

**REPUBLIQUE DU CAMEROUN**

**Paix - Travail - Patrie**

-----  
**MINISTERE DES POSTES ET  
TELECOMMUNICATIONS**  
-----



**REPUBLIC OF CAMEROON**

**Peace - Work - Fatherland**

-----  
**MINISTRY OF POSTS AND  
TELECOMMUNICATION**  
-----

## **RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL POUR LA REALISATION DE LA MISSION DE VEILLE SECURITAIRE.**

**MARCHE N°00000040/M//MPT/SG/DAG/2021 DU 15 OCTOBRE 2021 PASSE APRES APPEL  
D'OFFRES NATIONAL RESTREINT N°00000025/AONR/MPT/CIPM/2021 DU 17 AOÛT 2021 POUR LE  
RECRUTEMENT D'UN CABINET OU BUREAU D'ETUDES EN VUE DU RENFORCEMENT DES  
CAPACITES DU PERSONNEL DU MINPOSTEL POUR LA REALISATION DE LA MISSION DE  
VEILLE SECURITAIRE.**

## **RAPPORT DE LA FORMATION SUR CSCU**

**Aout 2022**



## **RAPPORT DE LA FORMATION SUR CSCU**



LE PRESENT DOCUMENT EST LE RAPPORT DE LA FORMATION SUR LE MODULE CSCU DANS LE CADRE DU MARCHE N°00000040/M//MPT/SG/DAG/2021 DU 15 OCTOBRE 2021 PASSE APRES APPEL D'OFFRES NATIONAL RESTREINT N°00000025/AONR/MPT/CIPM/2021 DU 17 AOUT 2021 POUR LE RECRUTEMENT D'UN CABINET OU BUREAU D'ETUDES EN VUE DU RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL POUR LA REALISATION DE LA MISSION DE VEILLE SECURITAIRE.

Tous droits réservés. Aucune partie de ce document ne peut être reproduite, mise en mémoire dans un système de recherche bibliographique ni transmis sous quelque forme ou par quelques procédés que ce soit électronique, mécanique, par photocopie ou autres sans autorisation préalable. Adresser une demande motivée, en indiquant les passages ou illustrations en cause au MINPOSTEL maître d'ouvrage de cette étude susmentionnée.

## SOMMAIRE

<b>1. AVANT-PROPOS .....</b>	<b>6</b>
<b>2. Introduction et contexte .....</b>	<b>7</b>
2.1. Contexte .....	7
2.2. Objet du projet .....	7
2.3. Consistance des prestations .....	8
<b>3. Objectifs de la formation .....</b>	<b>9</b>
3.1. Objectif général .....	9
3.2. Objectifs spécifiques.....	9
<b>4. Méthodologie choisie.....</b>	<b>10</b>
<b>5. Déroulement de la formation .....</b>	<b>11</b>
<b>6. Domaines abordés.....</b>	<b>12</b>
<b>7. Conclusion.....</b>	<b>13</b>
<b>ANNEXES.....</b>	<b>14</b>
A1/ ATTESTATIONS DE PARTICIPATION.....	15
A2/ LISTES DE PRESENCE .....	17
A3/ PHOTOS DE FAMILLE .....	21

## 1. AVANT-PROPOS

Le présent document est confidentiel et sa confidentialité consiste à :

- La non divulgation des informations de configurations et paramétrages auprès de tierce partie ;
- La non reproduction des informations considérées confidentielles, sauf accord du Ministère des Postes et Télécommunications ;
- Les savoir-faire y contenus ne doivent profiter qu'au Ministère des Postes et Télécommunications ;
- Considérer toutes les informations déclarées Confidentielles.

## 2. Introduction et contexte

### 2.1. Contexte

Le CIRT est une structure de l'ANTIC constituée de seize (16) personnels chargés au quotidien de la prévention et de la réponse aux actes cybercriminels au Cameroun. Afin de remplir convenablement ses missions, le CIRT a besoin de personnels compétents dans différents domaines de la cybersécurité. A cet effet, le renforcement des capacités est une activité continue au sein du CIRT et permet de maintenir les personnels à la hauteur des enjeux auxquels ils font face au quotidien.

