DOSSIER DE PRESSE

COMMUNIQUÉ DE PRESSE

Lancement de SOC4AFRICA : une offre panafricaine pour une cyberdéfense souveraine et accessible

Douala, le 1er juillet 2025

Les entreprises **ST Digital** et **RHOPEN Labs** annoncent aujourd'hui le lancement officiel de **SOC4AFRICA**, la première offre intégrée de Centre des Opérations de Sécurité (SOC) pensée par et pour l'Afrique. Cette initiative stratégique vise à renforcer la souveraineté numérique du continent, en rendant accessible une cyberdéfense de haut niveau, contextualisée et maîtrisée localement.

Une réponse forte aux enjeux cyber du continent

L'Afrique connaît une explosion des cyberattaques, mais reste encore sous-équipée face à ces menaces. Les organisations africaines sont souvent dépendantes de solutions importées, coûteuses, peu adaptées et parfois opaques.

SOC4AFRICA apporte une réponse concrète et ambitieuse : une **solution souveraine, évolutive et mutualisée**, alliant infrastructure locale, outils de cybersécurité open source avancés, et expertise terrain.

Pour Anthony SAME, CEO de ST Digital, *« Avec SOC4AFRICA, nous voulons faire passer l'Afrique de la dépendance cyber à la souveraineté active. »*

Un partenariat stratégique africain

SOC4AFRICA est né de la collaboration entre deux acteurs technologiques africains:

- **ST Digital**, spécialiste des infrastructures numériques et exploitant de datacenters dans plusieurs pays africains, assure l'hébergement sécurisé, la disponibilité et la proximité des services ;

- ∉ **RHOPEN Labs**, pionnier du cyberscoring et de la sécurité opérationnelle, fournit la technologie SOC Labs, les outils d'analyse, de surveillance et de remédiation, ainsi que la gouvernance cyber et le support expert.

« Cette alliance technique et commerciale montre que l'Afrique peut produire des solutions robustes, souveraines et compétitives. » selon **François-Xavier DJIMGOU, Président de RHOPEN Labs.**

Deux formules pour couvrir tous les besoins

L'offre SOC4AFRICA se décline en deux formats :

- ∉ **SOC as a Service** : pour les entreprises et administrations souhaitant externaliser la surveillance et la réponse aux incidents, via un abonnement souple et scalable.

- ∉ **Build Your Own SOC** : pour les structures désireuses de mettre en place leur propre SOC, avec un accompagnement complet de la conception au déploiement.

Une conférence de presse dans un SOC opérationnel

À l'occasion de ce lancement, une conférence de presse s'est tenue dans l'un des Centres des Opérations de Sécurité déjà aménagés par les partenaires. Ce fut l'opportunité de présenter la vision, les fonctionnalités de la solution SOC4AFRICA, les cas d'usage, ainsi que les modalités d'abonnement ou de partenariat.

Contact Médias

Jacques ABENG

Directeur Marketing Groupe ST Digital

+237 686016893 |jacques@st.digital

CONTEXTE ET ENJEUX

La cybersécurité en Afrique : un défi critique

L'Afrique traverse une transformation numérique accélérée qui, si elle ouvre de formidables opportunités de développement, expose également le continent à des vulnérabilités cybersécuritaires sans précédent.

Les chiffres alarmants :

- **+60% d'attaques** ciblant l'Afrique par rapport à la moyenne mondiale
- **5,13 millions de dollars:** coût moyen d'un rançongiciel pour les victimes africaines
- **19 millions de cyberattaques** subies par le seul Cameroun en 2024
- **68 000 postes** en cybersécurité non pourvus sur le continent

Les défis spécifiques au continent

- **Digitalisation rapide** créant de nouvelles vulnérabilités
- **Sophistication croissante** des cybermenaces
- **Menaces sur les infrastructures critiques** (énergie, télécommunications, finance)
- **Besoin de souveraineté numérique** et de solutions adaptées aux réalités africaines
- **Pénurie critique de talents** en cybersécurité

SOC4AFRICA : UNE SOLUTION RÉVOLUTIONNAIRE

Qu'est-ce qu'un SOC ?

