القمة الأفريقية للأمن السيبراني

الذكاء الاصطناعي والسحابة السيادية : ركيزة لتعزيز الأمن السيبراني

Forum Africain de la Cybersécurité

L'intelligence artificielle et le cloud de confiance : un pilier pour renforcer la cybersécurité

3 - 5 février 2025

Premier jour – 3 février 2025

08 h 00 – 08 h 45 | Retrait des badges et accueil avec rafraîchissements.
08 h 45 – 08 h 50 | Hymne national.
08 h 50 – 09 h 00 | Discours d'ouverture du Maître de cérémonie : *M. Khalid Al-Amrani, Sultanat d'Oman.*

Ouverture officielle

09 h 00 – 09 h 15 | Discours d'ouverture officiels des ministres.

- *S.E. M. Abdellatif Loudiyi, Ministre délégué auprès du Chef du Gouvernement chargé de l'Administration de la Défense Nationale.*
- *S.E. MME Amal El Fallah Seghrouchni, Ministre déléguée auprès du Chef du Gouvernement chargée de la Transition numérique et de la Réforme administrative.*
- *M. Lacina Koné, Directeur Général et Directeur Général de Smart Africa.*

Vision stratégique et collaboration

09 h 15 – 09 h 30 | Keynote 1 : La transformation numérique de l'Afrique : adopter la cybersécurité et la souveraineté technologique.

Ce discours introduira le séminaire, qui se concentrera sur le rôle crucial d'une cybersécurité robuste et souveraine dans la réalisation d'une transformation numérique résiliente en Afrique. À l'aide d'exemples, il souligne comment des technologies innovantes peuvent protéger les infrastructures critiques et renforcer l'écosystème numérique du continent. Il souligne également l'importance d'initiatives telles que Smart Africa et le Réseau africain des autorités de cybersécurité (ANCA) pour harmoniser les politiques numériques entre les pays africains et favoriser le renforcement des capacités grâce à une approche collaborative et visionnaire.

- *Monsieur le Général de Brigade El Mostafa Rabii, Vice-Président de l'Alliance des Autorités de Cybersécurité ANCA.*

09 h 30 – 10 h 10 | Panel 1 : Renforcer la résilience numérique de l'Afrique : l'IA, le cloud de confiance et le cloud fédéré comme catalyseurs stratégiques. Ce panel explorera des approches pratiques pour renforcer la résilience numérique de l'Afrique en exploitant le potentiel de l'intelligence artificielle (IA), du cloud de confiance et des solutions cloud fédérées. S'appuyant sur des expériences internationales et africaines, la discussion portera sur les stratégies opérationnelles, le développement d'écosystèmes durables et les collaborations public-privé essentielles nécessaires à la construction d'un avenir numérique sûr et souverain. En présentant des exemples concrets, le panel vise à traduire les discussions stratégiques en mesures concrètes adaptées aux contextes uniques de l'Afrique.

- *S.E. Shaikh Salman bin Mohammed Al-Khalifa, PDG du Centre national de cybersécurité (NCSC), Royaume de Bahreïn.*
- *Dr. Ammar Hassan Al-Husseini, ancien Directeur général de l'Agence centrale pour les technologies de l'information (CAIT), État du Koweït.*
- *Dr. Albert Antwi-Boasiako, Directeur général de l'Autorité de cybersécurité du Ghana (CSA) et Président de l'Alliance de l'Autorité de cybersécurité ANCA, République du Ghana.*
- *M. Didier Nkurikiyimfura, Directeur de la Stratégie et de la Croissance chez Smart Africa.*
- *M. Khalil Nossair, Directeur de l'Assistance, de l'Audit, de la Formation, du Contrôle et de l'Expertise, DGSSI.*
- *Dr. Redda Ben Geloune, expert en intelligence artificielle avec une vaste expérience en Afrique, se concentrant sur l'IA pour le développement économique et technologique.*
    - *Mme Neama Benhammou, Responsable Cybersécurité.*

10 h 10 à 10 h 25 | Keynote 2 : Rapprocher les continents : renforcer la cybersécurité grâce au renforcement collaboratif des capacités et au partage de l'expertise.

Cette keynote portera sur la nécessité de mettre en place une entité panafricaine affiliée opérationnellement à l'ANCA, en s'inspirant du modèle du Centre régional arabe de cybersécurité (ARCC) de l'UIT. Une telle structure jouerait un rôle stratégique dans l'échange de renseignements sur les menaces en temps réel, la coordination des interventions en cas d'incident et l'amélioration de la résilience face aux cybermenaces transfrontalières. Il explorera également les moyens de renforcer la coopération entre l'ANCA et les centres nationaux de cybersécurité des États membres de l'Organisation de la coopération islamique (OCI). Cette collaboration mutuellement bénéfique faciliterait l'échange d'expériences et de pratiques exemplaires tout en soutenant la mise en œuvre de programmes de formation et d'exercices régionaux visant à renforcer les capacités de cybersécurité des deux parties.

