

SÉCURITÉ DEVOPS/DEVSECOPS

FFCNCERCERXCS20

PRIX : 2 120 €

DURÉE : 2 JOURS

Pauses et déjeuners offerts



AVANCÉ



ATELIER



RÉALISABLE
EN ANGLAIS



FAISABLE À
DISTANCE

PRÉSENTATION

La sécurité ne peut plus être une étape ajoutée en fin de cycle. Dans un monde agile, cloud-native et automatisé, elle doit être intégrée à chaque étape du cycle de vie des applications, du développement jusqu'à la production.

Cette formation immersive couvre toute la chaîne DevSecOps : sécurisation du code, des pipelines CI/CD, de l'Infrastructure as Code, des conteneurs, de Kubernetes et de la plateforme. Elle aborde également les enjeux de l'IA. Chaque module alterne méthodes, démonstrations et ateliers pratiques pour développer des compétences directement applicables à vos projets.

OBJECTIFS

- Expliquer les enjeux de sécurité en environnement agile / DevOps / Cloud, et éviter les pièges classiques de la transformation
- Intégrer la sécurité dans le pipeline CI/CD : SAST, DAST, SCA, SBOM, secret scanning, IAST, WAF/RADP, supply chain
- Sécuriser l'infrastructure as Code (Terraform, Ansible), appliquer le policy-as-code et surveiller la posture cloud (CSPM)
- Durcir conteneurs et Kubernetes sur tout le cycle
- Gérer les secrets et la confiance
- Centraliser et prioriser les vulnérabilités par le risque (vulnerability management / ASPM)
- Appréhender l'IA en DevSecOps : l'IA au service de la défense

PROGRAMME

Introduction

- De l'agile et du DevOps au DevSecOps : contexte et enjeux
- Principes clés : shift-left, security-as-code, responsabilité partagée, monitoring continu
- Bénéfices et pièges classiques de la transformation

Sécurité du pipeline CI/CD

- Threat modeling et risques de la CI/CD
- Méthodes de test le long du pipeline : secret scanning, SCA & SBOM, SAST, pre-commit hooks, DAST, IAST
- Protection à l'exécution : WAF et RASP
- Sécurisation de la supply chain et du pipeline, security gates, priorisation
- Cas d'usage : Expérimentation des outils de sécurité du pipeline (SAST, SCA, secret scanning, DAST, etc.)

Infrastructure as Code

- Principes et bénéfices de l'IaC
- Terraform (concepts, workflow, state, providers) et Ansible (playbooks, rôles, modules)
- Risques et sécurisation de l'IaC, audit automatisé dans le pipeline
- Policy-as-code et Cloud Security Posture Management (CSPM)
- Cas d'usage : Scan et sécurisation d'une infrastructure IaC, mise en place du policy-as-code

Conteneurs et Orchestration

- Docker et OCI : bonnes pratiques d'images (multi-stage, distroless)
- Kubernetes : architecture et objets clés
- Risques par couche (image, cluster)
- Défenses build, ship, run : durcissement, admission control (Kyverno/Gatekeeper), NetworkPolicy, RBAC, Pod Security, détection runtime (Falco)
- Intégrité et provenance : SBOM, signature (cosign/Sigstore), SLSA
- Scanning (images, cluster, CNAPP)
- Cas d'usage : scan d'images et de cluster Kubernetes, durcissement de configuration et correction de findings

Sécurité de la plateforme

- Gestion des secrets et HashiCorp Vault (architecture, dynamic secrets, seal/unseal, injection runtime)
- IAM en contexte DevOps : identité humaine vs identité machine (workload identity)
- PKI as-a-service : TLS/mTLS, certificats à courte durée de vie, cert-manager, SSH
- Chiffrement as-a-service (Vault Transit)
- Gestion et centralisation des vulnérabilités : priorisation par le risque
- IA en DevSecOps : l'IA au service de la défense et sécurité des applications LLM
- Cas d'usage : Vault et ses fonctionnalités (secrets dynamiques, injection, PKI)

Synthèse et conclusion



PUBLIC/PRÉREQUIS

Experts sécurité, développeurs, exploitants (Ops/SRE), architectes et ingénieurs DevOps qui souhaitent comprendre et mettre en œuvre la sécurité en environnement agile/conteneurisé ou devenir Security Champions.

Des connaissances du cycle de développement logiciel et de ligne de commande (Linux, Git) sont souhaitables afin de tirer pleinement profit de cette formation.



RESPONSABLE(S)

Yohan BOYER

Tech Lead Security Engineer à Yubo. Il conçoit et opère au quotidien la sécurité d'une plateforme cloud-native à grande échelle, sur l'ensemble de la chaîne DevSecOps (CI/CD, IaC, conteneurs/Kubernetes, secrets, IAM, PKI).



MODALITÉS PÉDAGOGIQUES

Cours théorique avec retours d'expériences et mises en situation réelles.



CYBERSÉCURITÉ

FORMATIONS INTER-ENTREPRISES