Un SOC (Security Operations Center) est un centre d'opérations de sécurité informatique qui assure :

- **Surveillance continue** des réseaux, applications et terminaux
- **Détection proactive** des activités suspectes ou malveillantes
- **Analyse approfondie** des incidents de sécurité
- **Réponse rapide** pour minimiser les dommages
- **Gestion centralisée** de la sécurité informatique

Une proposition de valeur unique

SOC4AFRICA se distingue par cinq piliers fondamentaux :

1. Souveraineté garantie

- Données hébergées exclusivement en Afrique
- Conformité aux réglementations locales
- Maîtrise totale des infrastructures critiques

2. Expertise locale contextuelle

- Détections adaptées aux menaces spécifiques au continent
- Réponses calibrées selon les réalités africaines
- Connaissance approfondie de l'écosystème local

3. Technologies de pointe

- SIEM (Security Information and Event Management)
- XDR (Extended Detection and Response)
- CTI (Cyber Threat Intelligence)
- SOAR (Security Orchestration, Automation and Response)
- DFIR (Digital Forensics and Incident Response)

4. Proximité et réactivité

- Support local en langues nationales
- Équipes déployées sur le continent
- Temps de réponse optimisés

5. Flexibilité et accessibilité

- Offre SOCaaS (SOC as a Service)
- Option BYOS (Build Your Own SOC)
- Tarification adaptée aux budgets africains

OFFRE DE SERVICES COMPLÈTE

Les quatre piliers d'intervention

PRÉVENTION - Renforcer la posture de sécurité

- Monitoring continu des vulnérabilités
- Hardening et renforcement des configurations
- Formation et sensibilisation des collaborateurs

DÉTECTION - Surveillance permanente

- Supervision 24/7 par analystes certifiés
- Déploiement et gestion de sondes EDR/SIEM
- Collecte intelligente des logs et alertes
- Tableaux de bord personnalisés

RENSEIGNEMENT CONTEXTUALISÉ - Anticiper les menaces

- Cyberveille géopolitique et sectorielle
- Enrichissement des données d'alerte
- Renseignement stratégique sur les risques émergents

REMÉDIATION - Réponse efficace

- Force d'action rapide 24/7
- Plan de réponse à incident structuré
- Support à la résolution d'incidents
- Recommandations d'amélioration continue

Trois forfaits adaptés

Critère	BASIC	STANDARD	PREMIUM
Activités	EDR/XDR, réponse, reporting	Activités Basic étendues	Basic + renseignement contextualisé
Gouvernance	Mutualisée	Point focal dédié	Équipe dédiée

Couverture	9h-18h, 5j/7	9h-18h, 5j/7	24h/24, 7j/7
SLA	4 heures	3 heures	2 heures
Stockage	100 Go	120 Go	160 Go
Tarif mensuel	4 000 XAF/équipement	7 500 XAF/équipement	13 375 XAF/équipement

Tarifs hors mise en service

LES ACTEURS DE L'ALLIANCE

ST Digital : le pionnier du Cloud 100% Africain

Profil de l'entreprise :

- Opérateur indépendant de Cloud et d'IA souverain en Afrique de l'Ouest et du Centre
- 3 datacenters et 4 infrastructures de colocation
- Plateforme en ligne : www.cloudstore.africa
- Une centaine d'employés répartis dans 5 filiales

Implantation géographique :

- Cameroun (siège)
- Côte d'Ivoire
- Gabon
- Congo (Brazzaville et Kinshasa)
- Togo

Cœurs de métier :

- Services de transformation digitale
- Hébergement sécurisé de données
- Solutions d'Intelligence Artificielle

Rhopen Labs : L'expertise cybersécurité africanisée

Expertise unique :

