LIVRE BLANC

Renforcer la sécurité numérique en Afrique : l'importance stratégique du SOC

ST DIGITAL data center services

RHOPEN LABS
Le talent africain à la conquête du monde!

Avis de non-responsabilité

Ce document a été créé par ST DIGITAL et RHOPEN LABS. Les informations fournies ici le sont à des fins éducatives uniquement et ne constituent pas un avis juridique ou professionnel. Bien que nous ayons fait tous les efforts possibles pour assurer l'exactitude et la fiabilité des informations présentées, ST DIGITAL et RHOPEN LABS déclinent toute garantie ou représentation, expresse ou implicite, concernant l'exhaustivité, l'exactitude ou l'utilité de ce document. Toute confiance accordée aux informations contenues dans ce document est strictement à vos risques et périls. ST DIGITAL et RHOPEN LABS ne peuvent être tenus responsables de tout dommage résultant de l'utilisation ou de la confiance accordée à ce document, sans sollicitation d'une expertise avisée.

ST DIGITAL & RHOPEN LABS

SOMMAIRE

INTRODUCTION

La sécurité des systèmes d'information est devenue une préoccupation majeure pour les entreprises et les organisations à travers le monde. L'Afrique, en tant que continent en plein essor sur le plan technologique et économique, n'échappe pas à ces défis. C'est dans ce contexte que ce livre blanc, intitulé **"Renforcer la sécurité numérique en Afrique : L'importance stratégique du SOC"** prend toute sa signification.

En raison de l'augmentation constante des failles de sécurité, de la sophistication et du nombre croissant des cyberattaques, il est impératif que les entreprises ré-examinent leur approche de la cybersécurité aujourd'hui. Il est à présent indispensable de passer à une approche qui met l'accent sur une analyse complète des données en utilisant des outils de supervision avancés, de détection des menaces et de réponse aux cyberattaquants.. Afin d'y parvenir, il est impératif de franchir cette étape qui est de revoir les infrastructures informatiques déjà en place et d'en adopter des plus modernes et actualisées.

Le présent livre blanc se concentre sur un élément essentiel de la défense numérique : le Centre des Opérations de Sécurité (SOC). Ce document explore en profondeur les missions et fonctions, la structure organisationnelle, ainsi que le rôle central du SOC dans les organisations africaines, en mettant en lumière son impact sur la protection des infrastructures critiques et le maintien de la confiance numérique.

Ce livre blanc vise également à aider les organisations africaines à comprendre les enjeux spécifiques de la cybersécurité sur le continent et à mettre en place des SOC efficaces pour faire face à ces défis.

I. QU'EST-CE-QU'UN SOC ?

1. Définition du SOC

Un centre des opérations de sécurité (SOC) est une entité constituée d'un ensemble de processus, de technologies (SIEM, EDR...), et de personnes spécialisées ayant pour mission de surveiller, de détecter, d'analyser et de répondre aux incidents de sécurité dans l'infrastructure informatique d'une organisation. C'est en quelque sorte le système nerveux central de la cyberdéfense et du cyber-renseignement au sein d'une organisation, qui dans l'idéal opère 24 heures sur 24 pour la protéger contre les cybermenaces.

C'est le SOC qui collecte des données en temps réel à partir des réseaux, des serveurs, des terminaux et d'autres actifs numériques de l'organisation et utilise une automatisation intelligente pour identifier, hiérarchiser et répondre aux menaces potentielles en matière de cybersécurité.

1. Missions et fonctions d'un SOC

En fonction de l'organisation et du contexte, plusieurs types de missions peuvent être attribuées à l'entité SOC. Cependant, de façon générale, on peut identifier et énumérer cinq principales missions qui se démarquent et justifient l'existence-même d'un SOC au sein d'une organisation. Il s'agit notamment des missions suivantes:

- La surveillance (anticipation, protection)
- La détection de menaces (identification, classification, qualification, prioritisation)
- La réponse aux incidents (Investigation, isolation, éradication, restauration, notification.)
- La gestion des vulnérabilités
- Le renseignement sur les menaces.