A travers ce projet, il est question d'améliorer les capacités des personnels au cours dans les domaines suivants :

- Ethical Hacking ;
- Les investigations numériques ;
- L'analyse des programmes malveillants ;
- La sécurité des infrastructures critiques ;
- La protection des postes clients ;
- La collecte des informations à travers les outils OSINT et le Dark web ;
- La protection des infrastructures critiques.

### 2.2. Objet du projet

L'objectif global de ce projet est de renforcer les capacités des personnels du CIRT afin de leur permettre de mieux réaliser les missions de veille de sécuritaire au sein de l'ANTIC.

Les objectifs spécifiques de ce projet sont les suivants :

- Permettre aux personnels du CIRT de mieux comprendre les techniques utilisées par les hackers, les risques de sécurité des systèmes d'information et les différentes mesures de sécurité existantes.
- Renforcer les capacités des personnels du CIRT en matière de collecte et d'analyse des preuves numériques sur les appareils mobiles, les supports de stockage, les mémoires vives, etc.;
- Permettre au CIRT de gérer les risques de sécurité afférents aux infrastructures critiques et aux systèmes de contrôle industriels ;
- Permettre aux personnels du CIRT de comprendre le fonctionnement du Dark web et d'être capable d'utiliser les outils OSINT pour la collecte d'informations spécifiques sur Internet ;

- Permettre aux personnels du CIRT d'analyser et comprendre le fonctionnement des programmes malveillants ;
- Permettre aux personnels du CIRT de maîtriser la sécurisation des postes clients et des différents services qui s'y exécutent.

### 2.3. Consistance des prestations

Les prestations portent sur l'organisation de formation certifiante. Il s'agira donc concrètement de former les participants aux contenus en rapport avec le piratage éthique, l'investigation numérique, le test d'intrusion, la sécurisation des postes de travail, etc.

Chaque phase de cette formation (quatre au total) sera sanctionnée par un examen de certification pour évaluer l'assimilation et la mise en pratique des concepts appris.

Il s'agit des formations suivantes :

- Certified Ethical Hacker (CEH);
- Computer Hacking Forensic Investigator (CHFI);
- Certified Penetration Testing Professional (CPENT);
- Certified Secure Computer User (CSCU).

Le présent document constitue le rapport d'exécution de la formation sur CSCU.



### 3. Objectifs de la formation

#### 3.1. Objectif général

L'objectif de cette formation est d'acquérir des compétences sur les outils et techniques pour éviter les cybercriminels/ attaques cybernétiques.

#### 3.2. Objectifs spécifiques

Les participants à la formation sont désormais capables de :

- Saisir le niveau d'importance de la sécurité des données ;
- Appliquer des règles de sécurité sur vos ordinateurs personnel ou professionnel ;
- Connaître et comprendre le fonctionnement des logiciels malveillants ;
- Savoir choisir une solution antivirus adaptée à son utilisation ;
- Se rendre compte des risques liés aux diverses activités sur Internet ;
- Découvrir l'importance de bien sécuriser son navigateur web et appliquer des paramètres de sécurité ;
- Savoir reconnaître des sites web fiables et sécurisés ;
- Savoir se protéger des menaces sur les sites de réseaux sociaux ;
- Apprendre à sécuriser vos comptes sur les réseaux sociaux ;
- Se rendre compte des risques liés aux communications par e-mail et appliquer des paramètres de sécurité ;
- Se rendre compte des risques liés à l'usage du smartphone ou d'une tablette et comment s'en protéger ;
- Se rendre compte des risques liés aux services de stockage en ligne et quelles sont les moyens utilisés pour s'en protéger ;
- Savoir choisir un service cloud de qualité adapté à son utilisation ;
- Découvrir les différents types de réseaux informatiques et les menaces liées.

