

Pentest Cloud et conteneurs

5 jours (35 heures)

Expertise

Présentiel ou classe à distance

à partir de

4 375 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

Objectifs

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

- Cartographier et sécuriser les environnements Cloud (AWS, Azure, GCP) pour préparer un pentest
- Utiliser des outils automatisés (Prowler, ScoutSuite) et manuels pour détecter les mauvaises configurations et vulnérabilités
- Exploiter les faiblesses de services Cloud (IAM, S3, Lambda, Azure AD) pour obtenir un accès initial
- Auditer et attaquer des plateformes de conteneurs (Docker, Kubernetes) à l'aide de kube-hunter, Trivy et mise à jour de policies
- Rédiger un rapport complet incluant les recommandations de durcissement et de remédiation.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Pentesters et consultants Cloud, ingénieurs DevOps / DevSecOps, administrateurs Cloud et Kubernetes, auditeurs de sécurité et équipes SOC / IR.

Prérequis

Avoir des connaissances de base des services AWS / Azure / GCP, une expérience avec Docker et les principes Kubernetes ainsi qu'une familiarité avec Linux shell et scripting de base.

Programme

1 Pendant votre formation

Pentest Cloud et conteneurs

Jour 1 – Matin

Introduction au pentest Cloud

- Scope
- Limites (responsabilité partagée)
- Aspects légaux Cloud

Cartographie d'un environnement Cloud

- Architecture
- Comptes
- RBAC
- Network flows

Exemple de travaux pratiques (à titre indicatif)

- Création d'un compte de test AWS / Azure / GCP et configuration minimaliste

Jour 1 – Après-midi

Reconnaissance et discovery automatisés

- Prowler pour AWS CIS benchmarks
- ScoutSuite pour Multi-Cloud

Exemple de travaux pratiques (à titre indicatif)

- Exécution et interprétation d'un scan ScoutSuite

Jour 2 – Matin

Analyse manuelle des configurations IAM

- Escalade de privilèges via IAM misconfigurations (role chaining, politiques trop larges)

Exemple de travaux pratiques (à titre indicatif)

- Exploitation d'une policy AWS trop permissive

Jour 2 – Après-midi

Attaques sur services Cloud courants

- S3 bucket enumeration / exfiltration, Azure Blob, GCP Storage
- Exploitation de fonctions serverless (Lambda, Azure Functions)

Exemple de travaux pratiques (à titre indicatif)

- *Injection de payload dans une fonction serverless*

Jour 3 – Matin

Pentest Kubernetes : reconnaissance et énumération

- kube-hunter pour discovery
- Kubernetes API enumeration (kubectf)

Exemple de travaux pratiques (à titre indicatif)

- *Identification de namespaces, pods sensibles*

Jour 3 – Après-midi

Vulnérabilités de conteneurs

- Scanning d'images avec Trivy, Clair, Anchore
- Durcissement Dockerfile et posture run-as-non-root

Exemple de travaux pratiques (à titre indicatif)

- *Scan et remédiation d'une image vulnérable*

Jour 4 – Matin

Attaques de cluster Kubernetes

- Exploitation de misconfigurations RBAC
- Escalade de privileges dans le cluster
- Exécution de pods malveillants pour lateral movement

Exemple de travaux pratiques (à titre indicatif)

- *Compromise d'un cluster lab via un ServiceAccount exposé*

Jour 4 – Après-midi

Post-exploitation et pivot Cloud / conteneurs

- Exfiltration de secrets (Kube secrets, AWS keys)

Exemple de travaux pratiques (à titre indicatif)

- *Extraction et utilisation de secrets pour attaquer d'autres ressources*

Jour 5 – Matin

Capture-the-Flag Cloud et conteneurs – phase 1

- Mise en place d'un lab mixte (Cloud et k8s)
- Exécution guidée d'un scénario complet

Jour 5 – Après-midi

Capture-the-Flag – phase 2 et restitution

- Consolidation des findings, rédaction d'un rapport Cloud pentest

- Présentation des recommandations de durcissement et best practices
- Clôture et retours d'expérience

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités 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

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 4 octobre 2027 au 8 octobre 2027 (5 jours / 35 heures)

À distance

Du 4 octobre 2027 au 8 octobre 2027

À distance

- 4 octobre 2027 9h00 - 15h00
- 5 octobre 2027 9h00 - 15h00
- 6 octobre 2027 9h00 - 15h00
- 7 octobre 2027 9h00 - 15h00
- 8 octobre 2027 9h00 - 15h00