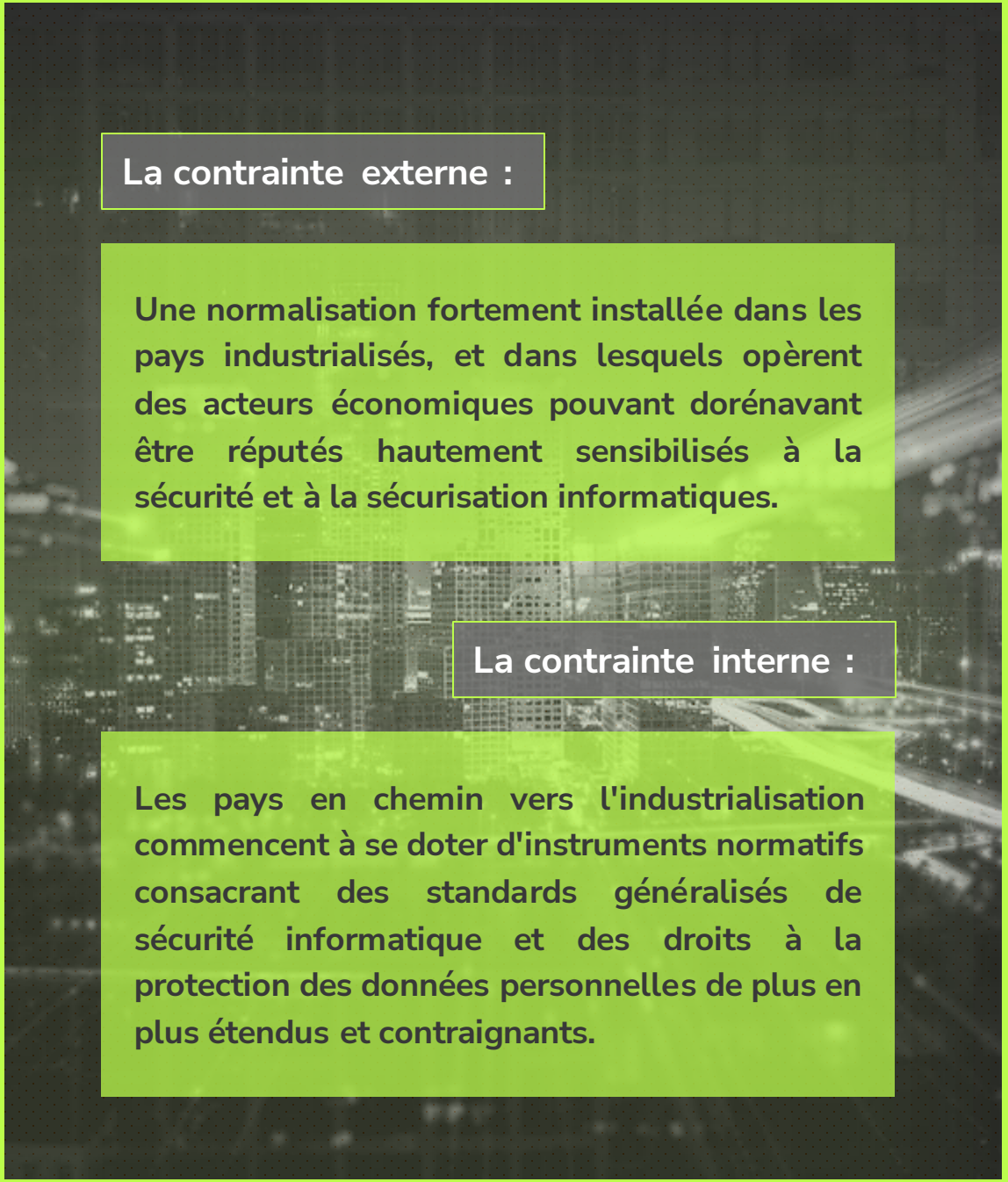
LockSchild

Votre expert cybersécurité et sécurité numérique sur le continent africain.

La SSI, un enjeu majeur de développement des opérateurs africains

La transformation digitale, désormais vecteur incontournable de croissance et de productivité des organisations, a placé la sécurité du système d'information au cœur des considérations stratégiques des opérateurs, et emporte avec elle **de nouvelles contraintes sur l'accès aux marchés** locaux, régionaux et internationaux.



