Développez vos talents
Certifiez vos compétences

Cloud privé et hybride / Multi-Cloud

Sécurité Pentest et déploiement dans le Cloud

5 jours (35h00) | ★★★★½ 4,6/5 | CLOUD-SEC | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cloud › Cloud privé et hybride / Multi-Cloud

À l'issue de ce stage vous serez capable de :

- Maîtriser les mesures de sécurité Cloud
- Connaître les stratégies de déploiement sécurisé dans le Cloud
- Maîtriser les méthodologies de tests d'intrusions dans le Cloud
- Effectuer des tests d'intrusion dans Cloud
- Sécuriser ses infrastructures Cloud.

Niveau requis

Avoir des connaissances de base des systèmes, réseaux, Cloud et en cybersécurité est préférable.

Public concerné

Directeurs du système d'information ou responsables du service informatique, Chefs de projet et toute personne en charge de la sécurité du Cloud Computing, responsables et chefs de projet, pentesteurs, auditeurs et architectes réseaux et systèmes.

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.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les 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.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

La sécurité des données dans le Cloud

- Les données dans le Cloud
  - Cycle de vie
  - Classification
  - Anonymisation
  - Pseudonymisation
  - Tokenisation
- L'approches BYOK (Bring Your Own Key) et les solutions HSM dans le Cloud
- Le CASB (Cloud Access Security Broker)
  - Principes
  - Solutions

Les référentiels de la CSA (Cloud Security Alliance)

- Les 14 domaines du Security Guidance for Critical Areas of Focus in Cloud Computing
- La certification CCSK (Certificate of Cloud Security Knowledge)
- La CCM (Cloud Controls Matrix) et le CAIQ (Consensus Assessments Initiative Questionnaire)
- Le framework de certification OCF et l'annuaire STAR (Security, Trust and Assurance Registry)
- Le code de conduite RGPD (CoC GDPR) pour les fournisseurs

Les risques dans le Cloud Computing selon l'ENISA (European Network and Information Security Agency)

- Evaluation et gestion des risques du Cloud par la norme ISO 27005
- Les spécificités de la gestion des risques dans le Cloud
- Les principaux risques identifiés par l'ENISA

L'évaluation de la sécurité des fournisseurs

- Panorama des certifications / qualifications (SecNumCloud, SSAE18, HDS...)
- La certification de sécurité européenne issue du Cybersecurity Act
- Intérêts et limites de la certification ISO 27001 pour les services Cloud

Découverte, reconnaissance et architecture à grande échelle

- Méthodologie d'évaluation de sécurité dans le Cloud
- Conditions d'utilisation et points de démarcation
- Domaines et certificats pour l'énumération
- Découverte d'hôte avec Masscan et Nmap
- Git Mirroring
- Services et bases de données dans le Cloud
- Reconnaissance et découverte grâce au suivi visuel

Mappage, authentification et services Cloud

- API
- SDK Cloud
- AWS / IAM et privilèges
- Création et utilisation de listes de mots puissantes
- Transformer les jetons en accès
- Persistance via AWS / IAM

Azure et services Windows dans le Cloud

- Azure Active Directory
- VHD et clichés instantanés de volume
- SAML et Microsoft ADFS
- Conteneurs Windows
- Rôles Azure
- API Microsoft Graph
- Office 365

Vulnérabilités dans les applications natives du Cloud

- Découverte de métadonnées AWS / IAM
- Kubernetes et évasions
- Actions Travis CI et Git
- Mouvement latéral à travers des conteneurs
- Conteneurs privilégiés et non privilégiés

Exploitation et Red Team dans le Cloud

- Techniques de "Red Teaming" et méthodologies
- Techniques d'exploitation avancé dans le Cloud
- OWASP (Open Web Application Security Project) : le top 10
- Exploitation
  - Azure AD
  - De vulnérabilités AWS
- Test d'exposition

La sécurité des infrastructures et des plateformes de Cloud Computing

- Les composants de l'infrastructure du Cloud Computing
- Evaluation des risques de l'infrastructure du Cloud Computing
- Conception et planification des contrôles de sécurité
- Conception et déploiement de plan de reprise et de continuité des services et des métiers

La sécurité des applications de Cloud Computing

- Formation et sensibilisation de la sécurité autour des services du Cloud Computing
- Validation et assurance des solutions logicielles du Cloud Computing
- Utilisation des logiciels vérifiés et approbation des API
- SDLS (Symmetric Digital Subscriber Line) : cycle de vie du développement de la sécurité logicielle
- Les architectures applicatives du Cloud Computing
- Conception et déploiement d'une solution d'IAM (Identity and Access Management)

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)