Missions et Fonctions d'un SOC (suite)

Surveillance

Le SOC surveille en permanence les activités du réseau et des systèmes pour anticiper les menaces éventuelles. Il met en place des mécanismes de détection précoce et de protection proactive afin de prévenir les incidents de sécurité.

Détection de menaces

Le SOC identifie, classe, qualifie et priorise les menaces en analysant les indicateurs de compromission, les comportements suspects, les anomalies ou les schémas d'activité malveillante. Cette détection permet de réagir rapidement face aux incidents de sécurité et de minimiser leur impact.

Réponse aux incidents

En cas d'incident de sécurité, le SOC mène des investigations approfondies pour comprendre l'origine, l'étendue et les conséquences de l'attaque. Il isole les systèmes compromis, éradique les menaces, restaure les services affectés et notifie les parties prenantes concernées, tout en assurant une gestion efficace de crise.

Gestion des vulnérabilités

Le SOC identifie et évalue les vulnérabilités existantes dans les systèmes, les applications et les infrastructures. Il met en place des mesures de gestion des vulnérabilités, telles que des correctifs de sécurité et des actions préventives, pour réduire les risques potentiels d'exploitation de ces failles.

Renseignement sur les menaces

Le SOC collecte, analyse et partage des informations sur les menaces actuelles et émergentes. Il surveille les activités des acteurs malveillants et les tendances du paysage de la cybersécurité. Ces renseignements permettent de renforcer la posture de sécurité en anticipant les attaques potentielles et en prenant des mesures préventives adaptées.

2. Structure organisationnelle d'un SOC

En fonction de la taille de l'organisation et de ses moyens financiers, un SOC se doit d'avoir une organisation ponctuelle pour assurer son fonctionnement dans l'espace et dans le temps.
Pour une organisation standard, le SOC est constitué des ressources suivantes chacune dans son rôle spécifique :

Le responsable du SOC (SOC Manager)

C'est la principale personne chargée du bon fonctionnement du SOC au quotidien. Il supervise les opérations du SOC, notamment la dotation et la gestion du personnel, l'élaboration du budget de fonctionnement, ainsi que la planification stratégique. Le responsable SOC veille à ce que cet entité s'aligne sur la stratégie de sécurité globale de l'organisation. Il est le point de contact entre le SOC et les autres équipes de l'organisation, et s'assure que le SOC dispose de tous les moyens nécessaires pour remplir ses missions.

Service Delivery Manager (SDM)

Il est responsable de la supervision et de la gestion globale des services fournis par le SOC. Son rôle principal est de s'assurer que les services de sécurité sont fournis de manière efficace, en respectant les exigences du client ou de l'entreprise et les objectifs de niveau de service convenus.

> Les analystes SOC sont les défenseurs de première ligne qui surveillent les événements de sécurité, enquêtent sur les incidents et répondent aux alertes. Ils possèdent une expertise technique en matière de cybersécurité, de réponse aux incidents et de diverses technologies de sécurité.

L'Analyste SOC niveau 1

encore appelé analyste SIEM, il est responsable des premières actions de base dans les activités d'un SOC: surveillance, triage des événements, classification et qualification sur la base de différents critères, traitement des incidents mineurs ou relevant d'un mode opératoire documenté.

Les Analystes SOC de niveau 2 & 3

Plus expérimentés et techniquement plus avancés que ceux du niveau 1, les Analystes SOC de niveau 2 et 3 constituent l'équipe de réponse aux incidents. Ils réalisent aussi les actions de recherche et de renseignement sur les cybermenaces.

Ingénieur DevOps (maintenance et évolution de l'infrastructure)

Il assure la mise en place, la configuration et l'automatisation des outils de sécurité, en facilitant l'intégration continue et le déploiement continu, en gérant les infrastructures et les environnements, et en favorisant la collaboration interfonctionnelle.