## 4. Méthodologie choisie

Notre méthodologie a consisté en un cours intensif de trois jours permettant aux participants d'acquérir une compréhension fondamentale de diverses menaces de Sécurité informatique et réseau telles que le vol d'identité, la fraude par carte de crédit, les escroqueries par hameçonnage bancaire en ligne, les virus et les portes dérobées, les canulars par e-mail, les délinquants sexuels qui se cachent en ligne, la perte d'informations confidentielles, d'attaques de piratage et d'ingénierie sociale.

Durant cette formation, les participants ont appris les mesures nécessaires pour atténuer leur exposition à la sécurité.

L'agenda observé était le suivant :

Horaire	Activités	Animateurs	Horaire
08h00-10h00	Cours	Formateur	08h00-10h00
10h00-10h30	Pause-café	Formateur + Participants	10h00-10h30
10h30-12h30	Cours	Formateur	10h30-12h30
12h30-13h30	Pause déjeuner	Formateur + Participants	12h30-13h30
13h30-17h00	Cours	Formateur	13h30-17h00

## 5. Déroulement de la formation

La formation s'est déroulée sur une durée de 3 jours ouvrables et a débuté le lundi 01 aout 2022 par l'installation des participants et le lancement officiel par les formateurs accompagnés de l'équipe projet de KIAMA SA.

Il a été rappelé les enjeux et les objectifs de la formation puis le matériel de formation a été distribué.

Le programme détaillé de la formation était le suivant :

Date	Modules dispensés
Jour 1 : 01 aout 2022	<ul style="list-style-type: none"> <li>• Introduction à la sécurité</li> <li>• Sécurisation des systèmes d'exploitation</li> <li>• Malware et antivirus</li> </ul>
Jour 2 : 02 aout 2022	<ul style="list-style-type: none"> <li>• La sécurité sur Internet</li> <li>• Sécurité sur les sites de réseautage social</li> <li>• Présentation de la Scrum Team</li> <li>• Sécurisation des communications par e-mail</li> </ul>
Jour 3 : 03 aout 2022	<ul style="list-style-type: none"> <li>• Sécurisation des appareils mobiles</li> <li>• Sécuriser le cloud</li> <li>• Sécurisation des connexions réseau</li> <li>• 10 Sauvegarde des données et désastre</li> </ul>

## 6. Domaines abordés

Les participants ont été entretenus sur les domaines suivants :

### **Domaine 1 : Durcissement réseaux et systèmes**

Objectif principal : S'assurer que le candidat à la certification CSCU est en mesure de comprendre les principaux problèmes du monde de la sécurité de l'information, le processus de gestion des incidents et les tests de pénétration.

### **Domaine 2 : Supervision des réseaux informatique**

Objectif principal : S'assurer que le candidat à la certification CSCU est en mesure de comprendre le concept de surveillance du bon fonctionnement des réseaux informatiques et des services informatiques connectés sur ces réseaux.

### **Domaine 3 : Mise en place et configuration sécurisé des firewalls**

Objectif principal : S'assurer que le candidat à la certification CSCU est en mesure d'identifier les types de firewalls et leurs usages, Rédiger des règles firewalls et de définir une politique de sécurité simple.

### **Domaine 4 : Mise en place et configuration sécurisé des VPN**

Objectif principal : S'assurer que le candidat à la certification CSCU est en mesure de configurer un VPN.

### **Domaine 5 : Techniques de Hacking.**

Objectif principal : S'assurer que le candidat à la certification CSCU est en mesure de détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage, d'appliquer des mesures et des règles basiques pour lutter contre le hacking et d'identifier le mécanisme des principales attaques.