- *S.E. M. Badar Ali Al-Salehi, Ingénieur général, Directeur général du CERT national d'Oman, Président des Centres nationaux de cybersécurité de l'OCI, Chef du Centre régional de cybersécurité de l'UIT, Sultanat d'Oman.*

10 h 25 – 10 h 40 | Discussion informelle : Faire le lien entre la cybersécurité et la diplomatie : naviguer dans la cyberdiplomatie dans la région MENA et au-delà. Cette discussion informelle explorera les principaux défis et opportunités dans la région MENA, en mettant l'accent sur le rôle de l'engagement diplomatique dans l'atténuation des cyberconflits et la promotion de la coopération. La discussion mettra également en lumière les expériences internationales en matière de cyberdiplomatie. En examinant les partenariats interrégionaux, la session découvrira des stratégies pour renforcer les cadres de cybersécurité, améliorer la résilience et promouvoir le développement numérique durable. À l'aide d'un point de vue diplomatique et technique, cette conversation fournira des conseils précieux pour relever les défis mondiaux en matière de cybersécurité tout en favorisant la stabilité et la coopération au-delà des frontières.

- *Dr. Nadher Alsafvani, conseiller cyber pour la région MENA au Centre pour le dialogue humanitaire (HD), Suisse.*
- *Dr. Najm Alotaibi, professeur agrégé d'informatique et directeur des programmes de qualification à l'Institut Prince Saud Al Faisal pour les études diplomatiques, Arabie saoudite.*
    - *M. Hicham Bayar, Chef de l'Unité du Désarmement et de la Non-Prolifération, Ministère des Affaires Etrangères, de la Coopération Africaine et des Marocains Résidant à l'Etranger.*

10 h 40 – 10 h 50 | Keynote stratégique : Cloud qualifié : une approche politique de la cybersouveraineté et de la confiance numérique.

Alors que les cybermenaces deviennent de plus en plus sophistiquées et omniprésentes, le cloud qualifié s'impose comme un pilier clé pour garantir la conformité réglementaire, la résilience et la sécurité des systèmes d'information sensibles. En s'appuyant sur une expertise éprouvée, elle aide les organisations à surmonter les contraintes internes et financières tout en améliorant la cybersécurité globale. De plus, la mise en place d'un cadre réglementaire clair permet aux parties prenantes de toutes tailles d'adopter en toute confiance des solutions cloud et des technologies émergentes, favorisant ainsi un écosystème numérique sécurisé et souverain.

- *M.* Saad El Khadiri, Directeur de la Stratégie et de la Régulation, DGSSI.

10 h 50 – 11 h 00 | Keynote 3 : L'évolution de l'IA et du cloud de confiance : façonner l'avenir de la résilience industrielle.

Cette conférence explorera comment l'intelligence artificielle (IA) et les technologies infonuagiques de confiance transforment les infrastructures essentielles en favorisant l'innovation, en améliorant la résilience et en permettant une transformation numérique sécurisée. Il se penchera sur les avancées de l'IA et de l'infrastructure cloud, en mettant en évidence leurs applications variées dans des secteurs tels que la santé, les transports et l'énergie. La session mettra l'accent sur les avantages stratégiques de ces technologies pour relever les défis spécifiques de l'industrie, promouvoir la durabilité et optimiser l'efficacité opérationnelle.

- *M. Jeff Wang, président du département Cybersécurité et protection de la vie privée, groupe Huawei.*

Sécurisation des secteurs critiques et des opérations industrielles

11 h 00 – 11 h 30 | Panel 2 : Renforcer la sécurité et l'efficacité des opérations industrielles à l'ère de l'IA et du cloud : Focus sur le secteur pétrolier et gazier.

Ce panel examinera l'impact stratégique de l'infonuagique qualifiée et de l'intelligence artificielle (IA) sur la sécurisation et l'optimisation des opérations industrielles, notamment dans l'industrie pétrolière et gazière. Il fournira des éclairages stratégiques et opérationnels aux professionnels des secteurs pétrolier, gazier et industriel, en proposant des solutions concrètes pour intégrer efficacement l'IA et des services cloud qualifiés dans leurs processus de transformation numérique.

- *M. Fouad Jellal, Directeur Général, Groupe CBI.*
- *M. Monir Kamal, Affaires nationales de cybergouvernance et d'assurance, Agence nationale de cybersécurité, État du Qatar.*
- *M. Abdullah Mah'd Hassan, Directeur de l'exploitation, Muscat Investment House (MIH), Sultanat d'Oman.*
- *M. Basem Ramadan Alkayyali, Président-directeur général (PDG), Muscat Investment House Group, Sultanat d'Oman.*
- *M. Amine Kandil, fondateur et PDG de OneCloud.*
- *M. Mounir Soussi, vice-président du département Cloud et IA de Huawei NA.* ○ *Mme Neama Benhammou, Responsable Cybersécurité.*

11 h 30 – 11 h 45 | Keynote 4 : Gestion proactive des risques pour la sécurisation des secteurs critiques.

Cette conférence examinera en profondeur la manière dont l'intelligence artificielle est déployée pour sécuriser des secteurs critiques tels que l'énergie, la santé et la finance. À travers des études de cas réels, la présentation démontrera les puissantes capacités de l'IA à détecter et à prévenir les cybermenaces avant qu'elles ne causent des dommages. En mettant l'accent sur une gestion proactive des risques, l'IA améliore la posture de sécurité de ces infrastructures essentielles, réduit les vulnérabilités opérationnelles et minimise les temps d'arrêt causés par les cyberincidents. Les participants acquerront des informations pratiques sur la façon dont les solutions d'IA sont intégrées dans les stratégies de cybersécurité afin de renforcer la résilience et de maintenir la continuité des services critiques.

- *Mme Kirsty Paine, directrice technique sur le terrain, Cisco.*

11 h 45 – 12 h 15 | Panel 3 : Stratégies de cybersécurité pour les grands événements internationaux : leçons de la Coupe du Monde de la FIFA.