Ingénieur DevSecOps (paramétrage et maintenance des solutions)

Il est responsable du paramétrage et de la maintenance des solutions techniques utilisées dans le SOC. Il veille à ce que les outils et les infrastructures nécessaires à la détection des menaces, à la gestion des incidents et à la sécurité globale du SOC soient correctement configurés, maintenus et mis à jour.

II. COMMENT SE PROCURER UN SOC ?

Sur le marché on distingue plusieurs options d'acquisition d'un SOC. Le choix d'un SOC dépend des besoins, du budget et des ressources humaines et matérielles de l'entreprise.

- **Construire un SOC interne**

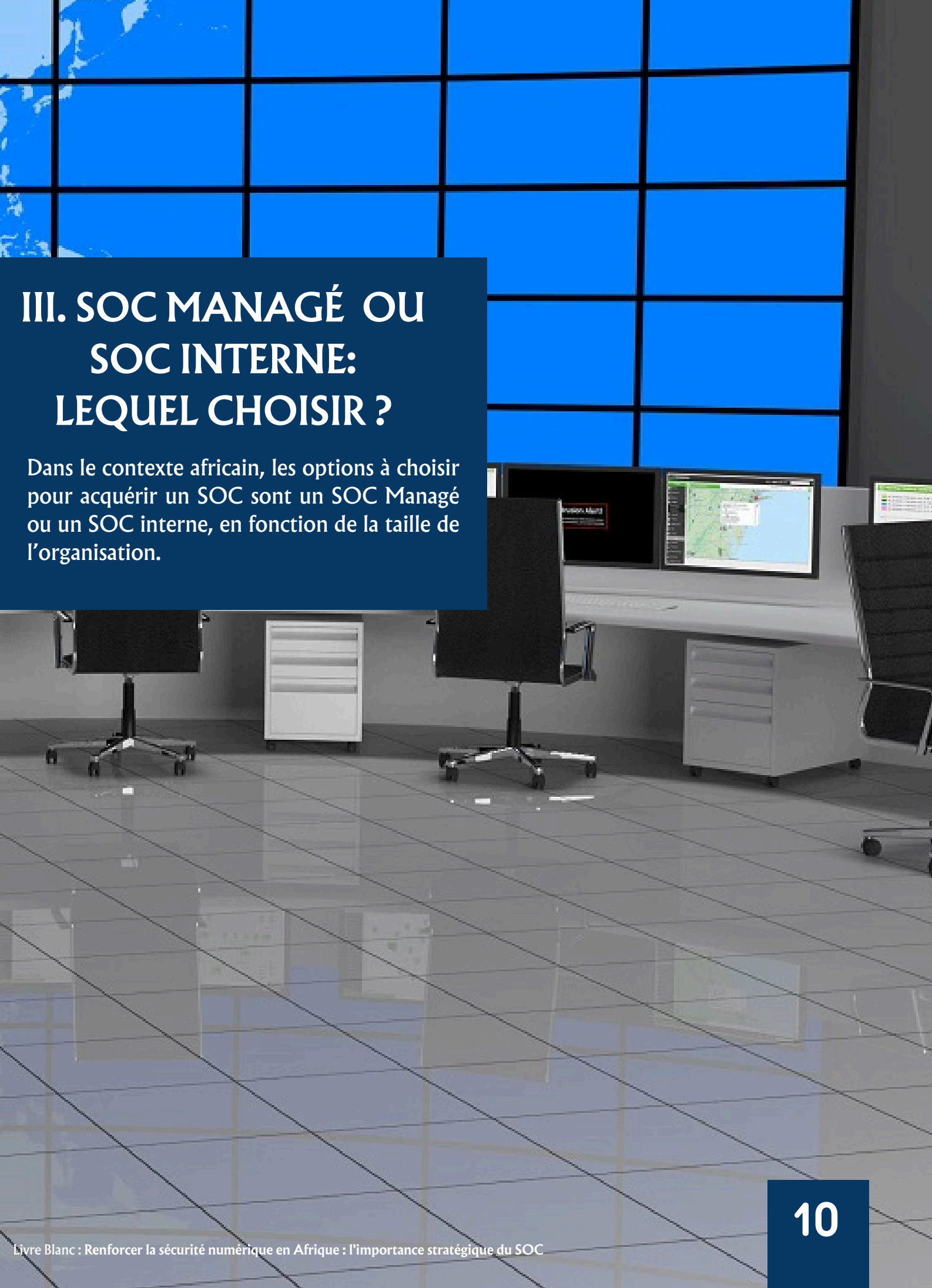
Cette approche consiste à mettre en place et à gérer un SOC au sein de l'organisation. Cela nécessite de recruter et de former une équipe spécialisée en sécurité, d'acquérir les outils et les technologies nécessaires, et de mettre en place les processus et les procédures de fonctionnement du SOC. Construire un SOC interne offre un contrôle total sur les opérations de sécurité, mais peut nécessiter des investissements importants en termes de temps, de ressources humaines et financières.

