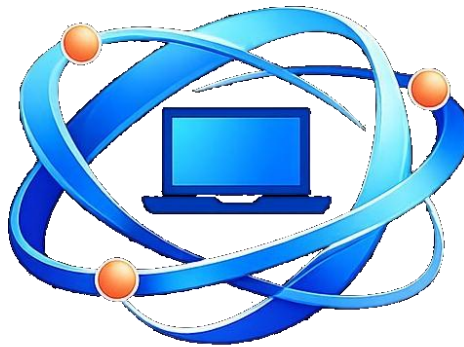




MFE-IT

Formation DevSecOps sur Azure (AZ-2001)

Sécurité intégrée dans CI/CD et pipelines DevOps

Référence : 2B-AZ2001

Durée : **1 jour** • Volume horaire : **7 h**

Distanciel · Sessions garanties dès 1 inscrit · 60 % de pratique

DESCRIPTION

Cette formation DevSecOps sur Azure – Sécurité intégrée dans CI/CD & pipelines DevOps vous enseigne comment implémenter des contrôles de sécurité automatisés directement dans vos processus d'intégration et de livraison continues. Vous apprendrez à intégrer des scans de code source, des analyses de dépendances et des tests de sécurité dynamique dans des pipelines Azure DevOps ou GitHub Actions.

Le programme couvre aussi la gestion des secrets, l'automatisation des gates de sécurité et le monitoring des artefacts de build. À travers des ateliers pratiques, vous construirez des pipelines sécurisés capables de stopper automatiquement une livraison en cas de faille. À l'issue, vous serez capable de déployer des workflows DevOps à la fois rapides, fiables et conformes aux bonnes pratiques de sécurité.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les fondements DevSecOps et les avantages d'intégrer la sécurité directement dans les pipelines DevOps.
- Savoir concevoir et configurer des pipelines CI/CD sécurisés dans Azure DevOps et GitHub Actions.
- Mettre en œuvre des outils et étapes de scanning automatisé pour détecter vulnérabilités, dépendances et secrets.
- Intégrer des tests de sécurité statiques (SAST), dynamiques (DAST) et de composition logicielle (SCA).
- Automatiser la gestion des configurations, le secrets scanning, les politiques de qualité et les mesures de sécurité.
- Assurer un retour d'information continu sécurisé, un suivi d'incidents et l'audit des artefacts DevOps.

PRÉREQUIS

- Connaissance d'Azure DevOps ou GitHub Actions (bases de pipelines CI/CD).
- Maîtrise de Git et compréhension des workflows DevOps.
- Notions de base de sécurité applicative et des pratiques de tests automatisés.
- Parce que chaque participant est unique, un entretien personnalisé avec notre expert nous permet de concevoir une formation parfaitement alignée avec ses objectifs, son niveau et ses enjeux professionnels.

PUBLIC VISÉ

- Développeurs, DevOps engineers, ingénieurs cloud/IT et sécurité souhaitant intégrer la sécurité dans leurs pipelines.
- Administrateurs systèmes, architectes cloud et responsables qualité/production.
- Toute équipe technique souhaitant renforcer ses processus de livraison continue avec une sécurité automatisée.

PROGRAMME DÉTAILLÉ

Module 1 — Fondements DevSecOps

- Introduction à DevSecOps : culture, objectifs, bénéfices.
- Différences entre DevOps classique et DevSecOps.

Module 2 — DevOps et pipelines CI/CD sur Azure

- Rappel des principes de pipelines Azure DevOps & GitHub Actions.
- Structures de pipeline : jobs, tasks, triggers.

Module 3 — Intégration de la sécurité dès la build

- Analyse statique du code source (SAST).
- Outils types : SonarCloud, Fortify, CodeQL.
- Automatisation dans le pipeline : qualité, dette technique, vulnérabilités.

Module 4 — Scanning de dépendances (SCA)

- Introduction au Software Composition Analysis.
- Mise en place de scans automatiques de dépendances pour détecter les vulnérabilités.
- Intégration avec OWASP Dependency-Check, GitHub Dependabot ou d'autres scanners.

