de consommateurs d'API

Utiliser des limites de débit dynamiques et définir des limites de débit statiques de manière sélective.

Renforcer la sécurité du réseau via l'infrastructure, et non dans le code

**Sécurité des données**

Utilisation du cryptage de manière sélective ou conformément à la réglementation

Utiliser des algorithmes et des bibliothèques de chiffrement bien contrôlés

Éviter l'envoi massif de données aux clients de l'API

Prévoir les risques liés au scraping à l'agrégation et à l'inférence des données.

**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.