CUSTOMER STORY

BANK OF AFRICA

“

L’outil contextualise automatiquement chaque alerte, prenant en compte l’ensemble de nos enjeux et priorités business, mais surtout élimine les faux positifs.

Yves KPANOU,
Responsable de la sécurité des systèmes d’information
Bank of Africa - PASS filiale tech de Bank of Africa

#BANQUE COMMERCIALE ET DE DÉTAIL #GESTION D’ACTIFS

#BANQUE D’INVESTISSEMENT #FINANCE #NDR

YVES KPANOU_

Responsable de la sécurité
des systèmes d'information
Bank Of Africa

*Enjeux cybersécurité_*

Centraliser
la visibilité d'un SI bancaire fragmenté et distribué sur 19 pays

Mutualiser
les capacités de détection et la gouvernance cyber à l'échelle de toutes les filiales

Prioriser
l'activité du SOC en réduisant le bruit d'alerte et en mettant en avant les signaux critiques

Accélérer
l'investigation et le confinement des incidents avant toute propagation réseau

Démontrer
la conformité, la traçabilité et la maîtrise du risque lors des audits réglementaires

01 QUELS ÉTAIENT LES PRINCIPAUX DÉFIS OU LACUNES IDENTIFIÉS DANS VOTRE STRATÉGIE DE DÉFENSE AVANT L'INTÉGRATION DU NDR ?

Avant de déployer une solution NDR, nous manquions de visibilité sur les menaces réelles au sein de notre réseau, au-delà des pares-feux en place. Cet angle mort dans notre stratégie de défense est devenu particulièrement préoccupant lorsqu'une tentative de ransomware a visé notre organisation. Nous avons alors rencontré des **difficultés significatives pour analyser l'incident en profondeur et fournir des informations précises et fiables à notre direction.** Ce manque de transparence et d'outils adaptés a souligné la nécessité de renforcer notre capacité de détection et d'analyse des menaces.

02 QUELS OBJECTIFS OPÉRATIONNELS OU CAS D'USAGE PRIORITAIRES AVIEZ-VOUS DÉFINIS POUR LE NDR LORS DE SON DÉPLOIEMENT ? VOYEZ-VOUS DE NOUVEAUX CAS D'USAGE ÉMERGER AUJOURD'HUI OU À MOYEN TERME ?

Avec une présence dans 19 pays en Afrique, un datacenter basé au Kenya et un SOC externalisé au Luxembourg, notre priorité était de **renforcer la visibilité sur l'ensemble de nos activités réseau, tant localement, qu'internationalement.** L'objectif était de **détecter rapidement et avec précision les menaces**, qu'elles soient internes ou externes, et de disposer d'un **outil centralisé capable de fournir des alertes claires et exploitables.** Nous souhaitions également pouvoir mieux **cartographier les interconnexions entre nos filiales.**

> ***« L'objectif était de détecter rapidement et avec précision les menaces, qu'elles soient internes ou externes, et de disposer d'un outil centralisé capable de fournir des alertes claires et exploitables. Nous souhaitions également pouvoir mieux cartographier les interconnexions entre nos filiales.***

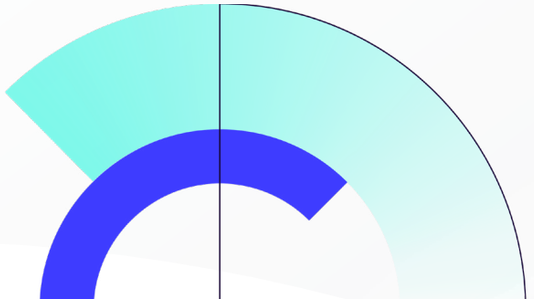
GATEWATCHER

03

FACE AUX IDÉES REÇUES SUR LE COÛT DU NDR EN MILIEU FRAGMENTÉ, COMMENT AVEZ-VOUS TRANSFORMÉ SON DÉPLOIEMENT EN LEVIER DE RATIONALISATION BUDGÉTAIRE ?

Dans un contexte où nos systèmes d'information sont répartis sur 19 filiales, la **mutualisation des coûts** et la **centralisation de la gestion de la cybersécurité** ont été des arguments décisifs pour surmonter les réticences initiales. Après la tentative de ransomware dans une de nos filiales, nous avons particulièrement pris conscience de la **nécessité d'un NDR**. À l'époque, nous n'avions pas les moyens techniques de fournir à notre direction un reporting détaillé et adapté, ce qui a compliqué notre capacité à expliquer la situation et à rassurer les autres filiales.

