SÉCURITÉ DEVOPS/DEVSECOPS

AVANCÉ | ATELIER | FAISABLE À DISTANCE | RÉALISABLE EN ANGLAIS

FFCNCERCERXCS20 | PRIX : 2 090 € | DURÉE : 2 JOURS

Pauses et déjeuners offerts

CYBERSÉCURITÉ

FORMATIONS INTER-ENTREPRISES

PRÉSENTATION

L'informatique suit actuellement des transformations majeures : agilité, DevOps, Cloud, automatisation, Infra as Code et containers. La sécurité doit impérativement s'adapter sur les plans à la fois techniques et organisationnels.

À l'issue de cette formation, vous serez capables de mettre en œuvre la sécurité pour adresser l'arrivée des nouvelles technologies et du contexte agile/DevOps. Vous connaîtrez les nouveaux moyens concrets de sécurisation des étapes successives d'un pipeline DevOps (du code au déploiement) et vous les aurez expérimentés.

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 l a 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 de l'intégration continue
- Principes du pipeline CI/CD
- Risques et vigilances à avoir avec l'intégration continue
- Secret scanning, SCA
- 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

Infrastructure as Code
- Intérêts de l'Infra as Code
- Exemple d'Ansible et 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

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

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

Synthèse et conclusion

PUBLIC/PRÉREQUIS

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 agiles sont souhaitables afin de tirer pleinement profit de cette formation.

RESPONSABLE(S)

Yohan BOYER
Ingénieur sécurité chez JobTeaser, son rôle est de garantir la sécurité et l'intégrité du système d'information et des données.
Titulaire d'un doctorat en sécurité et fort de plusieurs années d'expérience dans ce domaine, il accompagne les équipes techniques dans l'adoption de pratiques DevSecOps tout au long du cycle de vie des applications.

MODALITÉS PÉDAGOGIQUES

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