Pentest des infrastructures cloud (AWS, Azure, GCP) : techniques et outils

Lien : https://innov-systems.com/formation/pentest-des-infrastructures-cloud-aws-azure-gcp-techniques-et-outils

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI113**	**Pentest**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les architectures cloud AWS, Azure et GCP
- Identifier les vulnérabilités spécifiques aux environnements cloud
- Réaliser des tests d’intrusion en environnement cloud public
- Auditer les configurations IAM et réseaux cloud
- Détecter les mauvaises configurations de stockage et services
- Utiliser les outils de pentest cloud (Prowler, ScoutSuite, Pacu)
- Simuler des attaques cloud et scénarios d’exploitation
- Évaluer les risques liés aux services managés et serverless
- Rédiger des rapports de pentest professionnels
- Proposer des plans de remédiation efficaces
- Renforcer la posture de sécurité des infrastructures cloud
- Étudier des cas concrets de compromission cloud

POUR QUI ?

- Pentesters / Ethical hackers
- Cloud security engineers
- DevSecOps engineers
- Security analysts
- SOC analysts
- Cloud architects
- Administrateurs cloud
- Consultants cybersécurité
- Red teamers
- Ingénieurs infrastructure IT
- RSSI / CISO
- Toute personne impliquée dans la sécurité des environnements cloud publics

Innov Systems

Programme détaillé

1 / Introduction au pentest cloud

- Spécificités des environnements cloud publics
- Modèle de responsabilité partagée (AWS, Azure, GCP)
- Types de tests d’intrusion en environnement cloud

2 / Architecture des infrastructures cloud

- Composants IaaS, PaaS et SaaS
- Réseaux virtuels, IAM et services managés
- Surface d’attaque des environnements cloud

3 / Reconnaissance et cartographie cloud

- Identification des assets exposés
- Enumération des services cloud publics
- Analyse des configurations initiales

4 / Sécurité et audit des identités (IAM)

- Analyse des rôles et politiques IAM
- Escalade de privilèges dans le cloud
- Mauvaises configurations d’accès

5 / Tests de sécurité réseau cloud

- VPC, Security Groups et NSG
- Exposition des ports et services
- Attaques sur endpoints cloud

Innov Systems

6 / Sécurité des stockages cloud

- S3, Blob Storage, Cloud Storage
- Mauvaises configurations et fuites de données
- Analyse des permissions et accès publics

7 / Sécurité des services managés

- Bases de données cloud (RDS, Azure SQL, Cloud SQL)
- Containers et Kubernetes managés
- Fonctions serverless et risques associés

8 / Outils de pentest cloud

- AWS CLI, Azure CLI, GCP SDK
- ScoutSuite, Prowler, Pacu, CloudSploit
- Frameworks de sécurité cloud

9 / Exploitation et post-exploitation

- Escalade de privilèges cloud-native
- Persistence dans les environnements cloud
- Exfiltration de données et détection

10 / Reporting et remédiation

- Rédaction de rapports de pentest cloud
- Recommandations de correction
- Bonnes pratiques de sécurisation cloud

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

07 au 11 Déc. 2026	Distanciel
12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés