Réseau des Centres d'Excellence de l'UIT pour l'Afrique

Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC)

Atelier de formation en présentiel sur la

Sécurité du Cloud

Abidjan, Côte d'Ivoire
Du 03 au 07 mai 2021

PRESENTATION DE LA FORMATION

DESCRIPTION DU COURS

Titre	**Sécurité du Cloud**
Objectifs	La transformation digitale des systèmes d'information et des usages est un enjeu de développement crucial pour les organisations et les entreprises. Le Cloud est un des outils technologiques indispensables pour atteindre cet objectif à l'échelle mondial et encore plus en Afrique. Comme l'ont reconnu 17 pays Africains à l'ONU au début 2019 - dont la Côte d'Ivoire, le Cloud est un enjeu technologique majeur pour atteindre les «Sustainable Development Goals ». Encore faut-il maîtriser cette nouvelle technologie. La sécurité vient en premier dans les préoccupations liées à l'adoption, la pratique et l'usage du Cloud. L'objectif de cet atelier est d'aborder différentes problématiques et solutions de la sécurisation du Cloud : • Les normes et standards de sécurité dans le Cloud (ISO 27005 pour les risques en général, ISO 27017 et 27018 pour les données, ISO 17788/17889 pour l'architecture), • La réglementation et les aspects juridiques qui régissent en particulier la sécurité des données, • L'analyse des principales menaces, vulnérabilités et risques dans le Cloud, • L'offre de services de sécurité de fournisseurs Cloud, • L'approche « Security by design » pour appréhender la sécurité du Cloud par l'architecture des infrastructures et le choix des services **Prérequis :** Une connaissance des bases de la sécurité est souhaitable pour tirer un meilleur profit de cette formation.
Dates	03 au 07 mai 2021
Durée	5 jours
Date limite d'enregistrement	23 avril 2021
Frais de formation	930 USD / 500 000 F CFA (XOF et XAF)
Code du cours	21WS26470AFR-F

RESULTATS ATTENDUS

Aux termes de l'atelier, les auditeurs seront capables de :

- Comprendre comment s'appuyer sur des référentiels de normes et de standards pour sécuriser le Cloud,
- Savoir utiliser les services de fournisseurs Cloud pour sécuriser une infrastructure virtualisée,
- Acquérir les bonnes pratiques pour la sécurité du Cloud,
- Sécuriser ses données et assurer sa conformité règlementaire dans le Cloud.
- Être sensibilisé à la problématique de la sécurité du Cloud dans le contexte africain

PUBLIC CIBLE

Cet atelier de formation s'adresse principalement aux profils suivants :

- Directeur des Services Informatiques (DSI) ;
- Responsable de Sécurité des Systèmes d'Information (RSSI) ;
- Consultant, experts et auditeurs en sécurité ;
- Enseignants, chercheurs et étudiants en sécurité.

FORMATEUR

NOM DU FORMATEUR	CONTACTS
TETCHUENG Jean-Louis est un Docteur en Informatique de Télécom Bretagne en France. Il est également Architecte Logiciel et Expert Cloud certifié VMware VCP510 Professional on vSphere 5 et Amazon Developer Associate	jfoping@yahoo.com (+33) 6 33 81 66 26

EVALUATION

Evaluation théorique à travers un questionnaire à choix multiple

AGENDA

Date du 1er jour	Heure de début, Heure de fin	Sujets/Activités
03/05/2021	09 :00 - 09 :30	Accueil, enregistrement et ouverture du séminaire
		Thème du jour : Introduction à la sécurité du Cloud
	Session du matin (09 :30 - 12 :45)	**Concepts fondamentaux du Cloud** ▪ Définition et concepts de base du Cloud ▪ Comprendre pourquoi la sécurité est le principal frein à l'adoption du Cloud en Afrique et ailleurs. ▪ Architecture du Cloud Computing (NIST, ISO 17788/17889) ▪ Principales technologies employées dans les centres de données o Virtualisation o Stockage et distribution de contenu
	Session de l'après-midi (14 :00 - 17 :15)	**Problématiques de la sécurité du Cloud** ▪ Sécurité « On-Premise » Vs dans le Cloud ▪ Évaluer les principales menaces, vulnérabilités et risques dans le Cloud ▪ Les risques identifiés par l'ENISA,