Ce panel examine les exigences uniques en matière de cybersécurité liées à l'accueil d'événements internationaux de grande envergure, tels que la Coupe du monde de la FIFA. Les experts discuteront des cadres de sécurisation des infrastructures critiques, de gestion des menaces en temps réel et de garantie de la conformité aux normes de cybersécurité. Les panélistes exploreront

également le rôle de l'IA dans la surveillance des menaces et la réponse aux incidents, ainsi que l'importance de la coopération internationale entre les équipes de sécurité.

- *Mme Maryam Al-Muftah, Directrice exécutive des opérations d'événements TIC, État du Qatar.*
- *Mme Hind El Fal, Directrice exécutive, Orange.*
- *Mme Nor El Houda Sabbar, Directrice de l'écosystème Cybersécurité, Dataprotect.*
- *Dr. Bilal Issa, responsable technique et support, Trend Micro.*
- *M. Bashar Ismail Amin Al Khatib, V-CISO - COUPE DU MONDE DE LA FIFA Qatar 2022, FIFA.*
- *Dr. Otman Amghou, directeur de la ville intelligente, Microsoft Gulf.* ○ *M. Assad Arabi, Directeur général du Golfe et des marchés émergents, Trend Micro.*

12 h 15 – 12 h 30 | Discours d'orientation 5 : Améliorer la résilience des infrastructures essentielles face aux cybermenaces.

Cette conférence se penchera sur l'application de l'intelligence artificielle pour renforcer la résilience des infrastructures critiques face aux cybermenaces. Les technologies d'IA, telles que la surveillance en temps réel et les capacités de neutralisation des menaces, sont essentielles pour sécuriser des secteurs essentiels tels que l'énergie, les transports et les soins de santé. En tirant parti de l'IA, ces secteurs peuvent détecter les vulnérabilités et répondre aux menaces de manière proactive, garantissant ainsi un fonctionnement continu et réduisant les temps d'arrêt. À l'aide d'exemples pratiques, la présentation démontrera le rôle de l'IA dans la prédiction des risques potentiels, la rationalisation des réponses aux incidents et la fourniture de défenses robustes pour maintenir la stabilité et la sécurité des services essentiels.

- *M. Ali El Azzouzi, Fondateur et PDG, Dataprotect.*

Éthique, protection et développement des données

12 h 45 – 13 h 00 | Discours d'ouverture : La protection des données à l'ère numérique : protéger la vie privée et assurer la souveraineté.

Cette keynote soulignera l'importance de la protection des données en tant qu 'épine dorsale de la transformation numérique de l'Afrique. Il examinera comment la protection de la vie privée et la confiance stimulent la croissance économique et favorisent l'innovation tout en plaidant pour l'établissement de la souveraineté nationale sur les données sensibles. La session mettra l'accent sur la création de cadres de gouvernance solides et de pratiques éthiques pour guider les politiques de gestion des données, donnant le ton aux discussions sur la création d'un écosystème numérique sécurisé et inclusif à travers l'Afrique.

- *S.E. M. Omar Seghrouchni, Président de la Commission nationale de contrôle de la protection des données à caractère personnel, CNDP.*

13 h 00 – 13 h 15 | Keynote 6 : Sécurisation des environnements cloud de confiance : protection des données et détection des menaces.

Cette session explorera comment l'intelligence artificielle est exploitée pour sécuriser les environnements Trusted Cloud, en se concentrant sur trois domaines critiques : la protection des données sensibles, la détection des menaces sophistiquées et la garantie de la conformité aux normes de souveraineté numérique. Alors que les gouvernements et les organisations adoptent de plus en plus les clouds de confiance pour garder le contrôle des données à l'intérieur des frontières nationales, le rôle de l'IA devient vital. La présentation mettra en évidence des solutions basées sur l'IA qui offrent une protection renforcée des données, l'identification des menaces en temps réel et le respect des exigences réglementaires et de souveraineté.

- *Dr. Bilal Issa, responsable technique et support, Trend Micro.*
- *M. Amir Jamil, Directeur de l'architecture des solutions, CPX. Émirats arabes unis.*

13 h 15 – 13 h 30 | Keynote 7 : L'évolution de l'IA et du cloud : façonner l'avenir de la résilience numérique.

Cette conférence explorera comment l'intelligence artificielle (IA) et les technologies cloud de confiance transforment les infrastructures essentielles en favorisant l'innovation, en améliorant la résilience et en favorisant une transformation numérique sécurisée. Il se penchera sur les dernières avancées en matière d'IA et d'infrastructure cloud, en mettant en évidence leurs diverses applications dans des secteurs tels que la santé, les transports et l'énergie. La session se concentrera sur les avantages stratégiques de ces technologies pour relever les défis spécifiques de l'industrie, promouvoir la durabilité et optimiser l'efficacité opérationnelle.

- *Mme Kerissa Varma, conseillère en chef de la sécurité de Microsoft.*

13 h 30 – 14 h 00 | Panel 4 : Naviguer dans l'IA en cybersécurité : développement et éthique.

Ce panel se penchera sur le rôle multidimensionnel de l'intelligence artificielle (IA) dans la cybersécurité, en mettant l'accent sur les pratiques de développement sécurisées, les considérations éthiques et l'amélioration de la résilience des infrastructures. Les experts discuteront des défis et des stratégies liés au développement de systèmes d'IA sécurisés, aborderont des dilemmes éthiques tels que la confidentialité et la responsabilité, et exploreront comment des infrastructures robustes peuvent renforcer les mesures de cybersécurité. La session vise à fournir une compréhension complète de l'impact de l'IA sur la cybersécurité et à offrir des informations exploitables aux praticiens et aux décideurs.

