Forensics cloud et investigation d'incidents dans les environnements AWSAzure

Lien : https://innov-systems.com/formation/forensics-cloud-et-investigation-dincidents-dans-les-environnements-awsazure

DURÉE
5 jours (35h)

RÉFÉRENCE
SI96

CATÉGORIE
Analyse Apres Incident : Analyse Forensique, Investigation Numérique et Plan de Continuité

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes du cloud forensics en AWS et Azure
- Collecter et analyser les preuves numériques dans le cloud
- Maîtriser les outils natifs et solutions de sécurité cloud
- Identifier les compromissions et activités suspectes
- Mettre en place une chaîne de conservation des preuves fiable
- Réaliser des investigations sur workloads cloud
- Automatiser les processus d’investigation et de réponse
- Corréler les logs multi-sources pour analyse d’incidents
- Sécuriser les environnements cloud après incident
- Respecter les contraintes légales et réglementaires
- Améliorer la détection et la réponse aux attaques cloud
- Étudier des cas concrets d’incidents en environnement cloud

POUR QUI ?

- Cloud security engineers
- SOC analysts
- Incident responders
- Forensic analysts
- DevSecOps engineers
- Cloud architects
- Administrateurs AWS/Azure
- RSSI / CISO
- Consultants cybersécurité cloud
- Data engineers sécurité
- Threat hunters
- Toute personne impliquée dans la sécurité et l’investigation des environnements cloud

Innov Systems

Programme détaillé

1 / Introduction au cloud forensics

- Principes de l'investigation numérique en environnement cloud
- Différences entre forensics on-premise et cloud
- Défis liés à la volatilité et à la distribution des données

2 / Architecture des environnements AWS et Azure

- Composants clés AWS (EC2, S3, IAM, CloudTrail)
- Composants clés Azure (VM, Blob Storage, Azure AD, Activity Logs)
- Points de collecte de preuves numériques

3 / Chaîne de conservation des preuves (chain of custody)

- Principes de collecte et préservation des preuves
- Intégrité et traçabilité des données
- Documentation légale des investigations

4 / Collecte des logs et données cloud

- Logs AWS CloudTrail, CloudWatch, VPC Flow Logs
- Azure Monitor, Azure Sentinel et Activity Logs
- Centralisation et corrélation des événements

5 / Investigation des incidents cloud

- Identification des accès suspects et compromissions
- Analyse des comportements anormaux IAM
- Détection de mouvements latéraux dans le cloud

Innov Systems

6 / Analyse des workloads et ressources compromises

- Forensique sur machines virtuelles
- Analyse des conteneurs et services serverless
- Investigation sur stockage objet (S3 / Blob)

7 / Outils et techniques de cloud forensics

- Outils natifs AWS et Azure
- Solutions SIEM et SOAR (Sentinel, Splunk, etc.)
- Automatisation des investigations

8 / Réponse aux incidents en environnement cloud

- Isolation des ressources compromises
- Remédiation et récupération des environnements
- Coordination avec CSIRT et équipes cloud

9 / Sécurité, conformité et aspects juridiques

- Contraintes réglementaires (RGPD, NIS2)
- Juridiction et localisation des données cloud
- Collaboration avec fournisseurs cloud

10 / Cas pratiques et scénarios d’investigation

- Investigation d’une compromission IAM
- Analyse d’un incident sur stockage cloud
- Simulation complète de réponse à incident 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

25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca
06 au 10 Sep. 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