- Spécialiste cybersécurité et DevOps

- Développement de solutions souveraines contextualisées
- Portfolio : SOC Labs, ACYRA, CyberTeam

Engagement continental :

- Promoteur du Salon annuel SMI-Cyber (métiers et innovations cybersécurité & IA)
- Filiale africaine du Groupe technologique français RHOPEN
- Rhopen Labs Academy : institut de formation professionnelle agréé
- Co-porteur du "Programme des 100 000 Cyberveilleurs africains"

RÉFÉRENCES ET SUCCESS STORIES

Portefeuille clients de confiance

Secteur bancaire et financier :

- Afriland First Bank
- Banque Atlantique
- Banque Postale
- SCB Banque

Télécommunications et services :

- Gabon Telecom
- SABC

Infrastructures critiques :

- COTCO (Cameroon Oil Transportation Company)

AVANTAGES CONCURRENTIELS

SOC externalisé vs SOC interne

Critère	SOC Interne	SOC4AFRICA (externalisé)
Coût initial	Très élevé	Faible
Coût récurrent	Important et variable	Prévisible et maîtrisé
Flexibilité	Faible	Forte
Expertise	Variable selon les recrutements	Spécialisée et certifiée
SLA/Niveaux de service	À construire	Contractuels et garantis

Impact économique et stratégique

Pour les entreprises :

- ROI optimisé grâce à la mutualisation des coûts
- Accès à une expertise de niveau international
- Réduction du time-to-market pour la sécurisation
- Transformation digitale sécurisée accélérée

Pour le continent :

- Renforcement de la souveraineté numérique Africaine
- Création d'emplois qualifiés locaux
- Développement de l'écosystème cybersécurité
- Protection des infrastructures critiques nationales

VISION ET AMBITIONS

Mission

Démocratiser l'accès à la cybersécurité de niveau international pour toutes les organisations africaines, quelle que soit leur taille, en proposant des solutions souveraines, adaptées et accessibles.

Vision 2030

- Devenir la référence continentale en matière de SOC souverain
- Équiper 1 000+ organisations africaines
- Former 10 000+ professionnels de la cybersécurité
- Contribuer à la résilience numérique du continent

Valeurs fondamentales

- **Souveraineté** : Maîtrise africaine des technologies critiques
- **Excellence** : Standards internationaux adaptés au contexte local
- **Accessibilité** : Solutions démocratisées pour tous
- **Innovation** : R&D continue et anticipation des menaces
- **Responsabilité** : Engagement pour un numérique éthique et sécurisé

INFORMATIONS PRATIQUES

Contacts presse

ST Digital

- Nom : Jacques ABENG
- Fonction : Directeur Marketing Groupe
- Téléphone : +237 686 01 68 93
- Email : jacques@st.digital

Rhopen Labs

- Nom : François Xavier DJIMGOU
- Fonction : CEO RHOpen labs
- Téléphone : +237 6 90 16 36 27
- Email : hilaire.noubissi@rhopen.fr

Ressources disponibles

- Visuels haute définition du logo SOC4AFRICA
- Photos des dirigeants et équipes
- Infographies sur les menaces cyber en Afrique

- Démonstrations techniques disponibles sur demande
- Interviews avec les experts disponibles

Sites web et réseaux sociaux

- **ST Digital** : www.stdigital.africa | www.cloudstore.africa
- **Rhopen Labs** : www.rhopen-labs.com

ANNEXES

Glossaire technique

SOC (Security Operations Center) : Centre d'opérations de sécurité informatique centralisant la surveillance, la détection et la réponse aux incidents de cybersécurité.

SIEM (Security Information and Event Management) : Système de gestion des informations et événements de sécurité permettant la corrélation et l'analyse en temps réel.

XDR (Extended Detection and Response) : Solution de détection et de réponse étendues couvrant plusieurs vecteurs d'attaque.