- *M. Olivier Gakwaya, Chef de projet pour les technologies émergentes, Smart Africa.*
- *M. Ait Kaddour Youssef, Directeur de la cybersécurité et de la protection de la vie privée, Huawei Maroc.*
- *M. Reda El Bakkali, Directeur Général du Groupe INEOS-CYBERFORCES, Cyberforces.*
- *M. John Edokpolo, Directeur des affaires générales, externes et juridiques, Microsoft.*
- *Mme Nouhade Mechkour, Directrice des Solutions Techniques B2B, Orange Maroc.*
- *M. Anas Chanaa, co-fondateur et PDG, Nucleon Security.* ○ *Modératrice : Mme Yenataba Kignaman-Soro : Consultante principale en cybersécurité.*

Innovations en matière de conformité et de développement sécurisé

14 h 00 – 14 h 15 | Keynote 8 : Transformer le développement de logiciels sécurisés : gestion proactive des menaces et automatisation.

Cette présentation se penchera sur le rôle transformateur de l'intelligence artificielle dans l'amélioration du développement de logiciels sécurisés. La session mettra en évidence des solutions basées sur l'IA qui prennent en charge l'anticipation proactive des menaces, automatisent les contrôles de sécurité essentiels et renforcent la fiabilité globale des logiciels. En intégrant l'IA dans les flux de travail de développement, les entreprises peuvent rationaliser les contrôles de sécurité, identifier les vulnérabilités à un stade précoce et assurer une protection continue tout au long du cycle de développement. Les intervenants partageront des idées pratiques et des exemples concrets, illustrant comment l'IA peut être intégrée dans les processus de développement pour créer des solutions logicielles plus résilientes, sécurisées et robustes.

- *M. Colm Murphy, expert en cybersécurité, Bruxelles Cybersecurity Transparency, Huawei.*

14 h 15 – 14 h 30 | Discours d'orientation 9 : Rationalisation de la conformité en matière de cybersécurité et de la gestion des risques.

Cette session explorera comment l'IA peut aider les organisations à se conformer à des réglementations de plus en plus strictes en matière de cybersécurité. Grâce à des techniques d'analyse et d'automatisation avancées, l'IA permet de surveiller en temps réel les pratiques de sécurité, de détecter les violations de conformité et d'anticiper les risques. Les participants apprendront comment les outils d'IA peuvent simplifier la gestion de la conformité et renforcer la résilience organisationnelle face aux cybermenaces tout en respectant les normes internationales et les exigences légales.

- *M. Alain Sanchez, RSSI de terrain, Fortinet.*

15:00 – 18:00 - **Réunion de l'ANCA**

Deuxième jour – 4 février 2025

---

08 h 50 – 09 h 00 | Discours d'ouverture du Maître de cérémonie : *M. Khalid Al-Amrani, Sultanat d'Oman.*

Ouverture officielle

09 h 00 – 09 h 15 |Discours d'ouverture : Assurer l'avenir numérique de l'Afrique : renforcer la souveraineté et la résilience.

Cette keynote offre une perspective prospective sur l'exploitation de l'intelligence artificielle (IA) pour sécuriser le paysage numérique de l'Afrique. Il se penchera sur la manière dont l'IA peut renforcer la souveraineté numérique, protéger les actifs numériques uniques de l'Afrique et établir un cadre éthique pour son application en matière de cybersécurité. Les participants obtiendront des informations précieuses sur les opportunités et les défis de l'adoption de l'IA, avec des exemples concrets de la manière dont l'IA peut améliorer la résilience numérique de l'Afrique et renforcer les efforts de cybersécurité sur le continent.

- *Dr. Redda Ben Geloune : Expert en intelligence artificielle avec une vaste expérience en Afrique, se concentrant sur l'IA pour le développement économique et technologique.*

09 h 15 – 09 h 45 | Panel ministériel : Intégrer la cybersécurité dans les stratégies numériques nationales : renforcer la confiance numérique.

Ce groupe ministériel de haut niveau examinera comment les gouvernements ont intégré la cybersécurité dans leurs stratégies numériques nationales afin d'atténuer les risques et de renforcer la confiance du public. La discussion portera sur les principaux cadres stratégiques, les meilleures pratiques et les initiatives stratégiques pour une gouvernance efficace de la cybersécurité. Les ministres partageront leurs points de vue sur les approches réglementaires, les partenariats public-privé et les efforts de renforcement des capacités essentiels pour améliorer la résilience nationale et régionale en matière de cybersécurité. La session examinera également des études de cas réussies et des stratégies de collaboration transfrontalière qui renforcent la sécurité numérique tout en favorisant l'innovation et la croissance économique.

- *S.E. MME Amal El Fallah Seghrouchni, Ministre déléguée auprès du Chef du Gouvernement chargée de la Transition numérique et de la Réforme administrative, Royaume du Maroc.*
- *S.E. M. Ibrahim Kalil Konaté, Ministre de la Transition numérique et de la Digitalisation, République de Côte d'Ivoire.*
- *S.E. M. Léon Juste Ibombo, Ministre des postes, des télécommunications et de l'économie numérique, République du Congo.* ○ *Modérateur : Dr. Redda Ben Geloune : Expert en intelligence artificielle avec une vaste expérience en Afrique, se concentrant sur l'IA pour le développement économique et technologique.*

09 h 45 – 10 h 00 |Discours d'ouverture : Vision des priorités et des actions de l'ANCA pour assurer la sécurité et la durabilité du cyberespace africain.

