Sécurité opérationnelle dans le Cloud

Prix : 2 925 €HT

Durée : 3 jours

Code de Référence : CLOUDSECOPE

Catalogue Cloud Native et DevOps

Objectifs de la formation

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

- Identifier les principaux risques de sécurité liés aux environnements Cloud hybrides et multi-cloud
- Analyser les enjeux juridiques et contractuels d'un projet Cloud
- Mettre en œuvre les bonnes pratiques de sécurisation de l'infrastructure Cloud
- Configurer des dispositifs de sécurité réseau dans un environnement virtualisé
- Implémenter une stratégie IAM (gestion des identités et des accès) adaptée au Cloud
- Intégrer la sécurité dans les pipelines DevOps (DevSecOps)

Public

Cette formation s'adresse aux administrateurs systèmes, DevOps, responsables de la sécurité des SI (RSSI), architectes cloud, chefs de projet IT, ingénieurs réseau et sécurité, exploitants d'infrastructures cloud.

Prérequis

Connaissances fondamentales du Cloud (modèles de services et de déploiement) et bases en sécurité des systèmes d'information (réseaux, authentification, chiffrement, etc.)..

Programme de la formation

Jour 1 – Matin
Fondamentaux de la sécurité Cloud
Enjeux et spécificités de la sécurité dans le Cloud

- Cloud vs SI classique : quelle évolution des périmètres de sécurité ?
- Confidentialité, Intégrité, Disponibilité, Traçabilité… quelle sureté de fonctionnement dans le Cloud Computing
- Les modèles de responsabilités partagées entre Cloud Provider et Cloud Consumer
- Enjeux de sécurité liés au Cloud Computing

Quels référentiels et cadres règlementaires de sécurité

- Normes ISO 27001, 27005, 27017, 27018…
- Référentiels de sécurité : CSA CCM, ENISA CSF, ISAE3402, SOC 2/3, NIST SP 800-XXX, NIS2, DORA…
- Qu'en dit l'ANSSI… avec le SecNumCloud ?
- Que dire de l'EUCS (European Union Cybersecurity Certification Scheme for Cloud Services) ? Objectifs et impacts

Introduction à la sécurité réseau dans le Cloud

- Un modèle en couches hérité à adapter au Cloud Computing (protections par couches)
- Une surface d'exposition élargie nécessitant une surveillance renforcée
- Virtualisation du réseau et micro-segmentation
- Notion de "Zero Trust Network Architecture" dans le Cloud

Exemples de cas pratiques (à titre indicatif) :
Étude de cas : analyser une architecture Cloud sur la base du modèle partagé, cartographie des responsabilités et évaluation des zones critiques de sécurité
Analyser les principales menaces et vulnérabilités dans le Cloud Computing

Jour 1 – Après-midi
Analyse des risques et sécurité réseau avancée
Cartographie et typologie des risques Cloud

- Quelle cartographie des risques du Cloud Computing ?
- Les risques techniques et technologiques : failles et vulnérabilités, erreurs de configuration…
- Les risques organisationnels et juridiques : dépendance, non-conformité, juridictionnels…
- Quels sont les risques liés au Shadow IT ?
- Quelques exemples de menaces : hyperviseur, API, latéralisation…

Gestion des flux et interconnexions réseau Cloud

- Les enjeux de la sécurisation des flux réseaux dans le Cloud Computing
- Typologies des interconnexions et risques associés (Cloud-to-Cloud et Cloud-to-OnPremise)
- VPN, firewalls cloud-native et distribués, micro-segmentation et SASE (Secure Access Service Edge)
- Notions d'hybridation et sécurisation des flux inter-applications notamment pour les applications cloud natives et architectures orientées micro services

Exemples de cas pratiques (à titre indicatif) :
Évaluer les menaces sur un système hybride et cartographier les flux sensibles, matrice des risques associés
Analyser des intrusions exploitant des menaces et des vulnérabilités liées au Cloud Computing

Jour 2 – Matin
Aspects juridiques et gestion des identités (IAM)
Contrats Cloud et conformité juridique

- Contrats SaaS/IaaS/PaaS vs infogérance
- Clauses : SLA, sécurité, réversibilité, auditabilité, pénalités, coûts, cadre règlementaire…
- Outils contractuels : Cloud Auditor, grilles de conformité…
- Quelles exigences de sécurité pour des applications SaaS ?

IAM (Identity & Access Management) dans le Cloud

- Fondamentaux de l'IAM dans le Cloud Computing
- RBAC, ABAC, gestion du cycle de vie des identités
- Fédération d'identités : SAML, OIDC, ADFS, Entra ID (ex. Azure AD)
- Gestion des accès multi-Cloud et outils : Okta, Ping Identity, OneLogin…

Exemples de cas pratiques (à titre indicatif) :
Analyser, de manière critiques, de contrats d'applications SaaS
Mettre en place une fédération d'identités inter-applicative, définir la liste des protocoles et connecteurs nécessaires.