SOCaaS (SOC as a Service) : Modèle de service externalisé de centre d'opérations de sécurité.

CTI (Cyber Threat Intelligence) : Renseignement sur les menaces cybernétiques pour une détection proactive.

Sources et références

- Global Cybersecurity Forum & BCG - Rapport sur la cybersécurité en Afrique 2024
- Interpol - Étude sur les coûts des cybercrimes en Afrique 2024
- Kaspersky - Statistiques des cyberattaques au Cameroun 2024

QUESTIONS STRATÉGIQUES ET VISION

Q1 : Pourquoi lancer SOC4AFRICA maintenant ? Qu'est-ce qui vous a décidé à vous associer ?

Éléments de réponse :

- Urgence liée à l'explosion des cyberattaques (+60% vs moyenne mondiale)
- Coût dramatique : 5,13M$ par rançongiciel pour les victimes africaines
- Pénurie critique : 68 000 postes cybersécurité non pourvus en Afrique
- Complémentarité parfaite : infrastructure souveraine ST Digital + expertise cyber Rhopen Labs
- Moment favorable : maturité digitale des entreprises africaines + besoin de souveraineté

Q2 : En quoi SOC4AFRICA se différencie-t-il des solutions internationales existantes ?

Éléments de réponse :

- **Souveraineté** : données 100% hébergées en Afrique, conformité locale
- **Contextualisation** : menaces et réponses adaptées aux réalités africaines
- **Accessibilité** : tarifs adaptés aux budgets locaux (dès 4 000 XAF/mois)
- **Proximité** : équipes locales, support en langues nationales
- **Expertise régionale** : connaissance approfondie de l'écosystème africain

Q3 : Quels sont vos objectifs chiffrés pour les 3-5 prochaines années ?

Éléments de réponse :

- **2025-2026** : 100 organisations clientes, 5 pays couverts
- **2027-2028** : 500 organisations, extension Afrique de l'Est
- **2030** : 1 000+ organisations, 10 000 professionnels formés
- **Impact économique** : Réduction de 40% des coûts cyber pour nos clients
- **Souveraineté** : 80% des infrastructures critiques africaines protégées localement

QUESTIONS TECHNIQUES ET OPÉRATIONNELLES

Q4 : Concrètement, comment fonctionne votre SOC ? Quelles technologies utilisez-vous ?

Éléments de réponse :

- **SIEM** : corrélation intelligente des événements de sécurité
- **XDR** : détection étendue sur endpoints, réseaux, cloud
- **CTI** : renseignement sur menaces spécifiques à l'Afrique
- **SOAR** : automatisation des réponses aux incidents
- **Équipes 24/7** : analystes certifiés basés localement
- **Tableaux de bord** personnalisés pour chaque client

Q5 : Comment garantissez-vous la souveraineté des données ? Où sont hébergées les informations ?

Éléments de réponse :

- **Datacenters ST Digital** : 3 sites certifiés en Afrique (Cameroun, Côte d'Ivoire, Gabon)
- **Juridiction africaine** : respect des lois locales de protection des données
- **Chiffrement bout-en-bout** : données protégées en transit et au repos
- **Équipes locales** : aucun transfert vers l'extérieur du continent
- **Certifications** : conformité ISO 27001, SOC 2 Type II

Q6 : Quels sont vos délais de déploiement et niveaux de service ?

Éléments de réponse :

- **Déploiement** : 2-4 semaines selon la complexité
- **SLA contractuels** : 2h (Premium), 3h (Standard), 4h (Basic)
- **Disponibilité** : 99,9% garantie sur nos infrastructures
- **Support** : équipes dédiées par forfait (mutualisé → dédié)
- **Escalade** : procédures claires jusqu'au management

QUESTIONS ÉCONOMIQUES ET BUSINESS

Q7 : Vos tarifs paraissent très accessibles. Comment maintenez-vous la rentabilité ?