Dans ce discours, le Président de l'Alliance des Autorités Nationales Africaines de Cybersécurité (ANCA) présentera les principales décisions prises lors de la dernière réunion annuelle, mettant en exergue les progrès réalisés. Il présentera également le plan d'action stratégique de l'ANCA pour les années à venir, en mettant l'accent sur le renforcement de la coopération régionale,

l'harmonisation des législations en matière de cybersécurité et la mise en œuvre d'initiatives concrètes pour construire une Afrique plus résiliente face aux cyberattaques.

- *Dr. Albert Antwi-Boasiako, Directeur général de l'Autorité de cybersécurité du Ghana (CSA) et Président de l'Alliance de l'Autorité de cybersécurité ANCA, République du Ghana.*

Renforcer la cybersécurité en Afrique grâce à l'innovation et à la collaboration en matière d'IA

10 h 00 – 10 h 30 | Panel 1 : Tracer une voie unifiée : gouvernance de l'IA et cybersécurité en Afrique.

Cette session réunira des membres potentiels du Conseil de gouvernance de l'IA et des représentants du Réseau africain des autorités de cybersécurité (ANCA) afin d'élaborer conjointement une feuille de route complète pour la gouvernance de l'IA et la cybersécurité à travers le continent. Les participants identifieront les synergies entre les initiatives d'IA et les cadres de cybersécurité, dans le but d'établir des stratégies cohérentes qui répondent aux défis et aux opportunités uniques de l'Afrique dans le paysage numérique. La discussion portera sur l'alignement des objectifs, la définition d'objectifs réalisables et la promotion de partenariats pour améliorer la résilience numérique et le déploiement éthique de l'IA dans toute l'Afrique.

- *M. Bassirou Abdoul Ba, Directeur Général du Parc Sénégal Connecté, République du Sénégal.*
- *M. Adnane Ben Halima, vice-président des relations publiques pour l'Afrique du Nord, de l'Ouest et centrale, Huawei.*
- *M. Sukiraman Manivannan, directeur principal des services de conseil en cybersécurité, CPX Holding, Émirats arabes unis.*
- *M. Monir Kamal, Affaires nationales de cybergouvernance et d'assurance, Agence nationale de cybersécurité, État du Qatar.*
- *M. El Boukhari Amine, Directeur du Conseil et de l'Audit, Orange Cyber defense Africa.* ○ *Modératrice : Mme Yenataba Kignaman-Soro : Consultante principale en cybersécurité.*

10 h 30 – 10 h 45 | Keynote 1 : Construire des infrastructures numériques résilientes : la voie de l'Afrique vers l'excellence en cybersécurité.

Cette conférence aborde le rôle central de l'Afrique dans l'économie numérique mondiale, en mettant l'accent sur la nécessité cruciale de mesures de cybersécurité robustes et de souveraineté technologique pour assurer un développement durable. Il explore l'intégration de technologies innovantes telles que l'intelligence artificielle et les solutions cloud de confiance pour protéger les infrastructures critiques et stimuler la croissance économique. L'importance d'harmoniser les politiques numériques entre les pays africains est soulignée, en favorisant la collaboration à travers des initiatives telles que Smart Africa et le Réseau africain des autorités de cybersécurité (ANCA). Le développement des capacités locales est souligné comme essentiel pour assurer un avenir numérique sûr et prospère au continent.

- *M. stephane Guelfo, SVP Business Solutions, OneCloud.*

10 h 45 – 11 h 00 | Causerie au coin du feu : Lancement du livre du Dr Albert Antwi-Boasiako.

Cette discussion informelle marque le lancement d'un travail charnière en cybersécurité axé sur l'Afrique. Le livre du Dr Albert Antwi-Boasiako se penche sur des stratégies innovantes pour améliorer la résilience numérique et faire face à l'évolution des cybermenaces. Il offre des solutions pratiques à des défis critiques à la fois en Afrique et à l'échelle mondiale.

- *Dr. Albert Antwi-Boasiako, directeur général de l'Autorité de cybersécurité du Ghana (CSA) et président de l'Alliance de l'Autorité de cybersécurité ANCA.*
  - *M. Khalid Al-Amrani, Sultanat d'Oman.*

11 h 00 – 11 h 30 | Panel 2 : Constituer une main-d'œuvre en cybersécurité pour l'avenir.

Ce panel explorera des stratégies pour former des professionnels de la cybersécurité qualifiés afin de faire face aux menaces en constante évolution. Les discussions porteront sur le renforcement des capacités, la promotion des partenariats public-privé, la promotion de la diversité en matière de cybersécurité et la garantie d'un apprentissage continu par le biais d'initiatives d'éducation et de formation.

- *Dr. Assane Gueye Professeur à l'Université Carnegie Mellon Afrique Co-directeur du réseau Upanzi et CyLab-Africa Initiatives chercheur invité, Institut national de normes et de technologie (NIST), République du Sénégal.*
- *Mme Maryse Lydie Madiba Iloumbou, Directrice générale adjointe à l'Agence nationale des infrastructures et fréquences numériques, République du Gabon.*
- *M. Khaled Benjelloun, Directeur général adjoint, CBI.*
- *M. Abderrahim Maroufi, responsable de la cybersécurité NWCA, Cisco.*
- *M. Mohamed Sekkat, CBO, Casanet.*
- *M. Younes Benzagmout, Co-fondateur et PDG, SecDojo.* ○ *Mme Neama Benhammou, Responsable Cybersécurité.*

11 h 30 – 12 h 00 | Panel 3 : Tendances émergentes en matière de cybersécurité en Afrique : naviguer dans le paysage changeant des menaces.

