# Refocusing cybersecurity in Nigerian Banks



"Banking in a secured cyberspace"

**Cybercrime is by far the greatest potential threat banks face today with an estimated 0.08% of Nigeria's GDP at stake to cyber-attacks according to the office of the National Security Adviser. BlackSentry Insights investigates the benefits of its cybersecurity solutions to Nigerian banks.**

## The Challenges

While money is an obvious enticement, cybercriminals also look to steal or compromise valuable customer data held by banks. The current reality is that cyber criminals are not time bound nor discriminatory sometimes leveraging off-peak and non-business hours to perpetuate their activities. A greater risk often overlooked is the possibility of exposure that extends to a bank's partners and external parties. Worthy of note is the existence of internal threats arising from staff with criminal intent or uninformed staff that succumb to malicious sites and traditional phishing techniques.
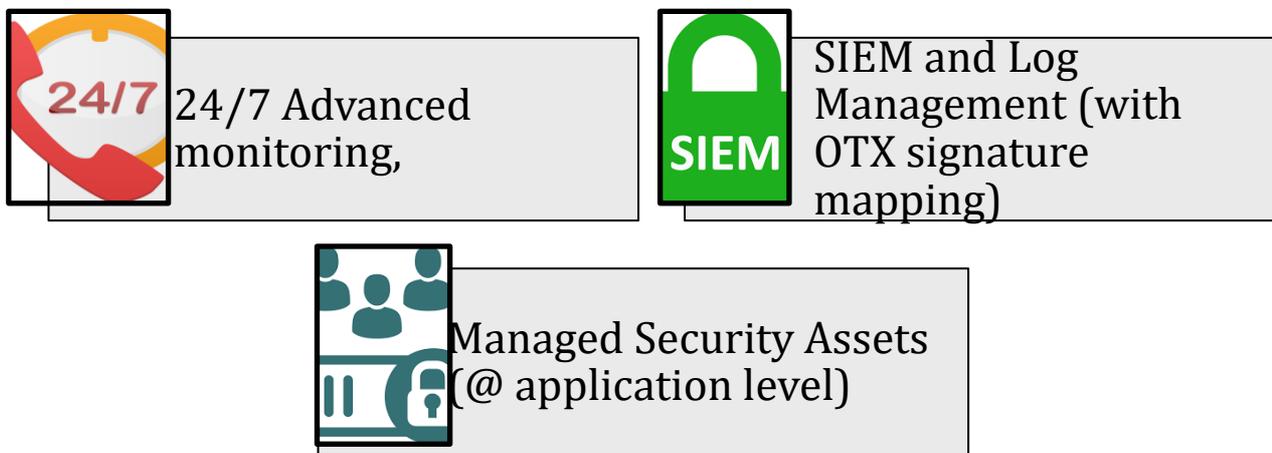
## CASE STUDY: From SIEM to Security Intelligence

A high profile bank in Nigeria invested in a SIEM solution to help manage threat but soon after realized that it lacked the necessary analytics and risk-monitoring capabilities for detecting insider and advanced external attacks. Furthermore, the bank's Chief Information Security Officer (CISO) had a serious blind spot over his key business applications and systems that were the very target of threats.

Faced with the prospect of building out its own analytical capabilities on top of the SIEM solution, the bank opted for our "security intelligence" layer by outsourcing to BlackSentry Managed Security Service. This new solution leveraged the existing SIEM for data collection and mapped it against our Open Source Threat Exchange (OTX) in addition to advanced detection and 24/7 monitoring capabilities that the bank desperately needed beyond the network perimeter to critical applications and users.

## Specific Solution

Research by BlackSentry *Insights* found great opportunities in Banks taking advantage of three key service offerings which are;

 24/7 Advanced monitoring,

 SIEM and Log Management (with OTX signature mapping)

 Managed Security Assets (@ application level)

All of these will be managed from our Security Operations Centre which is available 24/7

### S1: 24/7 Threat Monitoring & Cyber-Attack Defense

    I.     Advanced monitoring and investigation service available 24x7x365.

    II.    Analysis against malicious code to prevent security breaches to the bank's facility or environment.

    III.   With our service banks will adopt a proactive approach to security management of their environment

    IV.   Production of alerts, activities and reports for both security awareness and compliance purposes.

### S2: SIEM & Log Management (with OTX mapping)

    I.     Increased efficiency by collating event log and improved reporting processes across the business

    II.    Preventing potential security breaches

    III.   Reducing the impact of security events with the capability of analytics

    IV.   Added advantage of our OTX with a database growth of 10 million signatures daily.

## S3: Managed Security Assets (at application level)

I.  Our turnkey solutions will cover numerous mundane task allowing your team focus on high priority issues

II.  Banks will leverage our technological infrastructure rather than having to invest in more tools thus reducing capital cost.

III.  Banks will prevent insider threats such as access to a malicious site harboring malware or phishing tools.

IV.  Our comprehensive solution ensures your regulatory requirements are maintained



## Business Benefits

❖ The peace of mind that your assets are being monitored 24/7 with analysis and investigation of malicious code.

❖ Banks will benefit from our global OTX to identify attacks from known malicious sources that continuously attack the bank's environment. The OTX has participants across 140 countries who contribute over 10 million threat indicators daily.

❖ Our managed solution ensures you have a fixed cost irrespective of your security activity or capability needs thus facilitating budgeting and financial forecast.

❖ Your bank has the comfort of reduced risk of sensitive data theft and a proactive approach to data breaches prevention.

❖ The expertise and value we bring is comprehensive, freeing your Bank's Security Team of mundane chores allowing them focus on high risk tasks.

The capability our advanced cybersecurity solutions bring to Banks is more than asset surveillance or managed firewall, rather it's a new way of managing a core business risk to include digital forensics, analysis and structured incident management.

## Why BlackSentry?

For years as Layer3, we have been at the forefront of our customers' technology implementing solutions that have completely transformed the way they do business. Through BlackSentry we aim to continue to work with our customers, providing new and innovative solutions that will create value out of their data and securing their most critical data and network assets.

BLACKSENTRY is the Data Analytics and Cybersecurity division of Layer3 delivering a set of world class products and services within the African market. We are made up of a specialized team of experts with proven industry experience, a world-class 24/7 operations center and an experienced management team. We have an unwavering passion for service excellence, innovation and commitment to our customers' business success.

**Abuja Office**

5th Floor, IGI House Zone 4, Wuse Abuja

+234 0 7000 LAYER3 (+234 0 7000 529375)

enquiry@blacksentry.ng   www.blacksentry.ng

**Lagos Office**

198B, Jide Oki Street Victoria Island Lagos

# BLACKSENTRY

A division of LAYER3