Sécurité Cloud & Identity Access Management (IAM)

Maîtriser les fondamentaux de la sécurité Cloud et de la gestion des identités et des accès

Stage pratique
Sécurité

Code :
SCIAM

Durée :
1 jour(s) (7,00 heures)

Exposés : **60 %**
Cas pratiques : **20 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 990,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Cette formation introduit les concepts fondamentaux de la sécurité Cloud et de l'Identity & Access Management (IAM), devenus essentiels dans les environnements numériques modernes.

Les participants acquerront une compréhension des architectures Cloud, des principes de sécurisation des infrastructures et des enjeux liés à la gouvernance des identités et des accès. La formation couvre également les mécanismes d'authentification et d'autorisation, ainsi que les principales menaces et vulnérabilités propres aux environnements Cloud.

À l'issue de la formation, les participants disposeront d'une vision globale des bonnes pratiques permettant de renforcer la sécurité des usages et des systèmes d'information dans le Cloud.

OBJECTIFS PEDAGOGIQUES

- Analyser les enjeux et les impacts de la sécurité dans les environnements Cloud
- Expliquer et appliquer les principes fondamentaux de l'Identity & Access Management (IAM)
- Mettre en œuvre les bonnes pratiques de sécurité Cloud afin de réduire les risques liés aux accès, aux configurations et à la protection des données

PUBLIC CIBLE

Collaborateurs, managers SI et SSI, ainsi que toute personne souhaitant acquérir une compréhension des fondamentaux du Cloud et de l'IAM, sans exercer directement d'activités opérationnelles liées à ces domaines.

PRE-REQUIS

Connaissances générales en informatique (IT) et d'une sensibilisation aux principes fondamentaux de la sécurité des systèmes d'information (SSI).

METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

INTRODUCTION AU CLOUD : EXPLIQUER LES FONDAMENTAUX DU CLOUD COMPUTING ET ANALYSER L'ÉVOLUTION DES MODÈLES DE SÉCURITÉ INDUITE PAR LES ENVIRONNEMENTS CLOUD

- Les différents modèles de Cloud : public, privé et hybride
- Les modèles de déploiement et de services Cloud (IaaS, PaaS, SaaS)
- Les principaux fournisseurs de services Cloud (Cloud Providers)
- Les approches multi-cloud et hybrides

ANALYSER LES PRINCIPES DE GOUVERNANCE ET DE SÉCURITÉ CLOUD AFIN DE DISTINGUER LES RESPONSABILITÉS DES DIFFÉRENTS ACTEURS ET APPLIQUER LES CONCEPTS FONDAMENTAUX DE SÉCURISATION DES ENVIRONNEMENTS CLOUD

- Le modèle de responsabilité partagée
- Les différences entre les approches de sécurité on-premise et Cloud
- Les principes de gouvernance sécurité : politiques, standards et conformité
- Les concepts clés de sécurité Cloud :
  - Zero Trust
  - Security by Design
  - Défense en profondeur
  - Shift Left Security

LA SÉCURITÉ CLOUD : IDENTIFIER ET ANALYSER LES PRINCIPALES MENACES ET LES DÉFIS DE SÉECURITÉ PROPRES AUX ENVIRONNEMENTS CLOUD

- Paysage des menaces dans le Cloud
- Challenges clés
- Vision opérationnelle de la sécurité Cloud
- Evolution de la maturité de la sécurité Cloud
- Modernisation de la sécurité Cloud

COMPRENDRE ET EXPLIQUER LES PRINCIPES D'UNE ARCHITECTURE CLOUD SÉCURISÉE AFIN D'IDENTIFIER LES CONTRÔLES TECHNIQUES ESSENTIELS À LA SÉCURISATION DES ENVIRONNEMENTS CLOUD

- Landing Zones
- Identités et accès
- Protection des données
- Réseau et exposition
- Logs et supervision

COMPRENDRE ET COMPARER LES PRINCIPALES SOLUTIONS DE SÉCURITÉ CLOUD AFIN D'IDENTIFIER L'APPORT DES APPROCHES PLATEFORMES DANS LA GESTION DES RISQUES CLOUD

- Introduction CPSM/CNAPP
- Fonctionnalités CNAPP
- CNAPP : un marché prolifique
- Opérationnalisation de la sécurité sur une plateforme CNAPP
- L'importance croissante de l'IA

INTRODUCTION A L'IAM (IDENTIFY & ACCESS MANAGEMENT)

- Expliquer les fondamentaux de l’Identity & Access Management (IAM)
- Distinguer les différents types d’identités, mécanismes d’accès et concepts associés

GESTION DES IDENTITÉS DANS LE CLOUD

- Cycle de vie des identités
- Comptes à privilèges et enjeux associés à leur sécurisation
- Différences entre identités humaines et non humaines
- Fédération d’identités et SSO (vue d’ensemble)

GESTION DES ACCÈS ET AUTHENTIFICATION

- Mots de passe et Mise en place des mécanismes d'authentification forte (MFA, SSO)
- Accès conditionnels, gestion des secrets et des clés, accès temporaires
- Définition des rôles et des droits basés sur le principe du moindre privilège et gestion du cycle de vie des identités (création, modification, suppression)

MENACES ET RISQUES LIÉS AU CLOUD ET A L'IAM

- Compromission des comptes et fuite de données
- Mauvaises configurations et leurs impacts sur la sécurité Cloud
- Phénomène de Shadow IT et les risques associés
- Attaques ciblant les API et les services exposés
- Anticipation des impacts liés aux nouvelles menaces, usages et technologies émergentes

BONNES PRATIQUES DE SÉCURITÉ CLOUD ET IAM

- Sécurisation des comptes administrateurs et revue régulière des droits
- Segmentation des environnements, sauvegardes et résilience

CONCLUSION

- Synthèse de la journée
- Rappel des messages clés
- Évaluation finale

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com