		○ Evaluation et gestion des risques du Cloud par la norme ISO 27005 ○ Les 35 risques identifiés par l'ENISA ○ Les recommandations ENISA pour la sécurité des Cloud gouvernementaux
Date du 2ième jour	**Heure de début, Heure de fin**	**Sujets/Activités**
04/05/2021		**Thème du jour** : Standards de sécurité du Cloud
	Session du matin (09 :00 – 12 :15)	**Principes et règlements** ▪ Le principe de responsabilité partagée dans les modèles de service du Cloud ▪ Les référentiels de la Cloud Security Alliance (CSA) ▪ La sécurité dans les contrats Cloud ▪ Les réglementations et aspects juridiques ○ Les lois et dispositions européennes (RGPD). ○ Les lois et dispositions américaines (Privacy Shield, Patriot Act., FISA, Cloud Act ▪ Quelles lois et dispositions en Afrique ?
	Session de l'après-midi (13 :45 - 17 :00)	**Normes et techniques de sécurité des données** ▪ Les normes ISO 27017 et 27018 pour sécuriser les données dans le cloud ▪ La cryptographie dans le Cloud ○ Les fondamentaux (cryptographie, cryptanalyse, etc.). ○ Les approches de gestion des clés de chiffrement dans le Cloud. ○ Les approches BYOK (Bring Your Own Key) et KSaaS (Key Storage as a Service). ○ Les solutions hardware des clés (cartes et appliances HSM). ▪ Autres techniques de protection des données
Date du 3ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
05/05/2021		**Thème du jour** : Cas Pratique appliqué au Cloud Azure
	Session du matin (09 :00 – 12 :15)	**Gestion des identités et droits utilisateurs** ▪ Gestions des identités ○ Utilisation d'Azure Active Directory. ○ Ajout d'un utilisateur manuellement ○ Mise en place des groupes dans Azure AD ○ Mise en place authentification forte ○ Jonction d'un poste Windows 10 à Azure AD ▪ Droits utilisateurs sur les applications/services ○ Azure AD et les applications ○ Ajout d'une application dans le portail
	Session de l'après-midi (13 :45 - 17 :00)	**Règles et sécurisation** ▪ Configuration des modèles personnalisés ▪ Protection des documents avec Azure Information Protection

Date du 4ième jour	Heure de début, Heure de fin	Sujets / Activités
06/05/2021		**Thème du jour** : Cas pratique 2 - Approche "Security by design" dans le Cloud Amazon
	Session du matin (09 :00 – 12 :15)	**Principe du "Security by design"** ▪ Stratégies de sécurisation du Cloud Amazon ▪ Le principe du "Security by design" ▪ La gouvernance des comptes sur AWS
	Session de l'après-midi (13 :45 - 17 :00)	**Archivage Electronique Sécurisé** ▪ Création d'une identité ▪ Utilisation de la traçabilité ▪ Protection des données
Date du 5ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
07/05/2021		**Thème du jour** : Le bilan
	Session du matin (09 :00 – 12 :15)	▪ Les 7 Risques de sécurité du cloud computing ▪ Meilleures pratiques pour la sécurité du Cloud ▪ Les 10 principales recommandations de la liste de contrôle de sécurité pour les clients du Cloud ▪ Certifications de sécurité ISO 27001 ou SSAE16 type II (SAS 70) de fournisseurs Cloud ▪ Et le courtier en sécurité pour l'accès au Cloud (CASB) ? ▪ Quelles implications pour l'Afrique **Evaluation des auditeurs**
	Session de l'après-midi (12 :15 - 13 :30)	**Evaluation du séminaire et clôture de l'atelier.**

METHODOLOGIE

Exposés, travaux pratiques, étude de cas et échanges interactifs.

COORDINATION DE LA FORMATION

Coordinateur de la formation : Nom : KOSSONOU Rodolphe Chef du Service de la Formation Continue, ESATIC Tel. : + 225 21 218 100 Fax : + 225 51 400145 Email : rodolphe.kossonou@esatic.edu.ci	**Coordinateur de l'UIT :** Nom : M. Emmanuel Niyikora Responsable de Programme, bureau de zone UIT pour l'Afrique de l'Ouest, Dakar Tel : +250 788312939 Email: emmanuel.niyikora@itu.int

INSCRIPTION ET PAIEMENT

Inscription sur le portail de l'ITU Académie :
L'inscription et le paiement doivent se faire en ligne sur le portail web de l'ITU Académie. Afin de pouvoir vous inscrire à un cours vous **devez** au préalable créer un compte sur le portail web d'ITU Académie à l'adresse suivante : https://academy.itu.int/index.php/user/register

Inscription à une formation :
Si vous avez déjà un compte ou que vous créez un nouveau compte, vous pouvez vous inscrire en ligne pour la formation à l'adresse suivante :
https://academy.itu.int/index.php/training-courses/full-catalogue/securite-du-cloud

Vous pouvez également vous inscrire en trouvant le cours qui vous intéresse dans notre catalogue de formation https://academy.itu.int/index.php/training-courses/full-catalogue

Paiement

1. **Paiement en ligne**

Les frais de participation à cette formation sont de **USD 930**. Ce montant prend en compte l'inscription, la documentation, la pause-café et le déjeuner. Il est recommandé de procéder au paiement via le système de paiement en ligne en utilisant le même lien que celui de l'inscription en ligne :
https://academy.itu.int/index.php/training-courses/full-catalogue/securite-du-cloud

2. **Paiement par virement bancaire**

Lorsqu'il n'est pas possible d'effectuer un paiement via le système en ligne, sélectionnez l'option de paiement hors ligne ''offline'' pour générer une facture en utilisant le même lien que ci-dessus. Téléchargez la facture pour effectuer un virement sur le compte bancaire de l'UIT indiqué ci-dessous. Envoyez ensuite la preuve de paiement / la copie du bordereau de virement et la copie de la facture à Hcbmail@itu.intet mettre en copie le coordinateur du cours. **Tous les frais de transaction bancaire doivent être à la charge du payeur.**
Si les documents ci-dessus ne sont pas soumis, le candidat pourrait ne pas être inscrit à la formation.

3. **Paiement par groupe**

Si vous souhaitez payer pour plus d'un participant par virement bancaire et que vous avez besoin d'une facture pour tous, créez un compte comme **contact institutionnel.** Les contacts institutionnels sont des utilisateurs qui représentent une organisation. Tout étudiant peut demander à être un contact institutionnel ou à appartenir à une organisation existante.

Pour ce faire, accédez à la page de votre profil en cliquant sur le bouton **"My account"** dans le menu de l'utilisateur. Au bas de cette page, vous devriez voir deux boutons :

a. Si vous souhaitez **devenir un contact institutionnel**, cliquez sur le bouton "**Apply to be an Institutional Contact"**. Cela vous redirigera vers un petit formulaire qui vous demandera le nom de l'organisation. Une fois que vous avez renseigné le nom de l'organisation que vous souhaitez représenter, cliquez sur **"continue",** une demande est alors créée. Un responsable de l'Académie de l'UIT examinera manuellement cette demande et l'acceptera ou la refusera en conséquence.

b. Si vous souhaitez **appartenir à une organisation existante**, cliquez sur le bouton **"Request to belong to an Institutional Contact"**. Cela vous redirigera vers un petit formulaire qui vous demandera de sélectionner l'organisation à laquelle vous souhaitez appartenir à partir d'une liste d'organisations. Après avoir sélectionné la bonne organisation et cliqué sur **"continue"**, une demande sera créée. Le contact institutionnel qui représente cette organisation acceptera ou refusera manuellement votre demande d'adhésion à l'organisation.

Coordonnées bancaires de l'UIT :	
Nom et addresse de la Banque :	UBS SWITZERLAND AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiaire:	Union Internationale des Télécommunications
Numero de Compte :	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Montant :	930 USD
Reference du paiement :	CoE-AFR 26470 - P.40590.1.04

4. Autres méthodes de paiement

Si pour des raisons de régulations nationales il y a des restrictions ne permettant pas d'utiliser les options de paiement 1 et 2 ci-dessus, veuillez contacter le coordinateur de l'UIT pour plus d'assistance.