- **Externaliser le SOC à un prestataire de services**

Une autre option consiste à externaliser les opérations de sécurité à un prestataire de services spécialisé dans la gestion des SOC. Ces prestataires disposent de l'expertise, des ressources et des outils nécessaires pour surveiller les environnements informatiques, détecter les menaces et gérer les incidents de sécurité. L'externalisation du SOC peut offrir un accès à des compétences spécialisées sans nécessiter d'investissements initiaux importants, mais il est important de choisir un prestataire fiable et de s'assurer que les accords de niveau de service (SLA) répondent aux besoins de l'organisation.

- **SOC en tant que service (SOCaaS) :**

Cette approche est similaire à l'externalisation du SOC, mais elle est proposée sous forme de service cloud. Dans ce modèle, un fournisseur de services offre une plateforme de SOC entièrement gérée via le cloud. L'organisation souscrit à ce service et bénéficie d'une surveillance continue, de la détection des menaces et de la gestion des incidents, sans avoir à gérer l'infrastructure sous-jacente. Le SOCaaS peut offrir une flexibilité et une évolutivité accrues, tout en réduisant les coûts de mise en œuvre et de maintenance.



III. SOC MANAGÉ OU SOC INTERNE: LEQUEL CHOISIR ?

Dans le contexte africain, les options à choisir pour acquérir un SOC sont un SOC Managé ou un SOC interne, en fonction de la taille de l'organisation.

SOC Managé / Externalisé

SOC Interne

AVANTAGES

Expertise spécialisée, ce qui permet une détection et remédiation plus rapides	1	Contrôle total du SI
Évolutivité et flexibilité	2	Connaissance approfondie de l'environnement du SI
Accès à des technologies avancées	3	Adaptabilité aux besoins spécifiques de l'organisation
Réduction du coût total d'accès aux prestations d'un SOC	4	Confidentialité et contrôle des données
Mutualisation des ressources (humaines, méthodologiques et technologiques)	5	
Vision plus large sur les menaces	6	
Niveau de service garanti par le SLA	7	

INCONVENIENTS

Dépendance à un tiers

1 Coûts d'acquisition et d'exploitation élevés

2 Besoin de compétences spécialisées difficile à combler

3 Évolutivité limitée dans l'espace et dans le temps

4 Difficulté d'adaptation au paysage dynamique des menaces

Dans un contexte de pénurie de main d'œuvre qualifiée et de faible budget alloué à la cybersécurité, le SOCaaS est une vraie aubaine pour les organisations africaines. En comparaison à un SOC interne, cette option de service managé offre de nombreux avantages aux organisations.

