Sécurité défensive

DevSecOps par la pratique

3 jours (21h00) | ★★★★½ 4,6/5 | SEC-PLATDVO | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Identifier les enjeux de sécurité du DevSecOps
- Déterminer les impacts de la sécurité sur de la livraison continue
- Monter en compétence sur les notions d'automatisation de la sécurité dans une chaîne de CI/CD
- Décrire les nouvelles pratiques sécurité dans un contexte DevOps
- Porter un regard critique sur les notions de DevSecOps
- Utiliser les différents outils de sécurité
- Participer à la communauté DevSecOps et aux communautés d'experts.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir suivi les formations Ansible, Terraform, Docker, Kubernetes ou disposer d'un niveau administrateur sur ces technologies. Avoir de bonnes connaissances générales en informatique, développement, infrastructures et réseaux et une bonne maîtrise d'un Cloud Provider AWS, Azure ou GCP.

Public concerné

Responsables IT, chefs de projets IT, architectes infrastructure / Cloud, administrateurs infrastructure / système / Cloud, Devops, CloudOps, SRE, responsables de solutions, développeurs d'applications, ingénieurs réseaux, ingénieurs systèmes et sécurité.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Comprendre le DevSecOps

Introduction au DevSecOps

- Rappel de la notion DevOps
- Qu'est-ce que l'Infrastructure as Code ?
- Qu'est-ce que le CI/CD ?

Les défis et contraintes dans le DevOps

- Comment évoluent les méthodes de développement ?
  - Principe de la béta perpétuelle
  - "Release early, release often"
- Les technologies Cloud native
  - Les microservices avec les conteneurs
- Quelles menaces identifiées ?
- Top 12 des menaces par le CSA

Exemples de travaux pratiques (à titre indicatif)

- *Travaux dirigés : mettre en place une veille DevSecOps*
  - *Identifier les ressources Internet pertinentes pour réaliser sa veille DevSecOps*

Considérations générales sur la sécurité en mode DevOps

Comment assurer la conformité ?

- Mettre en conformité des environnements et des pratiques
  - Center for Internet Security
  - ISO 270XX
  - Cloud Security Alliance
- Compliance as Code, ou comment améliorer les processus de mise en conformité :

- Automatisation des tests et validations
- Mise en place de nouveaux processus

Quelle est l'importance de bien gérer l'identité dans un environnement DevOps ?

- Comprendre la notion d'identité et les challenges associés

Comment injecter la sécurité dans un processus DevOps ?

- Gagner en contrôle
- "Security by default"
- Architecture sécurisée

Qu'est-il possible de faire pour renforcer la sécurité ?

- Analyser les risques
- Sensibiliser
- Mettre en place des "war games"
- Réaliser du "hunting" et des audits
- Déployer des outils de "Chaos Engineering"

Exemples de travaux pratiques (à titre indicatif)

- *Réaliser du "hunting" et de l'analyse de logs*
- *Déployer et utiliser un outil de "Chaos Engineering"*
  - *Déploiement d'un cluster Kubernetes*
  - *Déploiement d'une application 3 tiers*
  - *Déploiement de l'outil de "Chaos Engineering"*
  - *Injection de dysfonctionnements dans le fonctionnement de l'application*
  - *Analyse des logs*

Implémenter la sécurité au niveau infrastructure

Existe-t-il des différences de management entre le On-Premise et le Cloud public ?

- Une philosophie : "Cattle vs Pets"

L'automatisation, une réponse directe aux nouveaux défis du Cloud

- Comprendre les apports de l'automatisation et de l'orchestration
- Tour d'horizon des outils
- Les bonnes pratiques : que faut-il faire ?

Exemples de travaux pratiques (à titre indicatif)

- *Automatisation et orchestration du déploiement d'un application*
  - *Automatisation des composants d'une application 3 tiers*
  - *Orchestration du déploiement de l'application 3 tiers*
  - *Modification de l'environnement et détection de l'anomalie depuis les outils d'automatisation et d'orchestration*
  - *Sécurisation et retour à la normale*

Le monitoring, ou comment gagner en contrôle et visibilité

- Les enjeux du monitoring en matière de sécurité
- Comment utiliser correctement les outils de monitoring en termes de sécurité ?

Exemple de travaux pratiques (à titre indicatif)

- *Utilisation d'un outil de monitoring pour détecter des anomalies*

La gestion des données, pilier de la sécurisation des infrastructures

- Comment protéger des données sensibles
  - Mise en place d'un Vault
  - Gestion des secrets
- Application des bonnes pratiques de virtualisation
  - Sauvegarde

Exemples de travaux pratiques (à titre indicatif)

- *Déploiement d'un Vault et injection SSL*
  - *Injection automatisée d'un certificat SSL dans un service Web depuis un Vault*
- *Automatisation de la sauvegarde*
  - *Automatisation de la sauvegarde à la création d'une charge de travail dans un Cloud public*

Microservice - Sécurisation d'un environnement conteneurisé

- Le cas de Kubernetes
- Que trouve-t-on au sein de la CNCF en matière de sécurité ?
  - Les notions de "Service Mesh"
  - Les projets de sécurité et de conformité

Exemples de travaux pratiques (à titre indicatif)

- *Injection SSL avec le "Service Mesh"*
- *Gestion de la segmentation avec les "NetworkPolicies"*
- *Gestion des stratégies*
  - *Utilisation de OPA et/ou Kyverno*
- *Gestion de la sécurité dynamique*
  - *Utilisation de Falco*

Implémenter la sécurité au niveau du développement

- Quelles sont les bonnes pratiques de développement ?
- Pour des applications dites microservices
  - 12 facteurs (vers les 15 facteurs)
  - L'intérêt des revues de code
  - Le "Pair Programming"
- Qu'en est-il de la sécurité dans un contexte de livraison continue ?
- Qu'est-ce que le SBOM (Software Bill of Materials) ?
- Le testing, élément de consolidation essentiel pour un développement sécurisé
- Quoi ? Comment ? Les bonnes pratiques :
  - TDD, Scanning, principe de validation "White Box"
  - Domaines à tester (Web, virtualisation, container...)
- Qu'avons-nous à disposition pour implémenter ce testing ?

Exemples de travaux pratiques (à titre indicatif)

- *Utilisation d'un outil de SBOM*
- *Scan de containers*

Communauté DevSecOps

- Quelles communautés ?
  - En France
  - Dans le monde
- Quelles sources d'information incontournables ?
- Comment contribuer à la communauté ?

Exemple de travaux pratiques (à titre indicatif)

- *Travaux dirigés : identifier les 3 dernières failles critiques dans Kubernetes ou dans une des solutions Graduated CNCF et leur résolution*

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Les + de la formation

Cette formation propose une vision complète du DevSecOps, des enjeux aux solutions du marché, par une mise en pratique importante.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.