La contrainte externe :

Une normalisation fortement installée dans les pays industrialisés, et dans lesquels opèrent des acteurs économiques pouvant dorénavant être réputés hautement sensibilisés à la sécurité et à la sécurisation informatiques.

La contrainte interne :

Les pays en chemin vers l'industrialisation commencent à se doter d'instruments normatifs consacrant des standards généralisés de sécurité informatique et des droits à la protection des données personnelles de plus en plus étendus et contraignants.

2017-2021: quelques chiffres sur la cybersécurité en Afrique

4.12 Mds €

Coût estimé des cybercrimes à l'échelle du Continent (2021)

237 M FCFA

Total des transferts frauduleux d'argent dans la BCAO

20.776 M FCFA

Retraits frauduleux au Sénégal via la duplication de 572 cartes BHS

Sources: PwC - Rapport d'enquête sur la cybersécurité en Afrique, Mars 2021

Interpol- Evaluation 2021 des cybermenaces en Afrique

Depuis 2017, nous accompagnons les opérateurs vers la sécurité et la résilience de leur SI.

Diagnostic et conseil

Evaluation d'exposition et plan d'action.

Audit

Audit technique et organisationnel.

Formation et sensibilisation

Fondamentaux et bonnes pratiques.

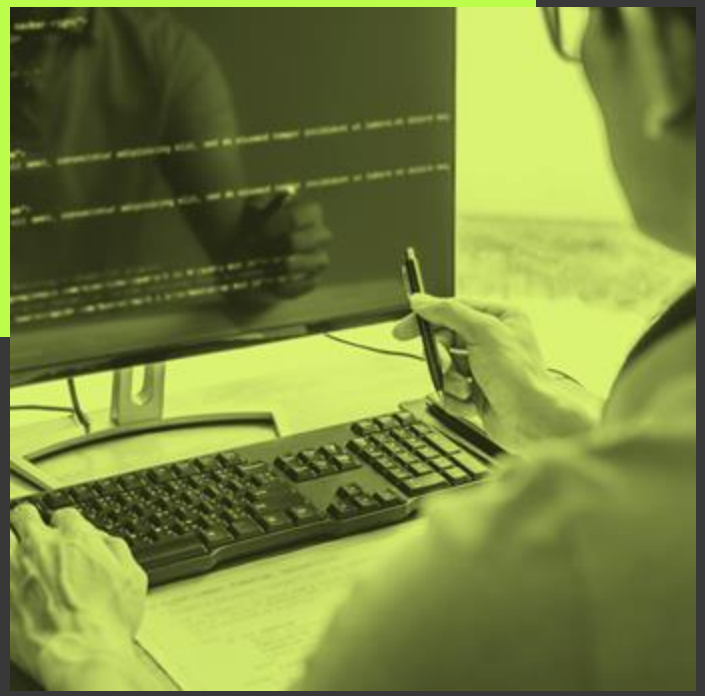
Zoom Audit

Audit d’architecture

L'objectif d'un audit d'architecture est de rechercher des faiblesses dans la conception, dans le choix des protocoles utilisés ou du non-respect de pratiques recommandées en termes de sécurité.

Nous nous basons sur une analyse documentaire et le résultat d’éventuels entretiens avec les personnes en charge de la conception, de la mise en œuvre, de l'administration, de la supervision et du maintien en condition opérationnelle du système d’information cible.

Audit de configuration



Nous réalisons des audits de configuration de différentes briques, tant logicielles que matérielles. Ces audits visent, d'une part, à prévenir la présence de faiblesses de configuration, qui pourraient à leur tour conduire à une diminution du niveau de sécurité, et, d'autre part, d'assurer que les configurations sont cohérentes avec l'architecture projetée.

Audit d'environnement de travail on-prem & remote

A partir de l'étude de la configuration d'un poste de travail, nous vérifions le durcissement de la configuration (selon les règles de l'état de l'art) et les failles éventuelles qui pourraient permettre à un agent malveillant d'obtenir des accès illégitimes.

Audit organisationnel et physique

Lors des audits organisationnels et physiques, Lockschild mène une analyse des politiques et procédures définies par votre organisation afin de vérifier leur conformité au regard des besoins de sécurité que vous exprimez, ou dans la définition desquels nous vous accompagnons, selon le cas.

Déroulement pratique des audits Lockschild

1

Initialisation

Définition du périmètre de l'audit et des modalités de son exécution

2

Réalisation

Déploiement des travaux techniques et/ou organisationnels

3

Restitution

Remise d'un rapport complet d'audit et présentation des recommandations

Le tout sur une application dédiée pour optimiser l'expérience client.

