Sécurité Cloud pour éditeurs de logiciels SaaS

Durée : 2 jours (14 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des architectures Cloud et des applications Web.
- Maîtrise des concepts de développement logiciel et d'architecture applicative.
- Une expérience dans le développement, l'exploitation ou l'administration d'environnements Cloud est recommandée.

PROFIL DES STAGIAIRES

- Architectes logiciels et Cloud
- Développeurs et Lead Developers
- DevOps et DevSecOps
- CTO et responsables techniques
- Responsables cybersécurité
- RSSI
- Product Owners techniques
- Éditeurs de logiciels SaaS souhaitant renforcer la sécurité de leurs plateformes Cloud.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les enjeux spécifiques de la sécurité des plateformes SaaS.
- Identifier les risques liés aux architectures Cloud modernes.
- Sécuriser les composants applicatifs et les infrastructures Cloud.
- Mettre en œuvre une gestion robuste des identités et des accès.
- Sécuriser les données des clients hébergées dans un environnement SaaS.
- Intégrer les principes de sécurité dans le cycle de développement logiciel.
- Renforcer la détection et la réponse aux incidents de sécurité.
- Construire une stratégie de sécurité adaptée à un éditeur SaaS.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et d'études de cas réels.
- Analyse d'incidents ayant affecté des plateformes SaaS.
- Ateliers collaboratifs de revue d'architecture.
- Exercices d'identification des risques et vulnérabilités.
- Études de cas orientées développement sécurisé et exploitation Cloud.
- Cas fil rouge permettant de construire une architecture SaaS sécurisée.

FORMATEUR

- Consultant expert en cybersécurité Cloud, architectures SaaS, DevSecOps et sécurité applicative disposant d'une expérience significative dans l'accompagnement d'éditeurs logiciels, de startups technologiques et d'entreprises développant des solutions SaaS.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Validation progressive des acquis à travers les ateliers et études de cas.
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestations des compétences acquises et de fin de stage adressée à chaque participant
- Questionnaire d'évaluation des acquis en fin de parcours.

CONTENU DU COURS

Jour 1 : Sécuriser l'architecture SaaS et protéger les données (7h)

Module 1 : Comprendre les enjeux de sécurité des plateformes SaaS (2h)

Objectifs

- Identifier les risques propres aux solutions SaaS.
- Comprendre les responsabilités de l'éditeur de logiciels.

Contenu

- Spécificités des modèles SaaS.
- Responsabilité partagée dans le Cloud.
- Multi-tenant et isolation des environnements.
- Menaces ciblant les plateformes SaaS.
- Risques liés aux API, aux accès et aux données.
- Retour d'expérience sur des incidents réels.

Mise en pratique

Brainstorming collectif :

- Identification des risques majeurs d'une plateforme SaaS hébergeant des données clients.

Module 2 : Concevoir une architecture Cloud sécurisée (2h)

Objectifs

- Sécuriser les composants techniques d'une plateforme SaaS.
- Réduire la surface d'exposition.

Contenu

- Architecture sécurisée dans le Cloud.
- Segmentation logique et réseau.
- Sécurisation des environnements de production.
- Gestion des secrets et des configurations.
- Haute disponibilité et résilience.
- Sécurisation des API et microservices.

Mise en pratique

Atelier :

- Analyse de l'architecture d'une plateforme SaaS et identification des points de faiblesse.

Module 3 : Gestion des identités et des accès (1h30)

Objectifs

- Renforcer le contrôle des accès utilisateurs et administrateurs.

Contenu

- Gestion des identités (IAM).
- Authentification forte (MFA).
- SSO et fédération d'identité.
- Gestion des rôles et habilitations.
- Comptes à privilèges.
- Sécurisation des accès administrateurs.

Mise en pratique

Étude de cas :

- Construction d'une matrice d'habilitation adaptée à un environnement SaaS.

Module 4 : Protection des données clients (1h30)

Objectifs

- Garantir la confidentialité et l'intégrité des données.

Contenu

- Classification des données.
- Chiffrement au repos et en transit.
- Gestion des clés de chiffrement.
- Sauvegarde et restauration.
- Sécurisation des données multi-clients.
- Exigences réglementaires.

Mise en pratique

Atelier :

- Élaboration d'une stratégie de protection des données pour une plateforme SaaS.

Jour 2 : Sécurité applicative, DevSecOps et résilience opérationnelle (7h)

Module 5 : Développement sécurisé des applications SaaS (2h)

Objectifs

- Intégrer la sécurité dès la conception des applications.

Contenu

- Secure by Design.
- Security by Default.
- Menaces applicatives courantes.
- Référentiel OWASP Top 10.
- Validation des entrées.
- Gestion sécurisée des sessions.
- Sécurisation des API.

Mise en pratique

Atelier :

- Analyse d'une application SaaS au regard des vulnérabilités OWASP.

Module 6 : Intégrer la sécurité dans la chaîne DevOps (2h)

Objectifs

- Automatiser les contrôles de sécurité.
- Réduire les risques liés aux cycles de développement.

Contenu

- Principes DevSecOps.
- Sécurité des pipelines CI/CD.
- Analyse de code.

- Gestion des dépendances logicielles.
- Gestion des vulnérabilités.
- Infrastructure as Code sécurisée.

Mise en pratique

Atelier :

- Identification des contrôles de sécurité à intégrer dans une chaîne de développement.

Module 7 : Supervision, détection et réponse aux incidents (2h)

Objectifs

- Détecter rapidement les incidents de sécurité.
- Organiser une réponse adaptée.

Contenu

- Journalisation et traçabilité.
- Surveillance des activités suspectes.
- Détection des compromissions.
- Gestion des vulnérabilités.
- Réponse aux incidents.
- Communication avec les clients en cas d'incident.

Mise en pratique

Étude de cas :

- Analyse d'un incident de sécurité affectant une plateforme SaaS.

Module 8 : Cas pratique de synthèse – Construire une plateforme SaaS sécurisée (1h)

Objectifs

- Mobiliser l'ensemble des compétences acquises.
- Formaliser une stratégie globale de sécurité.

Mise en pratique

Exercice fil rouge :

À partir d'un éditeur SaaS fictif :

- Analyse des risques.
- Sécurisation de l'architecture.
- Protection des données.
- Définition des contrôles DevSecOps.
- Mise en place de la supervision.
- Élaboration d'une feuille de route sécurité.
- Présentation des recommandations au groupe.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.