Cette session explorera les derniers développements en matière de cybermenaces à travers le continent, notamment l'essor des ransomwares, des schémas de phishing et des violations de données. Des experts discuteront des implications de ces tendances et partageront les meilleures pratiques pour que les organisations renforcent leur posture de cybersécurité en réponse à l'environnement de menace en constante évolution.

- *M. Philippe Gillet, directeur technique, Gatewatcher.*
- *M. Keyser Tabi, responsable SOC, Dataprotect.*
- *M. Waseem Youssef, Directeur Principal des Solutions Techniques et de l'Ingénierie des Systèmes Afrique du Nord-Ouest, Palo Alto Networks.*
- *M. Driss Kardi, Ingénieur Système d'Entreprise, Afrique Francophone, Exabeam/LogRhythm.*

- *M. Hicham Faik, Au-delà de toute confiance/ Sophos/ Modcod.*
- *M. Driss Benattou, directeur des services professionnels, CBI.* ○ *Modératrice : Mme Yenataba Kignaman-Soro : Consultante principale en cybersécurité.*

12 h 30 – 14 h 30 | Séances 1, 2, 3, 4, 5 et 6 (en parallèle).

Session 1 : Analyse prédictive des menaces avec l'IA et les métadonnées

Détection des menaces en temps réel :

Découvrez comment l'IA améliore l'identification préventive des menaces émergentes en exploitant les normes de métadonnées telles que CVE et CVSS.

(Se concentre sur la détection précoce pour éviter l'escalade, distincte de la gestion des incidents.) Gestion prédictive des risques avec EPSS et VEX :

Utilisez des outils tels que EPSS et VEX pour prévoir les vecteurs d'attaque potentiels et hiérarchiser les vulnérabilités pour des défenses proactives. *(Se concentre sur les prévisions et la hiérarchisation, séparément des flux de travail de gestion à long terme.)*

- *M. Driss Kardi, Ingénieur Système d'Entreprise, Afrique Francophone, Exabeam/LogRhythm.*

Session 2 : Threat Intelligence pilotée par l'IA et planification stratégique de la sécurité dans DevSecOps

Exploiter la Threat Intelligence avec l'IA.

Cette session se concentrera sur la façon dont les organisations peuvent tirer parti de l'IA pour recueillir, analyser et agir sur les renseignements sur les menaces. Les participants exploreront des techniques d'intégration de l'IA dans les flux de travail DevSecOps pour la détection des menaces en temps réel, la hiérarchisation des risques et la prise de décision rapide basée sur les flux de menaces mondiaux et les modèles d'attaque émergents.

Atténuation proactive des risques grâce à des informations stratégiques.

Les participants apprendront comment l'IA peut fournir des informations stratégiques en corrélant des données provenant de diverses sources, ce qui permet une planification éclairée de la sécurité. Cette section se concentre sur la création de cadres de gestion des risques adaptatifs qui s'ajustent dynamiquement à l'évolution du paysage des menaces.

Simulation et planification de la sécurité basées sur des scénarios.

La dernière partie de la session comprendra des exercices pratiques de simulation de scénarios alimentés par l'IA. Les participants apprendront à prévoir les vecteurs d'attaque potentiels, à évaluer leur posture de sécurité et à concevoir des plans de réponse aux incidents robustes basés sur la modélisation prédictive des menaces et l'analyse des données historiques.

- *M. Keyser Tabi, responsable SOC, Dataprotect.*

Séance 3 : Sécurisation de l'infrastructure et des données

Résilience des infrastructures essentielles :

Examinez des stratégies à long terme utilisant l'IA pour protéger dynamiquement les systèmes critiques contre les menaces en constante évolution. *(Se concentre sur les stratégies de sécurité adaptatives pour les systèmes essentiels.)* Sécurité des données dans le cloud :

Découvrez comment l'IA sécurise les environnements cloud en surveillant les flux de données et en détectant les violations spécifiques aux vulnérabilités du cloud.

(Dédié aux défis spécifiques au cloud, distinct de l'automatisation générale.)

Protection des appareils IoT :

Explorez les solutions basées sur l'IA pour protéger les réseaux IoT en identifiant les vulnérabilités et en atténuant les menaces ciblées sur les appareils.

(Spécialisé dans la sécurité de l'IoT, évitant les chevauchements avec des sujets d'infrastructure plus larges.) L'IA pour la gestion des identités et des accès :

Découvrez comment l'IA améliore les systèmes IAM grâce à la détection des anomalies et aux contrôles de sécurité automatisés. (Cible les améliorations spécifiques à l'IAM, indépendamment des discussions générales sur l'infrastructure ou l'automatisation.)

- *M. Adil Taleb, directeur technique exécutif, département des affaires d'entreprise, Huawei.*
- *M. Zhang Shaochen (Eddy), expert en cloud et en sécurité cloud, siège social de Huawei.*
- *M. Youssef Boukhary, expert en sécurité, Huawei Afrique du Nord.*

Séance 4 : Gestion stratégique des vulnérabilités

Gestion simplifiée des vulnérabilités grâce à l'IA :

Utilisez l'IA pour améliorer les flux de travail afin d'identifier, de hiérarchiser et de corriger les vulnérabilités, améliorant ainsi la posture de sécurité globale.