Lors du processus de sélection, **l'ensemble des responsables sécurité de nos filiales s'est unanimement prononcé en faveur de la solution Gatewatcher.** Cette décision reflétait non seulement l'adéquation de ses fonctionnalités avec nos besoins, mais aussi sa capacité à répondre à nos attentes stratégiques, notamment en matière de visibilité globale et de reporting précis. Aujourd'hui, ce choix nous permet de fournir des analyses fiables et exploitables à la direction, renforçant ainsi la confiance et la transparence au sein de l'organisation.



> *Cette décision reflétait non seulement l'adéquation de ses fonctionnalités avec nos besoins, mais aussi sa capacité à répondre à nos attentes stratégiques, notamment en matière de visibilité globale et de reporting précis.*

04

COMMENT S'EST DÉROULÉ LE PROCESSUS DE DÉPLOIEMENT ET D'INTÉGRATION DU NDR DANS VOTRE ARCHITECTURE EXISTANTE ET COMMENT CETTE SOLUTION S'EST-ELLE ALIGNÉE SUR VOS POLITIQUES DE SÉCURITÉ (PSSI) ET VOS OBJECTIFS STRATÉGIQUES ?

L'intégration du NDR dans notre architecture s'est faite en pleine cohérence avec notre PSSI, où il vient **renforcer de manière significative la détection des menaces.** Combiné à nos solutions EDR et SIEM, il nous offre une couverture complète des techniques et tactiques du framework MITRE ATT&CK®. Le déploiement, bien que globalement fluide, a nécessité quelques ajustements techniques, notamment pour optimiser le trafic sur nos réseaux satellites à faible débit et réduire les alertes non-pertinentes grâce à des paramétrages adaptés. Ces efforts ont permis une intégration harmonieuse avec nos objectifs stratégiques.

SIÈGE SOCIAL
Casablanca, MAROC

SECTEUR D'ACTIVITÉ
> Banque commerciale et de détail
> Banque d'investissement et corporate
> Crédit à la consommation et crédit immobilier
> Gestion d'actifs et services spécialisés (leasing, factoring, assurance)
> Services digitaux (e-banking, solutions de paiement, etc.)

+7000 COLLABORATEURS

PÉRIMÈTRE SURVEILLÉ
19 pays, supervision locale et cadre de conformité groupe

PARC INFORMATIQUE
IT digitalisé + SOC et cybersécurité avancée

PRODUIT NET BANCAIRE
2 milliards de dollars le 31/12/2025

05 DANS UN ENVIRONNEMENT OÙ DES SOLUTIONS DE SÉCURITÉ COEXISTENT SOUVENT, COMMENT LE NDR S'EST-IL INTÉGRÉ À VOTRE ARSENAL EXISTANT ? QUELS BÉNÉFICES SPÉCIFIQUES AVEZ-VOUS CONSTATÉS EN TERMES D'INTEROPÉRABILITÉ OU DE COMPLÉMENTARITÉ AVEC VOS OUTILS ACTUELS (SIEM, EDR, FIREWALLS, ETC.) ?

Le NDR s'est intégré de manière fluide avec notre arsenal existant, notamment grâce à sa **compatibilité** native avec notre SIEM IBM. Nous exploitons également la capacité de réponse de la plateforme de NDR de Gatewatcher. **Cette interopérabilité renforce l'efficacité de notre système de défense et améliore notre capacité de réponse, particulièrement en dehors des horaires de bureau.** Cela nous donne une vue unifiée et cohérente des menaces, tout en maximisant la complémentarité de nos outils.