SOC4AFRICA
BY ST DIGITAL & RHOPEN LABS

IV. NOTRE SOCaaS : SOC4AFRICA

Un Centre des Opérations de Cybersecurité (SOC) à la portée de toutes les organisations

Notre offre SOCaaS

Le SOC as a Service (SOCaaS) est un modèle de service de sécurité managé dans lequel un fournisseur tiers (comme SOC4AFRICA) déploie, exploite et maintient un SOC entièrement géré pour le compte des clients qui souscrivent à un abonnement.

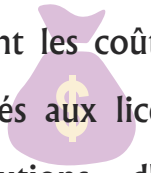
Le SOCaaS fournit toutes les fonctions de sécurité exécutées par un SOC traditionnel en interne, notamment : la surveillance du réseau, la gestion des journaux, la détection et le renseignement sur les menaces, l'investigation et la réponse aux incidents, la création de rapports, la gestion du risque et la conformité. Le fournisseur SOC assume également la responsabilité de l'ensemble du personnel, des processus et des technologies nécessaires à la mise en œuvre de ces services et à la fourniture d'une assistance 24 heures sur 24 et 7 jours sur 7 (selon la classe de service).

Notre approche Open Source

Le choix d'utiliser des solutions open source dans notre infrastructure SOC4AFRICA est d'échapper à la dépendance des éditeurs de solution SOC/SIEM dont aucun "major" n'est africain, contribuant ainsi à la souveraineté numérique des organisations sur le continent.

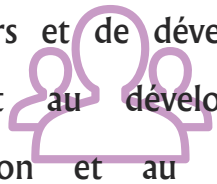
Les avantages d'utilisation des solutions Open Source :

Coût réduit



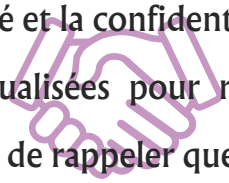
Les solutions open source étant libres d'accès, ce qui peut réduire considérablement les coûts d'acquisition bien souvent liés aux licences quand il s'agit de solutions d'éditeur. Cela représente un avantage significatif pour les clients dans un contexte de budget limité pour la cybersécurité comme c'est le cas en Afrique.

Communauté active et support



Les projets open source bénéficient souvent d'une communauté active d'utilisateurs et de développeurs qui contribuent au développement, à l'amélioration et au support des solutions garantissant une mise à jour régulière.

Transparence et contextualisation



Les solutions open source offrent une transparence totale sur le code source, permettant de comprendre et de vérifier le fonctionnement des outils utilisés dans le SOC. Cela offre une plus grande confiance dans la sécurité et la confidentialité des données. De plus, les solutions open source peuvent être contextualisées pour répondre aux besoins spécifiques d'un environnement. Il convient d'ailleurs de rappeler que la plupart des solutions dites d'éditeurs sont en fait basées sur des composants open source qui ont été contextualisés (par ajout de modules ou fonctionnalités spécifiques).

CONCLUSION

Un centre des opérations de sécurité (SOC) joue aujourd'hui un rôle essentiel dans la gestion des vulnérabilités, la détection des cybermenaces, ainsi que la réponse aux incidents de sécurité. Cependant, dans un contexte comme celui de l'Afrique caractérisé par des faibles budgets dédiés à la cybersécurité et une pénurie chronique d'experts qualifiés, mettre en place un SOC interne peut être périlleux et voir inaccessible pour certaines organisations.

Pour répondre à cette problématique, il est intéressant de constater que de nouveaux acteurs émergents qui proposent désormais sur le marché africain les prestations d'un SOC sous ses différentes modalités d'exploitation. C'est par exemple le cas de l'offre SOC4AFRICA issu du partenariat entre ST DIGITAL et RHOPEN LABS, un modèle inédit qui s'articule autour de deux propositions: le SOCaaS (service de sécurité managé) disponible par abonnement mensuel, et l'accompagnement des organisations africaines dans la construction de leur SOC interne en réduisant drastiquement le coût d'acquisition et le temps de mise en place.

Contact

DOUALA BONANJO

info@st.digital

contact@rhopenlabs.africa

(+237) 2 43 70 24 20 / 678 22 16 20