(Se concentre sur la planification stratégique, en évitant les chevauchements avec les processus opérationnels en temps réel.) Cadres de gestion fondés sur des normes :

Découvrez comment intégrer les normes de métadonnées telles que CVE, CVSS, EPSS et VEX dans les stratégies de gestion des vulnérabilités à long terme.

(Met l'accent sur l'intégration stratégique, distincte des outils de prévision dans la session 1.) Optimisation proactive des vulnérabilités :

Apprendre des techniques avancées pour transformer les processus de gestion des vulnérabilités, réduire les risques et améliorer l'efficacité. *(Dédié à la transformation du flux de travail, en évitant les chevauchements avec l'automatisation des tâches opérationnelles.)*

M. Bilal Issa, responsable technique et support, Trend Micro.

Séance 5 : Maîtriser la sécurité avec l'IA

Libérer le potentiel de l'IA pour la cyberdéfense

Plongez dans le pouvoir de transformation de l'apprentissage automatique (ML) et de l'intelligence artificielle (IA) pour améliorer les opérations de sécurité. Découvrez comment ces technologies peuvent détecter les menaces, découvrir les activités suspectes et renforcer vos défenses.

Apprentissage pratique avec des scénarios du monde réel

Participez à des exercices pratiques qui reproduisent les défis du monde réel, en vous dotant des compétences nécessaires pour appliquer efficacement le ML et l'IA dans les flux de travail de sécurité.

Intégration transparente pour une détection avancée des menaces

Découvrez comment intégrer le ML et l'IA dans vos processus existants pour optimiser la détection des menaces et améliorer les temps de réponse, tout en gardant une longueur d'avance dans un paysage de cybersécurité en constante évolution.

- *M. Mehdi Benali, Partner Technical Manager Splunk, Cisco.*

Séance 6 : Améliorer la sécurité du cloud grâce à l'IA : défis et solutions

Sécuriser le Cloud grâce à l'IA

Cette séance explorera comment l'intelligence artificielle (IA) est exploitée pour améliorer la cybersécurité dans les environnements infonuagiques. Les participants découvriront les outils basés sur l'IA qui permettent de détecter les menaces en temps réel, d'identifier les anomalies et de répondre automatiquement pour atténuer les risques associés à l'infrastructure cloud.

Défis et solutions en matière de sécurité du cloud

Nous aborderons les défis uniques en matière de cybersécurité qui se posent dans les environnements cloud, tels que les problèmes de confidentialité des données, les configurations multicloud et la sécurisation des applications cloud natives. Des experts partageront les meilleures pratiques et les solutions basées sur l'IA pour relever efficacement ces défis.

Approches pratiques pour l'intégration de l'IA

À travers des études de cas réels, cet atelier guidera les participants sur la façon d'intégrer de manière transparente l'IA dans leurs stratégies de sécurité du cloud. Les participants acquerront une expérience pratique de l'application de l'IA pour améliorer la veille sur les menaces, améliorer la surveillance de la conformité et automatiser les opérations de sécurité dans le cloud.

- *M. Stephane Guelfo, SVP Business Solutions, OneCloud.*
- *Mme Salwa El Ouattab, Experte en cybersécurité, OneCloud.*
- *M. Badr El Aissaoui, chef d'équipe Cloud Presales & Architect, OneCloud.*

15 h 00 – 18 h 00 – **Réunion du Conseil IA**

مجلس الذكاء الاصطناعي

Conseil de l'IA

Deuxième jour - 4 février 2025

14 h 00 à 14 h 30 | Arrivée et connexion des participants.

Ouverture officielle

14 h 30 - 15 h 00 : Discours ministériel

Session du Conseil africain de l'IA : Ouverture et discussions stratégiques

15h00 - 15h10 : Mot d'introduction/d'ouverture

- *Qhala.*
- *C4IR.*
- *Smart Africa.*

15h10 - 15h30 : État des lieux de la préparation de l'Afrique à l'IA

15h30 - 16h00 : Examen de la note conceptuelle du Conseil africain de l'IA

16h00 - 16h45 : Discussion

Déclaration de Kigali sur l'IA en Afrique : Présentation et discussion

17h00 - 17h30 : Présentation de la Déclaration de Kigali sur l'IA en Afrique

17 h 30 - 18 h 15 : Discussion

Présentation de la boîte à outils pour la gouvernance de l'IA en Afrique

18h15 - 18h30 : Présentation de la boîte à outils pour la gouvernance de l'IA en Afrique

18 h 30 - 18 h 40 : Mot de la fin

- *Qhala.*
- *C4IR.*
- *Smart Africa.*

Troisième jour – 5 février 2025

09 h 00 – 11 h 30 | Séances 7, 8, 9, 10, 11 et 12 (en parallèle).

Séance 7 : Analyse des incidents et intervention rapide

Analyse médico-légale avec l'IA.

Cet atelier abordera l'utilisation de l'IA dans l'analyse post-incident afin d'accélérer les enquêtes cybercriminelles en automatisant la collecte et l'analyse des preuves numériques.

Intégration de l'IA dans les centres d'opérations de sécurité (SOC).

L'intégration de l'IA dans les SOC sera explorée pour améliorer la gestion des incidents en temps réel, en automatisant la surveillance continue et la réponse aux menaces.

Simulation d'IA et de cyberattaques pour les tests de résilience des systèmes.

Cet atelier montrera comment l'IA peut être utilisée pour simuler des cyberattaques complexes, en permettant des tests de résilience et en renforçant les défenses contre les menaces réelles.

