FORMATION "CLASSE ALIMA"

TITRE : SENSIBILISATION ET FORMATION SUR LA CYBERSÉCURITÉ : L'USAGE OSINT POUR UNE CYBER INTELLIGENCE

SYLLABUS FCL-A

1. Introduction

1.1 Objectifs

L'objectif principal des Universités de la Cybersécurité est de sensibiliser à la problématique de la cybercriminalité et d'initier aux principaux enjeux de la cybersécurité ainsi qu'à l'utilisation des technologies de pointe innovantes.

Comprendre l'OSINT (Open Source Intelligence) : l'apprentissage sur l'utilisation de l'internet et à exploiter du renseignement en provenance de sources ouvertes afin de mener à bien des recherches et investigations en ligne.

La formation Classe Alima permettra de :

- Comprendre les enjeux et le cadre réglementaire de l'OSINT ;
- Maîtriser les outils et méthodologies pour mener une enquête en sources ouvertes ;
- Savoir définir des besoins en recherche et analyser des sources numériques variées ;
- Réaliser des investigations OSINT et produire des rapports professionnels ;
- Préparer la création et le lancement d'un fichier digital en utilisant l'OSINT ;
- Développer son réseau et sa visibilité en tant qu'expert OSINT ;
- Être capable d'aider les décideurs à comprendre les menaces sécuritaires avenir sur la base des outils OSINT pour la sécurité nationale.

1.2 Prérequis pour les apprenants

Cette formation est ouverte à tous. Néanmoins l'expérience professionnelle fera la différence.

De plus, les connaissances de base suivantes faciliteront la compréhension des étudiants, mais ne sont pas impératives :

– Connaissances de base sur les systèmes d'information (biens, fonctionnement, le modèle OSI, le protocole TCP/IP, etc.) ;

– Connaissances de base sur le fonctionnement technique des réseaux, des systèmes d'exploitation et des applications.

1.3 Cibles privilégiées

– Les agents des institutions techniques/stratégiques de la République (la Justice, les grandes entreprises et les journalistes) ;
– Les agents des forces de sécurité et de défense (la gendarmerie, la police, les services de renseignements, l'armée, ...).

2. Animateurs

1. **Stanislas NYOKAS** (Animateur principal)
   - Expert et Leader en Cybersécurité
   - Enquêteur Expert en Cybercriminalité
   - Docteur en Mathématiques pures
   - PDG iTM Systems, Londres (Angleterre) [www.itmsystems.net]
2. **Marius Gabin ETA** (Assistant)
   - Expert en Transmission des Données et Sécurité de l'Information
   - Consultant en Cybersécurité
   - Enseignant-Chercheur en TIC et en Maths Appliquées à l'Université Marien Ngouabi
   - Président du CyberSecurity Club Congo, Brazzaville (Congo)
3. **Colonel Alain EKONDZI** (Assistant)
   - Docteur en Informatique
   - Enseignant-Chercheur, Université Marien Ngouabi, Brazzaville (Congo)
   - Directeur du Centre de Formation de l'Informatique (CFI) du Centre d'Informatique et de Recherche de l'Armée et de la Sécurité (CIRAS).

3. Programme de la formation

Cette formation de base de deux niveaux (niveau 1, et niveau 2 sur les trois que nous proposons habituellement) est constituée de 5 modules étalés sur 10 jours.

L'usage OSINT pour une Cyber Intelligence des Forces de sécurité	
Objectifs	*Initiation à l'OSINT (Open Source Intelligence), ou ROSO en français (Renseignement d'origine sources ouvertes), méthode d'analyse, de collecte d'informations à partir de sources ouvertes telles que les réseaux sociaux, les sites Web, les blogs, les forums de discussion, les moteurs de recherche en tous genres, les plateformes de partage de vidéos ou de photos en mode public, la presse en général, les publications spécialisées et les bases de données publiques. Tout au long de cette formation, vous découvrirez l'OSINT sous plusieurs angles, des outils, des techniques, la mise en place d'un laboratoire virtuel et comment vous protéger.* *Il s'agit d'un cours complet qui utilise des outils open source gratuits pour enquêter sur les personnes et les entreprises par les forces de sécurité et de défense. Ces dernières seront sensibilisées et averties sur les techniques des hackers. Une explication sera donnée sur la manière dont les hackers et les enquêteurs utilisent ces outils et pourquoi. L'OSINT peut être utilisé dans le cadre de la Cyber Intelligence et de la Collaboration pour collecter des informations sur les menaces potentielles, les vulnérabilités, les*

	attaques, les acteurs malveillants, etc. Les informations collectées peuvent être partagées avec d'autres membres de l'équipe pour aider à identifier les menaces potentielles, à affiner les tests d'intrusion et à élaborer des stratégies de défense. *En somme, l'OSINT est une technique de renseignement au service de l'intelligence cyber, destinée à prendre une place de plus en plus importante dans la construction de cyberdéfenses efficaces.*
Module 1	**Introduction**
Module 2	**Recherche et conclusion**
Module 3	**Sources**
Module 4	**Technique**
Module 5	**OSINT appliqué**

4. Durée

La durée de cette formation est de 10 jours, soit deux jours par module.

7 Heures/jour

5. Coût de la formation

Négociable à la demande.