## 7. Conclusion

Le cabinet KIAMA SA, mandataire du groupement adjudicataire du marché de renforcement des capacités du personnel du MINPOSTEL pour la réalisation de la mission de veille sécuritaire a, dans cette étape réalisé le premier module portant sur la préparation à la certification CSCU. Il était question dans cette phase du marché, d'assurer la formation de cinq (04) personnels du MINPOSTEL et de l'ANTIC sur la protection des données personnels et une utilisation sécurisée de son poste de travail. La formation s'est déroulée comme prévu et les participants ont bénéficié des attestations de fin de formation. L'ensemble des personnels conviés ont bénéficiés des packs iLeand de ECCOUNCIL contenant :







- Un an d'accès aux cours en ligne ;
- Six mois d'accès à l'environnement officiel de laboratoire en ligne d'EC-Council (i-Labs) ;
- Un voucher pour l'examen de certification d'EC-Council ;
- Un accès d'un an aux modules de formation d'experts d'EC-Council avec des présentations vidéo en continu pour un programme de formation complet qui offre les avantages d'une formation en classe à votre propre rythme ;
- Un accès au portail d'examen (<https://www.eccexam.com>) grâce à auquel chaque apprenant peut passer l'examen en ligne depuis le confort de sa maison ou de son bureau.





Le suivi d'après formation est effectif et se déroule dans le groupe whatsapp créé à cet effet.

Dans ce groupe, les apprenants remontent les difficultés éventuelles auxquelles ils font face et sont coachés en prélude à leur examen.

# ANNEXES

## A1/ ATTESTATIONS DE PARTICIPATION

   	
<b><u>ATTESTATION DE FORMATION</u></b>	
<p>Nous certifions par la présente que</p> <p>M./Mme : <b>TABE BAIJE BISMAL</b></p> <p>A suivi de façon effective le renforcement des capacités pour la réalisation de la mission de veille sécuritaire. Il a été dans ce cadre préparé au passage de la certification <b>Certified Secure Computer User (CSCU)</b>.</p> <p>Dates de la formation : du 01 Aout 2022 au 03 Aout 2022. Durée totale de la formation : 24 heures Lieu de formation : Ecole Nationale Supérieure Polytechnique - Yaoundé</p>	
<b><u>Le responsable des formations</u></b>	<b><u>Le formateur</u></b>
	

   	
<b><u>ATTESTATION DE FORMATION</u></b>	
<p>Nous certifions par la présente que</p> <p>M./Mme : <b>TCHALA MBOUDOU LANDRY</b></p> <p>A suivi de façon effective le renforcement des capacités pour la réalisation de la mission de veille sécuritaire. Il a été dans ce cadre préparé au passage de la certification <b>Certified Secure Computer User (CSCU)</b>.</p> <p>Dates de la formation : du 01 Aout 2022 au 03 Aout 2022. Durée totale de la formation : 24 heures Lieu de formation : Ecole Nationale Supérieure Polytechnique - Yaoundé</p>	
<b><u>Le responsable des formations</u></b>	<b><u>Le formateur</u></b>
	



### ATTESTATION DE FORMATION

Nous certifions par la présente que

M./Mme : **WANDEU NOUPIE FIDELE**

A suivi de façon effective le renforcement des capacités pour la réalisation de la mission de veille sécuritaire. Il a été dans ce cadre préparé au passage de la certification **Certified Secure Computer User (CSCU)**.

Dates de la formation : du 01 Aout 2022 au 03 Aout 2022.

Durée totale de la formation : 24 heures

Lieu de formation : Ecole Nationale Supérieure Polytechnique - Yaoundé

Le responsable des formations

Le formateur



*[Signature]*



### ATTESTATION DE FORMATION

Nous certifions par la présente que

M./Mme : **DJDUSSEU NGUENANG ALAIN PASCAL**

A suivi de façon effective le renforcement des capacités pour la réalisation de la mission de veille sécuritaire. Il a été dans ce cadre préparé au passage de la certification **Certified Secure Computer User (CSCU)**.

Dates de la formation : du 01 Aout 2022 au 03 Aout 2022.

