



FICHE TECHNIQUE

FORUM BRAZZA CYBERSECURITY

ÉDITION 2024



DU 26 AU 27 NOVEMBRE 2024



**CENTRE INTERNATIONAL DE CONFERENCE
DE KINTELE**



Table des matières

I.	Présentation générale.....	3
II.	Résultats Escompté.....	4
III.	Durée, organisation et format du forum.....	5

31



I. { Présentation générale }

() FORUM BRAZZA CYBERSECURITY

Créé en 2021 par l'impulsion de la société **SKYTECH-CONGO**, le Forum Brazza Cybersecurity, en sigle FBC, est l'évènement de référence en matière de Cybersécurité, Cyberdéfense, Cyber-Intelligence et criminalité numérique en **Afrique Centrale**.

Le FBC réunit un parterre de sachants de divers horizons, décideurs politiques, dirigeants des institutions publiques aux experts, professionnels et universitaires autour des panels, tables rondes, conférences et ateliers pratiques pour des retours d'expériences et de partages des bonnes pratiques.

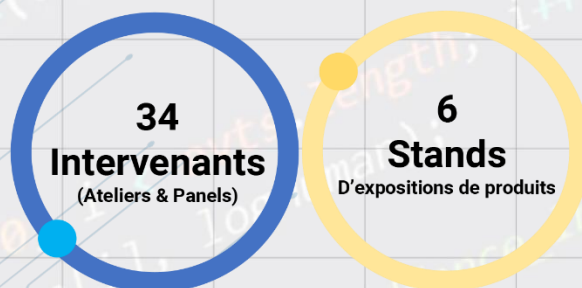
() RETOUR SUR LA PREMIERE EDITION

Elle s'est tenue du 16 au 17 septembre 2021 à Brazzaville en République du Congo, sous le thème : **La cybersécurité, un enjeu stratégique pour les États, les entreprises et institutions en Afrique.**


() LES CHIFFRES



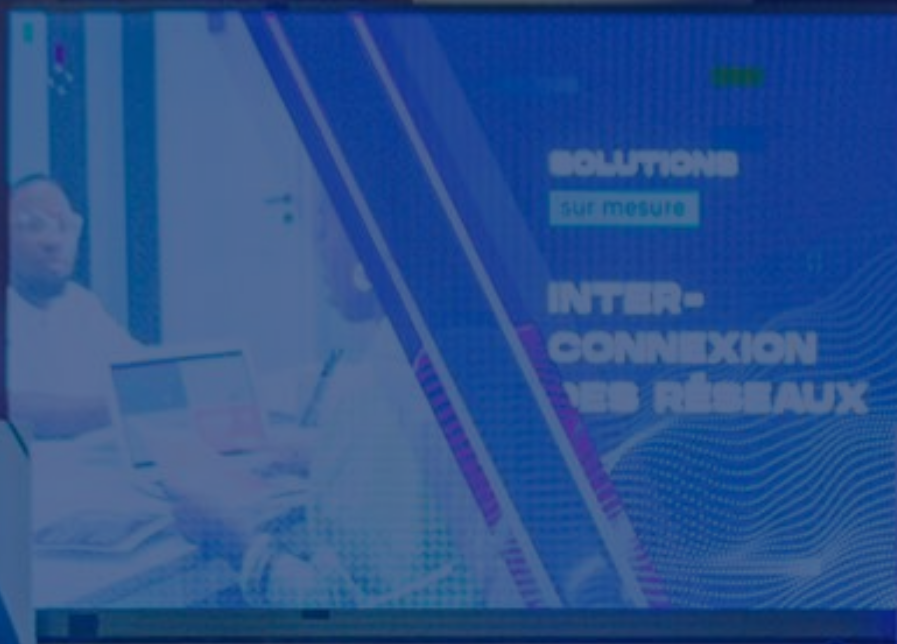
● 159 participants se sont inscrits surplace et ● 218 personnes ont répondu à l'invitation émise par le comité d'organisation dont ● 50 étudiants du CFI-CIRAS et ● 50 gendarmes.



13 pays ont pris part au **Forum Brazza Cybersecurity**, entre autres

-  République Démocratique du Congo
-  République Centrafricaine
-  République du Gabon
-  République du Mali
-  République du Tchad
-  République d'Angola
-  Egypte
-  République du Togo
-  Madagascar
-  République du Benin
-  République du Sénégal
-  France
-  Suisse





PREMIÈRE PLATEFORME PRIVILÉGIÉE D'ÉCHANGE
SUR LE RISQUE CYBER EN AFRIQUE CENTRALE

PHOTO THEQUE







() CONTEXTE ET JUSTIFICATION

Trois années après la première édition, la 2ème édition du FBC ouvre ses portes le 26 novembre 2024, en prélude de la journée mondiale de la sécurité informatique, célébrée chaque 30 novembre. Créée en 1988 par l'Association for Computing Machinery (ACM), cette journée vise à rappeler l'obligation et le besoin de protéger les données contre les menaces cyber.