- *Mme Imane Bachane, Experte en Cybersécurité, CBI-BLUESEC.*
- *M. Jamel Eddine Hadini, Expert en Cybersécurité, CBI-BLUESEC.*

Séance 8 : Prévention et identification des menaces

Détection avancée du phishing avec l'IA.

Les participants apprendront à utiliser l'IA pour détecter les tentatives de phishing et autres cyberattaques en analysant les comportements suspects et en identifiant les menaces en temps réel.

Intégration de l'IA dans les systèmes de détection d'intrusion (IDS).

Cet atelier montrera comment intégrer l'IA dans l'IDS pour améliorer la détection des menaces en temps réel en analysant les comportements anormaux et en automatisant les réponses.

Cybersécurité prédictive avec l'IA : anticiper les menaces.

L'accent sera mis sur l'utilisation de l'IA pour anticiper les cybermenaces avant qu'elles n'apparaissent en analysant des données à grande échelle et en identifiant les modèles d'attaque potentiels.

Utilisation de l'IA pour la prévention de la fraude en ligne.

Cet atelier portera sur la détection et la prévention de la fraude en ligne à l'aide de l'IA en analysant les comportements suspects et en identifiant les transactions anormales.

- *M. Youness Fikhar, ingénieur système senior, Fortinet.*

Session 9 : Prédiction avancée des menaces et des attaques

Analyse avancée des menaces et prédiction des attaques.

Cet atelier explorera l'utilisation de l'apprentissage automatique et de l'apprentissage profond pour analyser de grands ensembles de données et identifier les menaces potentielles avant qu'elles ne se produisent.

Détection des menaces internes à l'aide de l'IA.

Les participants apprendront à utiliser l'IA pour détecter les menaces internes et analyser les comportements anormaux afin d'identifier les activités suspectes des employés ou des appareils compromis.

- *M. Moussa Koita, consultant en cybersécurité, Gatewatcher.*

Séance 10 : Stratégies de cyberdéfense basées sur l'IA

Renseignements proactifs sur les menaces

Exploitez la puissance de l'apprentissage automatique pour révolutionner les stratégies de cybersécurité. Ce segment se concentrera sur la façon dont les algorithmes avancés permettent la détection précoce de menaces complexes, fournissant aux organisations les outils nécessaires pour anticiper et atténuer les risques avant qu'ils ne s'intensifient.

Analyse comportementale alimentée par l'IA

Plongez dans l'application de l'analyse comportementale pilotée par l'IA pour identifier les anomalies subtiles dans les activités des utilisateurs et des appareils. Découvrez comment ces informations peuvent révéler des menaces internes, des tentatives d'accès non autorisé et des systèmes compromis, renforçant ainsi la sécurité globale.

Transformer la cyberdéfense grâce à l'IA

Explorez l'impact plus large de l'intelligence artificielle sur la cyberdéfense moderne. Qu'il s'agisse de prédire les attaques ou d'améliorer les processus de prise de décision, cette session montrera comment l'IA remodèle le paysage de la cybersécurité proactive.

- *M. Tarik Dahni, Au-delà de toute confiance.*
- *M. Zouhair Slaoui, Sophos.*
- *M. Serge Simissi, Modcod.*

Séance 11 : Sécurité des données et conformité réglementaire

Sécurisation de l'IA générative.

Cet atelier abordera la protection des modèles d'IA générative, en expliquant comment sécuriser les données qu'ils traitent et prévenir les abus. Développer des algorithmes d'IA pour la protection des données personnelles.

Les participants découvriront comment l'IA peut être utilisée pour renforcer la protection des données personnelles tout en garantissant le respect des réglementations en matière de protection de la vie privée.

L'IA pour la conformité réglementaire en matière de cybersécurité.

Cet atelier démontrera comment l'IA peut aider les organisations à automatiser les audits de cybersécurité et à assurer la conformité aux normes de sécurité.

- *M. Anas Chanaa, co-fondateur et PDG, Nucleon Security.*
- *M. Younes Benzagmout, Co-fondateur et PDG, SecDojo.*
- *M. Youssef Agoumi, Managing Partner, Formind Afrique et Moyen-Orient.*

Séance 12 : Améliorer la gestion des risques dans DevSecOps pour un développement sécurisé

Automatisation de la sécurité avec l'IA dans DevSecOps.

Cette session se concentrera sur la façon dont l'IA peut automatiser et renforcer les processus de sécurité dans DevSecOps. Les participants découvriront comment l'IA peut être intégrée dans les outils de développement pour analyser le code en temps réel, identifier les vulnérabilités au début du cycle de développement, optimiser les tests de sécurité dans les pipelines CI/CD et accélérer la résolution des problèmes.

Surveillance continue de la sécurité dans les environnements de développement.

La deuxième partie abordera la surveillance continue des environnements de développement et de production. L'IA permet une analyse proactive des activités suspectes et des comportements anormaux, ce qui garantit que les vulnérabilités et les menaces potentielles sont détectées et traitées rapidement.

Réduction des risques et optimisation de la réponse aux incidents.

Cette dernière partie se concentrera sur la façon dont l'IA optimise les réponses aux incidents de sécurité, en minimisant l'impact des attaques. Associée aux pratiques DevSecOps, l'IA permet une gestion proactive des incidents grâce à la hiérarchisation des vulnérabilités, à l'automatisation des réponses rapides et à la réduction des temps d'intervention.

- *M. Amjad Jabali, consultant en solutions Prisma Cloud, Palo Alto Networks.*

12h00 – 12h30 – **Séance interactive interentreprises (B2B)**