Durée totale de la formation : 24 heures

Lieu de formation : Ecole Nationale Supérieure Polytechnique - Yaoundé

Le responsable des formations

Le formateur



*[Signature]*



## A2/ LISTES DE PRESENCE



**KIAMA S.A.**, au capital de 40 000 000 de FCFA,  
Basos, en Face de l'ANOR, Rue Ambassade De Chine,  
Contact@kiama.cm www.kiama.cm  
Tel : (237) 697 812 515 / 682 202 675  
Fixe : (237) 222 209 043  
BP : 15709 Yaoundé Cameroun

Au cœur de l'innovation

Yaoundé le, 01 Août 2022.

### FICHE DE PRESENCE A LA FORMATION CSCU

N°	NOM ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE
01	NOUGI Etienne Achille	Consultant	652 58 35 22	e.nougi@gmail.com	
02	DJOUSSOU EUGENIUS Alain Pascal	Ministère de l'Industrie et du Commerce Cellule Impression	67916169	delaunypascal@minpostel.gm.cm	
03	WANDEU NOUPIE Fidele	Centre ANITIC	693821594	fidele.wandeu@antec.cm	
04	TCHALA MBODOU Lumbuy	Cadre ANTEC	680735161	Laudyngtchala@gmail.com	
05	TABE BAYE BISMAL	Cadre ANITIC	670741839	baye.bismal@gmail.com	
06					
07					



**KIAMA S.A.** au capital de 40 000 000 de FCFA.  
Bastos, en Face de l'ANOR, Rue Ambassade De Chine.  
contact@kiama.cm www.kiama.cm  
Tel : (237) 697 812 515 / 682 202 675  
Fixe : (237) 222 209 043  
BP : 15709 Yaoundé Cameroun

Au cœur de l'innovation

Yaoundé le, 02 Août 2022

FICHE DE PRESENCE A LA FORMATION CSCU

N°	NOMS ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE
01	NOUGI Evariste Achille	Consultant	652 58 35 82	e.nougi@gmail.com	
02	Wandou noupie fidelé	Cadre / ANTIC	693 82 11 54 674 34 07 11	fidelé.wandou@cert.cm	
03	TABE BAYE BISMAL	Cadre / ANTIC	670 74 18 39	baye.bismal@gmail.com	
04	TEHALA MBOUNDO LANDRY	Cadre / ANTIC	680 79 33 16	landry.tehala@gmail.com	
05	DJOUSSOU NGUEWANG Alain Pascal	Cadre / Dinsatel	679 91 61 69	djoussounguew@minpostel.gov.cm	
06					
07					



**KIAMA S.A.** au capital de 40 000 000 de FCFA.  
Bastos, en face de l'ANOR, Rue Ambassade De Chine,  
Contact@kiama.cm www.kiama.cm  
Tel : (237) 697 812 515 / 682 202 675  
Fixe : (237) 222 209 043  
BP : 15709 Yaoundé Cameroun

Au cœur de l'innovation

Yaoundé le, 03 Août 2022.

FICHE DE PRESENCE A LA FORMATION CSCU						
N°	NOMS ET PRENOMS	FONCTION/Structure	CONTACT	MAIL	SIGNATURE	
01	NOUGI Jeanne Achille	Consultant	652 58 35 22	e.noug@kiama.cm		
02	TOUSSOU NGUESSANG Alain Tarsa	Min Postel Cellule / Cadre	679 16 169	alain.nguessang@minpostel.gov.cm		
03	TC HALA MBOUDOU LANDRY	Cadre / AN TIC	680 79 3 161	landry.tchinda@gmail.com		
04	TABE BAYE BISMAL	Cadre / AN TIC	670 74 1839	baye.bismal@gmail.com		
05	WANDEU NOUPIE Fidele	Cadre / AN TIC	693 82 1154 674 34 07 11	fidele.wandou@minpostel.gov.cm		
06						
07						

### A3/ PHOTOS DE FAMILLE