A l'ère de l'IA et de l'infonuagique, la donnée n'est plus seulement une ressource stratégique, à l'instar du pétrole, mais elle est devenue le véritable nerf de la guerre. Dans l'industrie 4.0, cette ressource précieuse est convoitée par les États, les gouvernements, les entreprises et les cybercriminels.

Au cœur de cette ère, la cyber intelligence, un domaine qui exploite des technologies avancées pour analyser et transformer d'énormes volumes de données en connaissances exploitables, constitue un pilier central pour anticiper les menaces, optimiser les opérations, développer une défense proactive et renforcer la résilience des infrastructures numériques.

() OBJECTIFS

Sensibiliser et accroître les connaissances des acteurs sur les enjeux de la cyber intelligence, de l'industrie 4.0, le développement d'une défense proactive de l'infonuagique et le renforcement de la cyber-résilience des infrastructures numériques.

Spécifiquement, il s'agit de :


- Dresser un état des lieux des nouvelles menaces numériques à l'ère de l'IA ;

- Identifier les défis et les opportunités pour la mise en place d'un écosystème de cybersécurité robuste, résiliente au niveau de la sous-région ;

- Sensibiliser les acteurs clés des secteurs névralgiques tels que le secteur minier, le secteur pétrolier, le secteur bancaire etc. sur les opportunités et défis de Cyber threat intelligence ;

- Mettre en exergue les atouts de l'infonuagique et de l'industrie 4.0 dans la sous-région, y compris les innovations des startups ;

- Informers et former les agents en charge de l'ordre public et de la sécurité



II. { RESULTATS ESCOMPTE }

Le résultat attendu sera un ensemble de recommandations concrètes pour aider les États, les gouvernements, les institutions et les entreprises à développer une défense proactive de l'infonuagique et à renforcer la cyber-résilience de leurs infrastructures numériques pour garantir la cyber-souveraineté.

Ces recommandations seront consignées dans le **Livre blanc du Forum Brazza Cybersecurity**. L'objectif du FBC est d'aider ces acteurs à trouver aux problèmes concrets des solutions pragmatiques qui pourront à la fois assurer la protection des nouvelles chaînes de valeur et garantir la souveraineté numérique de leurs États.

III. { DUREE, ORGANISATION ET FORMAT DU FORUM }

Durée

2 jours

() ORGANISATION

Le FBC se déroulera en séances plénières, tables rondes, panels et en ateliers de travail autour du thème général :

« Cyber Intelligence et l'industrie de la donnée ».

Il comprendra des Keynote suivies de débats autour des sous-thèmes. L'objectif du FBC est d'aider ces acteurs à trouver aux problèmes concrets des solutions pragmatiques qui pourront à la fois assurer la protection des nouvelles chaînes de valeur et garantir la souveraineté numérique de leurs États.

() SOUS-THEMES

- Infonuagique et souveraineté : Comment concilier sécurité, évolution et souveraineté en matière d'infonuagique
- Comment les modèles d'IA peuvent-ils s'adapter aux nouvelles tactiques des cybercriminels ?
- Comment garantir une collaboration efficace entre les équipes de renseignement et de sécurité ?
- Donnée : principal pilier de l'industrie 4.0
- Cybersécurité à l'ère de l'Intelligence Artificielle : quelles conséquences sur les pays africains ?
- Infonuagique comme véritable accélérateur de l'industrie 4.0
- Comment renforcer la coopération entre les ANSSI pour faire face aux défis globaux de la cybersécurité ?
- Fraude digitale : Quelles méthodes proactives pouvons-nous utiliser pour identifier et contrer les escroqueries en ligne ?
- Cyber combat : Quelles réalités dans l'utilisation de l'IA dans les systèmes militaires ?
- Banques et institutions financières : sont-elles la cible préférée des cyberattaques ?
- Évolutions des cybermenaces : Mieux appréhender le rôle des États
- Depuis les accords de Malabo en 2014, de nombreux pays ont accéléré le renforcement des cadres juridiques et réglementaires en matière de protection des données, qu'en est-il ?
- Comment garder une souveraineté du contrôle des données dans un monde de plus en plus connecté ?
- Construire une culture de la sécurité digitale
- Sécuriser l'IoT : Défis et Solutions pour l'Afrique
- Finance et cyber : défis et innovations pour protéger les institutions bancaires
- Cyber Intelligence dans le contexte de l'intégration sous régionale.
- Perspectives sur l'évolution des menaces et solutions innovantes à l'ère de l'IA
- Intelligence économique et espionnage économique
- Du Big Data à l'évolution de la cyber intelligence
- Innover en cyber intelligence pour l'avenir



contact@skytechcongo.cg
infos@forumbrazzacybersecurity.cg



(+ 242) 05 200 58 58
(+ 242) 06 625 73 73



www.forumbrazzacybersecurity.cg

