MAJ 25/10/2024

# Formation « Sécurité des environnements cloud »

**Réf : PENTESTCLOUD**

**À l'ère où les infrastructures cloud et les pratiques DevOps prédominent, il est crucial de comprendre et de sécuriser chaque étape de leur cycle de développement. L'objectif de cette formation est de vous permettre d'identifier les différents vecteurs d'attaques, tout en vous apportant des compétences nécessaires pour exploiter et corriger les vulnérabilités dans des environnements utilisant ces technologies (versioning, IaC, CI/CD, Kubernetes, AWS, etc.). Au travers d'une approche offensive, apprenez à intégrer au mieux la sécurité dans l'ensemble des briques que contiennent vos cycles de développement logiciel afin de protéger vos applications et données dans le cloud.**

## Objectifs

- Comprendre le fonctionnement et les risques de sécurité inhérent aux solutions de développement agile
- Identifier les points faibles de ce type d'infrastructures
- Exploiter les faiblesses afin d'en évaluer l'impact
- Comprendre les solutions de remédiations les plus efficaces

## Durée & horaires

- 4 jours soit 28 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

## Nombre de participant

- Minimum 8 participants – Maximum 15 participants

## Public visé

- Pentesters
- Consultants SSI
- RSSI
- Architectes Cloud
- DevOps

## Pré-requis

- Des notions en IT et/ou SSI
- Notions d'utilisation d'un système Linux
- Notions relatives aux services standards d'AWS (IAM, Réseaux, Calculs)

## Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables lors d'audits
- Une infrastructure vulnérable fidèle à la réalité sert de plateforme pour les tests
- Tous les outils utilisés sont issus du monde libre et peuvent être réutilisés librement en dehors de la formation
- Les techniques et outils classiques ainsi que modernes sont utilisés tout au long de la formation

## Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé
- Ordinateur portable prêté pour la réalisation des exercices

## Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

- **Evaluation de pré-formation envoyée avant le début de la formation**
- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**
- **Examen final à la fin de la formation (cf certification)**

**Ces évaluations ont pour but de valider les compétences acquises.**

## Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTCLOUD par HS2.**

## Programme

**Introduction aux environnement agiles**

- Introduction générale
- Présentation des concepts et technologies

**Outils DevOps et CI/CD**

- Présentation des concepts et technologies
- Outils DevOps et CI/CD :
  - Présentation du fonctionnement (Gitlab CI, Github Action, Jenkins, etc.)
  - Sécurisation des secrets
  - Exercice : récupération de secrets
  - Gestion des droits
  - Gestion des runners
  - Exercices :
    - Attaque de supply chain (artifact poisoning, etc.)
    - Pipeline poisoning (shared runners abuse, container escape, déplacement latéral, etc.)
- Infrastructure As Code (IaC):
  - Introduction et présentation des technologies (Terraform, CloudFormation)
  - Présentation des risques
  - Exercices :
    - Template backdooring
    - Développement d'un module malveillant
    - Exploitation de tfstate
- Bonne pratiques et mesures correctives

**Cloud**

- Introduction
  - Concepts et services principaux :
    - Gestion des identités (IAM, policies, roles, boundaries, SCP, etc.)
    - Gestion réseau (cloisonnement, VPC, ACL/SG, peering, etc.)
    - Gestion des secrets (Secrets Manager, SSM, etc.)
    - Serverless (Lambda, Fargate, etc.)
- Exercices :
  - Élévation de privilèges au travers de divers services (confused deputy, assume role.)
  - Contournement de restrictions réseau
  - Récupération de secrets dans divers ressources (user data, stack cloudformation, etc.)
  - Persistance (role backdooring, lamda backdooring, etc.)
    - Usine logiciel, conteneurisation et orchestration :
  - Gestion des images (AMI, ECR)
  - Fondamentaux Kubernetes (composants, k8s vs EKS, etc.)
  - Modèle de sécurité (méthode d'authentification, NetworkPolicy, RBAC, etc.)
    - Exercices :

- Reconnaissance
- Elévation de privilèges (role abuse, container escape, volume access, etc.)
  - Bonne pratiques et mesures