Éléments de réponse :

- **Mutualisation des coûts** : économies d'échelle du modèle SaaS
- **Optimisation technologique** : automatisation poussée des processus
- **Expertise locale** : coûts RH optimisés vs consultants internationaux
- **Infrastructure existante** : capitalisation sur les datacenters ST Digital
- **Modèle évolutif** : montée en gamme naturelle des clients

Q8 : Qui sont vos clients cibles ? Quels secteurs prioritaires ?

Éléments de réponse :

- **Secteur bancaire/financier** : réglementation stricte, cible naturelle
- **Télécommunications** : infrastructures critiques, enjeux de continuité
- **Secteur public** : ministères, collectivités, services publics
- **PME/ETI** : besoin croissant, budgets limités = cible prioritaire
- **Multinationales** : filiales africaines cherchant la conformité locale

Q9 : Comment vous positionnez-vous face à la concurrence internationale ?

Éléments de réponse :

- **Avantage souveraineté** : enjeu critique post-COVID et géopolitique
- **Coût total** : TCO inférieur de 60% vs solutions internationales
- **Réactivité** : équipes sur le même fuseau horaire
- **Personnalisation** : solutions adaptées aux spécificités locales
- **Partenariats stratégiques** : écosystème local vs approche parachutée

QUESTIONS SECTORIELLES ET RÉGLEMENTAIRES

Q10 : Comment SOC4AFRICA s'adapte-t-il aux différentes réglementations africaines ?

Éléments de réponse :

- **Veille réglementaire** : suivi permanent des évolutions légales
- **Conformité native** : conception selon les standards les plus stricts
- **Adaptabilité** : paramétrage selon les exigences nationales
- **Expertise juridique** : partenariats avec cabinets spécialisés
- **Anticipation** : préparation aux futures réglementations (RGPD africain)

Q11 : Quelle est votre stratégie face à la pénurie de talents cybersécurité en Afrique ?

Éléments de réponse :

- **Programme de formation** : 100 000 cyberveilleurs africains (Rhopen Labs)
- **Partenariats académiques** : universités et écoles d'ingénieurs
- **Certification** : programmes de montée en compétences internes
- **Rétention** : conditions attractives, projets stimulants
- **Essaimage** : formation de futurs entrepreneurs cyber

QUESTIONS TECHNIQUES APPROFONDIES

Q12 : Comment gérez-vous les menaces spécifiques à l'Afrique ?

Éléments de réponse :

- **Threat Intelligence locale** : analyse des menaces régionales
- **Patterns africains** : connaissance des modes opératoires locaux
- **Langues locales** : détection d'attaques en français, anglais, langues nationales
- **Secteurs sensibles** : focus mines, pétrole, télécoms, banque
- **Géopolitique** : prise en compte des tensions régionales

Q13 : Quelle est votre stratégie de R&D et d'innovation ?

Éléments de réponse :

- **IA et Machine Learning** : détection comportementale avancée
- **Blockchain** : traçabilité et intégrité des logs
- **Edge Computing** : traitement local pour réduire la latence
- **Partenariats tech** : collaboration avec éditeurs internationaux
- **Open Source** : contribution à l'écosystème communautaire

MESSAGES CLÉS À RETENIR

Pour les dirigeants présents :

1. **Insister sur la souveraineté** : enjeu géopolitique majeur
2. **Mettre en avant l'accessibilité** : démocratisation de la cybersécurité
3. **Valoriser l'expertise locale** : "by Africa, for Africa"
4. **Souligner l'urgence** : statistiques alarmantes des cyberattaques
5. **Projeter la vision 2030** : impact continental et transformation digitale

Messages à éviter :

- Comparaisons directes dépréciatives avec la concurrence
- Promesses irréalistes sur les délais ou performances
- Détails techniques trop pointus pour un public généraliste
- Critiques des solutions existantes ou des politiques publiques
- Annonces prématurées sur des développements futurs non confirmés