Sécurité du cloud et des services externalisés

CYBERSÉCURITÉ

Objectifs	Comprendre les enjeux de la sécurité dans le cloud et les environnements externalisés - Maîtriser le modèle de responsabilité partagée selon les fournisseurs (AWS, Azure, GCP). -Appliquer les bonnes pratiques de sécurité (chiffrement, IAM, audit, durcissement) - Savoir sécuriser une architecture cloud avec des ateliers techniques concrets.
Participants	Professionnels IT - ingénieurs DevOps - administrateurs systèmes - architectes cloud - consultants cybersécurité - étudiants avancés en sécurité informatique.
Prérequis	Connaissance des environnements cloud (IaaS, PaaS, SaaS) - gestion des contrats fournisseurs - architecture sécurisée - chiffrement et contrôle d'accès - conformité réglementaire - gestion des SLA.
Moyens pédagogiques	1 poste par participant - 1 vidéoprojecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et évaluation des acquis tout au long de la formation
Méthodes pédagogiques	Exposés interactifs et démonstrations - Travaux pratiques individuels et en groupe - Échanges d'expériences et de bonnes pratiques
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	4150 € HT
Durée	5 jour(s) - 35 heure(s)

Code : NCI_GMDXX8ZZ

Programme :

Fondamentaux et architecture

Introduction au cloud computing (IaaS, PaaS, SaaS)

Panorama des services cloud (AWS, Azure, GCP)

Modèle de responsabilité partagée (comparaison AWS / Azure / GCP)

Risques liés au cloud (perte de contrôle, shadow IT, erreurs de configuration)

Normes et référentiels (ISO 27017, CIS Benchmarks, ANSSI, NIST SP800-53)

Cas pratique

Mise en place d'un environnement AWS (EC2, S3, IAM)

Premiers tests de configuration non sécurisée (bucket S3 public, EC2 mal configurée)

Gestion des identités et accès (IAM)

IAM : rôles, politiques, groupes, utilisateurs

MFA, principes de moindre privilège

Séparation des comptes, stratégies d'accès conditionnel

Cas pratique

Création de politiques personnalisées AWS IAM

Tests de montée de privilèges (Privilege Escalation IAM)

Utilisation d'AWS Access Analyzer & IAM Policy Simulator

Chiffrement, journalisation, surveillance

Chiffrement au repos/en transit (KMS, TLS, client-side vs server-side)

Logging : CloudTrail, CloudWatch, GuardDuty

Gestion des clés et rotation

Détection d'incidents dans le cloud

Cas pratique

Chiffrement d'un bucket S3 + KMS custom key

Mise en place de CloudTrail pour audit

Déclenchement d'alertes via CloudWatch + scénario d'incident (exfiltration S3)

Durcissement, sécurité réseau & DevSecOps

Sécurité réseau : VPC, NACL, Security Groups, bastions

Bonnes pratiques de déploiement sécurisé

Introduction au DevSecOps : intégration sécurité dans CI/CD

Gestion des vulnérabilités (images Docker, Lambda, AMI)

Cas pratique

Configuration d'un VPC avec sous-réseaux publics/privés + bastion

Intégration d'un scanner (Trivy ou Snyk) dans une pipeline CI/CD

Analyse de logs de conteneur sur ECS/EKS

Atelier final : Red Team / Blue Team Cloud

Atelier technique

Scénario Blue Team : Réception d'un environnement compromis (bucket exposé, rôle IAM vulnérable)

Analyse des logs, mise en place de contre-mesures

Remédiation des erreurs de configuration

Scénario Red Team : Exploitation de failles dans une infrastructure cible cloud

Reconnaissance, exploitation IAM, exfiltration

Évasion de journalisation CloudTrail (techniques d'obfuscation)

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon

Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille

www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20