Module 5 — Scanning dynamique et tests DAST

- Scénarios de tests de sécurité dynamique (DAST) dans le pipeline.
- Configuration des tests automatisés sur API et interfaces web.

Module 6 — Sécurité des artefacts et secrets

- Secrets scanning : détection de clés, tokens, secrets.
- Stockage sécurisé des variables et secrets en pipeline (Key Vault, GitHub Secrets).

Module 7 — Gates, security checks et quality gates

- Quality gates et conditions de succès de pipeline basées sur un score de sécurité.
- Arrêts automatiques de déploiement si les seuils ne sont pas atteints.

Module 8 — Monitoring, logs et audit DevSecOps

- Métriques, alertes et journaux de sécurité intégrés.
- Traçabilité et conformité dans le pipeline.

Module 9 — Ateliers pratiques et mise en œuvre

- Construction d'un pipeline CI/CD intégrant SAST, SCA et DAST.
- Retours automatisés sur la qualité de code, les vulnérabilités et les secrets.
- Déploiement sécurisé sur Azure (App Services / AKS).

LES PLUS

- Centrée sur l'intégration de la sécurité dans la chaîne CI/CD Azure DevOps.
- Couvre l'analyse de code, la gestion des secrets et la sécurité des pipelines.
- S'appuie sur de nombreux ateliers pratiques de mise en œuvre.
- Prépare à industrialiser une démarche DevSecOps en entreprise.

MODALITÉS PÉDAGOGIQUES

Format et déroulement

MFE-IT privilégie un format en mini-groupe (1 à 3 participants), garanti dès un seul inscrit (sauf cas de force majeure). La formation se déroule en distanciel (classe virtuelle synchrone, sessions également enregistrées) ou en présentiel dans vos locaux. Le programme alterne apports théoriques et ateliers pratiques de mise en œuvre sur des pipelines CI/CD.

Format ultra-personnalisé

Un entretien préalable est organisé avec le participant et/ou un représentant de l'entreprise afin d'adapter le contenu à son niveau, à ses besoins et à ses enjeux professionnels.

Moyens techniques

Un support pédagogique complet est remis à chaque participant. Les sessions s'appuient sur des ateliers pratiques Azure DevOps / GitHub Actions. Une connexion internet et un poste de travail sont requis pour les sessions à distance.

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants au moyen de mises en situation et d'ateliers pratiques. Une attestation de fin de formation est remise à l'issue du parcours.

Accessibilité et handicap

Nos formations peuvent être adaptées aux personnes en situation de handicap. Merci de nous contacter en amont afin d'étudier ensemble les modalités d'accueil et d'aménagement (référént handicap : contact@mfe-it.com).

Assistance post-formation

Chaque participant bénéficie d'un accompagnement de 30 jours après la formation pour toute question relative au contenu abordé.

INFORMATIONS PRATIQUES

Prise en compte du handicap

MFE-IT s'engage à étudier toute demande d'aménagement. Un échange avec notre référent handicap permet d'adapter les conditions d'accueil et de déroulement de la formation.

Modalités pédagogiques et techniques

Formation en distanciel (classe virtuelle synchrone) ou en présentiel dans vos locaux, en mini-groupe. Alternance de théorie et d'ateliers pratiques sur des pipelines CI/CD sécurisés.

Moyens du formateur

Formateur expert du domaine, support de cours complet et ateliers pratiques Azure DevOps / GitHub Actions.

Validation et sanction

Attestation de fin de formation remise à chaque participant.

Type de formation

Action de formation professionnelle continue : acquisition et perfectionnement de compétences.

Suivi de l'exécution

Feuilles de présence signées, évaluations en cours de formation et attestation de fin de formation.

Modalités d'évaluation

Mises en situation et ateliers pratiques tout au long de la formation.

Aide à l'orientation

Cette formation complète un parcours DevOps / cloud sur Azure (Azure DevOps, GitHub Actions, conteneurs et Kubernetes).