FC9CS20 **1 750 €** **2 jour(s)**

ATELIER AVANCÉ

Sécurité DevOps/DevSecOps

OBJECTIFS

- Expliquer les enjeux et les changements importants de l'approche sécurité pour les nouveaux environnements : agile, DevOps, Cloud, Containers, Infrastructure as Code
- Mettre en œuvre la sécurité avec ces nouvelles technologies et contextes de fonctionnement
- Disposer des pointeurs pour savoir où et comment implémenter rapidement les premières étapes d'une sécurité DevOps
- Utiliser les Containers et l'Infra as Code pour automatiser et améliorer la sécurité
- Lister les pièges habituels de la transformation sécurité afin de savoir les éviter

PROGRAMME

Introduction

- Agilité
- DevOps
- Nécessité d'une nouvelle approche sécurité
- Pièges de la transformation sécurité
- Sécurité dans un modèle Spotify ou dans un Train SAFe

Sécurité de l'intégration continue

- Principes du pipeline CI/CD
- Risques et vigilances à avoir avec l'intégration continue
- Tests de sécurité par analyse statique (SAST)
- Tests de sécurité par analyse dynamique (DAST)
- Tests de sécurité par analyse interactive (IAST)
- Protection sécurité de l'environnement d'exécution (RASP)

Travaux pratiques

- Utilisation de Dependency Check et NPM audit pour l'identification de dépendances vulnérables
- Utilisation d'un Linter sécurité
- Utilisation de Gitleaks pour la détection de secrets

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Ce cours s'adresse à toute personne, expert sécurité, développeur ou exploitant IT qui souhaite comprendre et mettre en œuvre la sécurité dans un environnement agile, DevOps, Cloud et/ou de Containers. Les Dev et les Ops peuvent aussi participer et ainsi, en plus, devenir Security Champion dans leur équipe.

Des connaissances des services IT, notamment de la sécurité et des méthodologies Agile permettent de tirer un meilleur profit de la formation.

COORDINATEURS

Ons JELASSI

Enseignante-chercheuse à Télécom Paris en Machine Learning et en apprentissage statistique distribué, elle est également consultante en métrologie des réseaux auprès de grandes entreprises pour lesquelles elle effectue des missions d'audit et d'expertise. Ses travaux de recherche actuels, au sein du département Image, Données et Signal portent sur le passage à l'échelle des algorithmes d'apprentissage statistique.

MODALITES PEDAGOGIQUES

dans le code

Cours théorique avec retours d'expériences. Travaux pratiques pour assimiler l'application concrète.

Infrastructure as Code

- Intérêts de l'Infra as Code
- Exemple d'Ansible
- Exemple de Terraform
- Risques et vigilances à avoir avec l'Infra as Code
- Audit automatisé avec l'Infra as Code
- Infra as Code utilisée pour le passage à l'échelle de la sécurité

Travaux pratiques

- Utilisation d'InSpec pour l'audit automatisé
- Utilisation d'Ansible pour le renforcement automatisé

Containers

- Intérêts des containers et de leur orchestration
- Exemple de Docker et de Kubernetes
- Risques et vigilances à avoir avec les containers
- Bonnes pratiques et renforcement avec les Containers
- Scan automatisé d'images de Container

Travaux pratiques

- Scan de vulnérabilité sur images Docker
- Identification de mauvaises configurations et leurs impacts

Autres nouvelles mesures de sécurité

- Gestion automatisée des secrets (Vault)
- Identity et Access Management en contexte DevOps
- PKI TLS as a Service
- PKI SSH

Travaux pratiques

- Utilisation de Vault Hashicorp pour le stockage de secrets

Synthèse et conclusion