06 QUELLES TYPOLOGIES DE MENACES MAJEURES AVEZ-VOUS PU MIEUX APPRÉHENDER GRÂCE AU NDR ?

Un incident récent a démontré l'efficacité du NDR. Lors de la mise à jour d'une application dans notre datacenter, un sous-traitant a accidentellement connecté un ordinateur portable équipé d'une clé USB compromise. Grâce au NDR, une alerte critique a été immédiatement générée, nous permettant **d'isoler rapidement la machine infectée.** Plus important encore, l'outil a permis **d'analyser l'ensemble de la chaîne de propagation** et de **neutraliser complètement le malware** avant qu'il ne puisse se propager au reste du réseau. Sans cette solution, l'incident aurait pu avoir des conséquences beaucoup plus graves, avec un risque de propagation globale. Grâce à l'IA agentique, Gatewatcher développe depuis de nombreux mois de nouvelles capacités intelligentes pour le NDR. Ainsi nous avons désormais **un véritable outil d'aide à la décision, permettant à nos équipes SOC de gagner un temps inimaginable dans leurs actions de remédiation.** L'outil **contextualise automatiquement chaque alerte,** prenant en compte l'ensemble de nos enjeux et priorités business, mais surtout **élimine les faux positifs. L'humain est donc focalisé sur la réponse aux tentatives d'intrusion en total control car il a à sa disposition toutes les explications nécessaires très simplement.** Nos équipes ne naviguent plus entre les outils et gagnent ainsi en maîtrise et rapidité opérationnelle améliorant quotidiennement notre efficacité.

Les bénéfices **NDR_**

Visibilité complète et centralisée
sur l'ensemble du réseau, local et international, même dans des environnements fragmentés

Détection proactive
des menaces internes et externes, enrichie par l'IA pour anticiper les mouvements latéraux

Aide à la décision renforcée
qui permet au SOC et à la direction de se concentrer sur ce qui compte vraiment, en distinguant urgence, impact et nécessité d'action

Intégration fluide avec l'écosystème existant
interopérabilité avec SIEM, EDR, pare-feux et autres outils de sécurité

Cloisonnement par filiale et supervision unifiée
harmonisation des pratiques de sécurité et contrôle centralisé des activités réseau

Réduction du MTTD et du MTTR
grâce à l'automatisation

Mise en conformité simplifiée
sans impact sur la performance opérationnelle

*À PROPOS_*

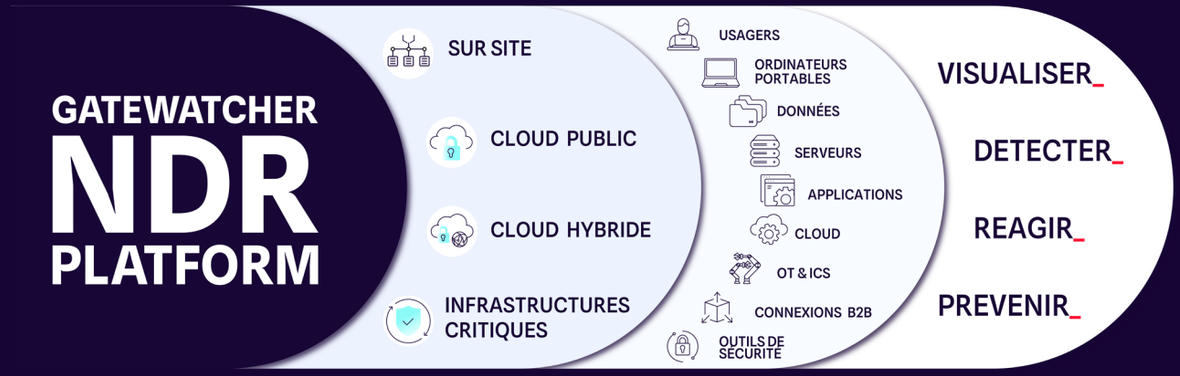
Leader de la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux des entreprises et des institutions publiques, y compris les plus critiques. Grâce à l'association de l'intelligence artificielle et de techniques d'analyse dynamiques, sa plateforme NDR offre une visibilité avancée et contextualisée sur l'ensemble des activités réseau, dans le cloud et on-premise.

Au-delà de la détection, Gatewatcher étend les capacités des SOC avec son Decision Center, une plateforme de Cyber Decision Intelligence qui transforme les signaux de sécurité en décisions exploitables, gouvernées et traçables. En consolidant les données issues de multiples sources (réseau, endpoint, cloud, identité), Gatewatcher permet aux équipes sécurité d'accélérer la prise de décision, de réduire le temps de réponse et de gagner en efficacité opérationnelle.

Compatible IT, OT et IoT, la solution sécurise l'ensemble des actifs critiques tout en simplifiant les opérations. Gatewatcher allie performance technologique et impact métier.

Gatewatcher est reconnue comme Visionary dans le 2025 Gartner® Magic Quadrant™ for Network Detection and Response (NDR).

Contactez-nous



Envie d'en *savoir plus ?_*

[PODCAST]
Au cœur de la finance publique : quand la cybersécurité soutient l'économie

[USE CASE]
SOC entreprise : Décision automatisée à l'échelle

[ARTICLE]
Le prochain NDR sera autonome, copilote du SOC de demain