« Réaliser des audits de sécurité sur des périmètres ciblés permet aux organisations de **se prémunir** contre d'éventuelles vulnérabilités, de **connaître ses forces et faiblesses** mais surtout de **savoir se situer** dans la mise en œuvre de sa politique de sécurité. »

François-Xavier DJIMGOU, expert LockSchild, *in* « **Souveraineté numérique: un enjeu de taille pour l'Afrique** »

Zoom formation

Sensibilisation et compréhension des fondamentaux de la cybersécurité et de la sécurité numérique

Enjeux

Comprendre les enjeux de la cybersécurité en Afrique et dans le monde

Objectifs

Comprendre les principaux objectifs d'un dispositif de sécurité numérique

Notions fondamentales

Notions essentielles de cybersécurité (risque, menace, vulnérabilité, attaque)

Menaces

Examen du panorama des principales cybermenaces en Afrique et dans le monde

Zoom formation

Initiation aux *best practices*: mesures *de minimis* à appliquer tant au niveau de l'organisation que de l'individu

Analyser

Comprendre ce qu'est un risque numérique et l'appliquer à votre environnement.

Maîtriser

Maîtriser votre SI en identifiant les composants, terminaux, utilisateurs.

Gérer

Gestion des privilèges d'accès aux ressources du SI, prévention et réaction aux incidents de sécurité.

Une formation spécifique à vos besoins? Contactez-nous pour construire un programme individualisé!

Lockschild

La marque Lockschild est le fruit d'une vision globale de la cybersécurité, portée par le Groupe RHOPEN.

Implantés en France et au Cameroun, nos ingénieurs mettent en commun leur savoir-faire unique acquis de multiples horizons pour proposer une expertise contextualisée répondant aux plus hauts standards de l'industrie.

Notre équipe, le 360° de la sécurité

François-Xavier DJIMGOU

CEO RHOPEN LABS

Cybersecurity Expert, Strategy & Risk Mgmt

Patrick AZOGNI

CTO RHOPEN LABS

Cloud & Systems Security Architect

Paulin KAMHOUA

Managing Partner
RHOPEN GROUP

Data Security Expert

Keti MUSUMBU

Technical Advisor
RHOPEN GROUP

Infrastructure Security Architect

Ils nous font confiance

Business Services

Etablissements de crédit, de microfinance et de paiement :

LC-COB/04 : Quelles sont les nouvelles exigences de la COBAC à compter de 2022 ?

Consulter la LC-COB/04

Remise obligatoire de rapports d'audit à la COBAC

Il est dorénavant exigé des établissements financiers d'effectuer un audit indépendant, d'établir un diagnostic des vulnérabilités du SI, et de dresser un plan de remédiation

Prévention, renforcement et réactivité

Les établissements financiers doivent dorénavant mettre en place des mesures spécifiques de détection, de réponse et de rétablissement face au risque d'opérations non-autorisées et d'attaque touchant le SI.

Rehaussement de la SSI aux standards ISO

Enfin, les établissements concernés devront s'aligner sur les standards et bonnes pratiques internationaux, et notamment ISO/CEI 27001-02 et PCI-DSS.

Préparez votre mise en conformité au LC-COB/04 avec Lockschild

- Elaboration d’une politique globale de cybersécurité
- Politique de gestion des accès et des privilèges
- Evaluation des vulnérabilités du système d'information (test d'intrusion)
- Ségrégation des environnements du système d'information
- Point de mise en conformité PCI-DSS & ISO 27001 - 02

Contactez-nous

Afrique

(+237)6 90 16 36 27

contact@lockschild.africa

Station Nepture, Kotto Bloc
Douala, Cameroun

Europe

(+33)1 34 10 22 03

info@lockschild.fr

5, rue Marceline
95110 Sannois, France

RHOPEN
S.A.S. au capital de 35000€
RCS Pontoise n° 833 489 164
5, rue Marceline
95110 Sannois, France
Centre de formation agrée n° DDA 11 95 06337 95
Certification QUALIOPI n°199 0F Ind. 0
IDD: 0062443

RHOPEN LABS
S.A.S. au capital de 1.000.000 FCFA
RCCM du TPI de NDOKOTTI n° RC/DLN/2022/B/488
B.P. S/C 3768
Douala, Cameroun

LockSchild