Jour 2 – Après-midi
Sécurité opérationnelle et gouvernance technique
Exploitation sécurisée d'un environnement Cloud

- Cloisonnement des environnements de prod/dev/test/sandbox…
- Journalisation, alerting et traçabilité
- Continuité et reprise d'activité PCA/PRA et sauvegardes, réplication, redondance
- Gouvernance du cycle de vie, audit et gestion de l'obsolescence : tags, CMDB, SAM…

Observabilité et gouvernance technique

- Observabilité Cloud : gestion de la supervision, du traçing et des logs…
- Les Cloud Management Platforms (CMP) : gestion multi-cloud, configuration, coûts et sécurité
- Tableaux de bord sécurité et indicateurs clés
- La gestion des incidents dans le Cloud et intégration avec les outils d'ITSM
- Gouvernance des rôles et responsabilités (rôle de la DSI, DevOps, SecOps…) : de l'importance d'un RACI clair et partagé

Exemples de cas pratiques (à titre indicatif) :
Déployer un environnement IaaS sécurisé avec mécanismes de supervision, configuration de sauvegardes et tableau de suivi sécurité.
Définir les outils à utiliser dans une Landing Zone sécurisée pour une application hébergée chez un Cloud Provider public

Jour 3 – Matin
Sécuriser les applications Cloud Native : Build & Deploy

Build – Intégrer la sécurité dès le développement et la construction

- Qu'est-ce que le DevSecOps ? Pourquoi adopter une posture shift left ?
  Sécurité dans le code : SAST, analyse de dépendances, politiques de codage sécurisé
- Construction d'images de containers : minimisation, durcissement, gestion des UID, bonnes pratiques de Dockerfile
- SBOM (Software Bill of Materials) : intérêt, outils (Syft, CycloneDX), automatisation
- CNAPP & scanners de build (Trivy, Grype, Checkov…) : premiers contrôles dès le commit

Deploy – Sécuriser l'Infrastructure as Code et les déploiements CI/CD

- Risques liés à l'IaC : quelles vulnérabilités fréquentes dans les fichiers Terraform, Ansible… ?
- Scanners IaC : tfsec, Checkov, KICS, intégration dans le pipeline
- Sécurisation des secrets et configurations (Vault, SOPS, Sealed Secrets)
- GitOps sécurisé : auditabilité, contrôle des merges, GitOps pull vs push
- CI/CD sécurisé : signature d'image, scan automatique, contraintes de conformité
- Admission controllers Kubernetes (OPA/Gatekeeper, Kyverno) : bloquer les déploiements non conformes

Exemples de cas pratiques (à titre indicatif) :
Réaliser une analyse de sécurité sur image Docker avec Trivy & construire une pipeline CI/CD intégrant des scanners IaC et un contrôleur d'admission.

Jour 3 – Après-midi
Sécuriser les applications Cloud Native : Run & Respond
Run – Durcir et surveiller la plateforme d'exécution

- Sécurité des containers : moteur containerd/CRI-O, isolation, exécution en rootless, readonly FS
- Sécurité des nœuds : OS minimal (Talos, Bottlerocket, Flatcar), activation de seccomp, AppArmor, SELinux
- Sécurité native Kubernetes : RBAC et Network Policies, Security Contexts et PodSecurity Standards (PSS), Gestion des secrets, journaux et audit logs…
- Intégration d'un service mesh (Istio, Linkerd) pour sécuriser les communications

Respond – Observer, détecter, réagir en cas d'incident

- Quelles traces et signaux surveiller : logs, métriques, évènements runtime ?
- Outils de détection et réponse : Falco (eBPF), Audit Logs K8s, Prometheus, Loki
- Intégrer un CNAPP ou SIEM cloud native pour corréler et alerter
- Bonnes pratiques de réponse : rollback GitOps, rotation de secrets, pause de workloads
- Chaos Engineering pour valider la résilience sécuritaire

Exemples de cas pratiques (à titre indicatif) :
Déployer une application sur K8S avec RBAC, PSS et NetworkPolicy & détecter un comportement anormal avec Falco et rollback GitOps

Méthodes pédagogiques

- Ce cours se présente sous la forme d’un séminaire ponctué de démonstration afin d’illustrer les concepts théoriques abordés.

- Le formateur tient compte de la situation de chaque apprenant et se base sur les expériences, les connaissances et les questions particulières des participants pour nourrir le groupe de cas concrets et de retours d’expériences ciblées

Les supports de formation seront les suivants :

- Présentation théorique au format pdf

Ces supports seront fournis aux participants au cours de la formation au format PDF.

Méthodes d’évaluation des acquis

Avant la formation :

- Le questionnaire de positionnement et d’auto-évaluation des compétences adapté à la formation :
  - Complété individuellement par chaque stagiaire avant la formation
  - Permet de recueillir et de mettre à disposition du formateur avant la formation

En cours de formation :

- Points d’étapes réguliers par le formateur sur la compréhension des stagiaires, de la réponse de la formation à leurs attentes et à leurs besoins
- Retour d’expérience en fin de journée de formation pour ajustements éventuels de la suite de la formation.

Après la formation « à chaud » :

- Le questionnaire d’auto-évaluation des compétences complété individuellement par chaque stagiaire après la formation et ajusté (si besoin) puis validé par le formateur en fonction des évaluations réalisées en cours de formation.
- Le questionnaire de satisfaction « à chaud » complété individuellement par chaque stagiaire en fin de formation.
- Le compte rendu formateur complété par le formateur.

Après la formation « à froid » :

Le questionnaire de satisfaction « à froid » complété individuelle par chaque stagiaire quelques semaines après la session de formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.