International Journal of Functional Research in Arts & Humanities
Volume 4; Issue 4; December 2025; Page No. 27-37.

ENHANCING CYBERSECURITY IN ANAMBRA STATE, NIGERIA, THROUGH A NOVEL FRAMEWORK FOR DETECTING INSIDER THREATS IN SMALL AND MEDIUM ENTERPRISES USING MACHINE LEARNING

[1] **Victoria Okoma**

[1] Federal Polytechnic Oko, Anambra State, Nigeria

Abstract

White collar criminals are a serious security issue to the organization of cybersecurity, especially in small and medium enterprise (SME) where funds to build advanced defenses are unavailable. The paper will build a new machine learning model to be used to identify insider threats in SMEs in Anambra State, Nigeria, and deal with the most common trends like the inappropriate access to data and suspicious user activities. The main idea is to detect the patterns of the threats with the help of the empirical data, create a diagnosis model based on ML along with the application of the Random Forest algorithm, analyze the model with the help of the real-life examples, and recommend scaling solutions to further deploy it on a larger scale to Nigeria. The study is a mixed-method study, undertaken in commercial centers such as Onitsha, Nnewi and Awka. This study will use 50 SMEs as the target population and stratified random sampling will employ sampling proportions of 50 out of the target population of 50 SMEs. Structured questionnaires of 250 employees and 60 managers, semi structured interviews with 25 owners and anonymized system logs are to be used as primary data collection. Random Forest model, which was trained on features such as the frequency of the logging in as well as access to files, was able to validate at 88% and 90 percent. The demographics will show that the background of the participants is mainly male (65%), 25-45 (70%), secondary education (55%) as the workforce in the SME sector in Anambra. The qualitative data provide such contextual variables as insufficient cybersecurity awareness and financial limitations contributing to the threat. The framework provides a lightweight and cheap tool that can use minuscule resources to facilitate cybersecurity efforts in environments that are resource constrained which helps in building resilience to cybersecurity in constrained environments. This study, offering behavioral analytics with local data-driven data, helps to bridge the gaps in the context-specific studies facilitating the policy recommendations on the improved SME protections and the national cybersecurity approaches.

Keywords: Insider Threats, Machine Learning, Random Forest, SMEs, Cybersecurity Framework, Anomaly Detection

Introduction

Cybersecurity has now become one of the key fields in the field of computer science, and the field includes safeguarding information systems against unauthorized access, interference, or destruction. Within the framework of emerging economies such as Nigeria, where digital change is taking place at a rapid rate, Hispanics are particularly vulnerable because they lack the funds and professional skills to do so. The case of Anambra State, a commercial giant in southeastern Nigeria, is illustrative of this problem, whereby its SMEs in other economic sectors like manufacturing and retailing are simultaneously becoming more dependent on digital solutions and still face risks of insider attacks malicious or lax behaviors by internal agents that undermine security. This paper presents a new technology based on machine learning (ML) that is expected to improve cybersecurity resilience in such businesses, as a new framework that would be able to identify these threats.

Insider threats are as old as the literature on cybersecurity, with initial discussions placing significant focus on human aspects of vulnerabilities of the systems. As an example, the insider problem was identified by Anderson (1980) in his landmark paper on computer security threats because insiders escaping perimeter security was easier than attacks by external parties. The scholars who developed this view in the 1990s, such as Wood (1999), categorized insider threats based on case studies and applied the categories of sabotage, theft, and fraud to the cases and observations. The first categories developed formed the basis of the interpretation of the motivation such as financial profit or outrage and are still applicable today. By the early 2000s, detection mechanisms became the focus of research, with Cappelli et al. (2009) comparing more than 200 insider attacks after reviewing the CERT Insider Threat Database, finding such patterns as the growing privileges and data leaving before the actual attack.

Modern literature incorporates cutting-edge computational methods (mostly ML) to deal with such threats dynamically. Recent reviews, including that of Al-Mhiqani et al. (2020), have reviewed the ML applications in insider threat detection, and the authors have highlighted the effectiveness of supervised algorithms in identifying abnormal behaviors. Gamachchi and Boztas (2017) study offers graph-based ML models to conduct user behavior analytics in resource-limited conditions, with a high detection rate and low false positive rates. In the case of SMEs, in particular, ENISA (2020) documents that 77 percent of the data breaches are insider-related, which is why affordable solutions are in demand. The issue of infrastructural inadequacy and lack of awareness is one of the factors that exacerbate cybersecurity issues in Nigeria, as indicated by Osho and Onoja (2015), who reported the effects of cybercrime on a business and how SMEs are impacted unequally by it, given the inappropriate in relation to this sector.

The economic environment of Anambra State, with a vibrant market in both Onitsha and Nnewi is a strong motivator to invest in SMEs which contribute more than 40 percent of the GDP of the state and provide 70 percent of employees (Nwanmuoh et al., 2024). But here, insider threats tend to come in the form of situational influences such as financial sufferings resulting in ways of sharing unauthorized data to benefit self-interests. The socio-technical techniques of technical monitoring and organizational psychology are proposed by older studies like the ones by Probst et al. (2010) in their book on insider threats in cybersecurity. Combining this and with the recent developments, Yuan et al. (2023) show the Random Forest ensembles to detect anomalies, which are 15-20 times more accurate than the classic approaches.

Theoretical grounds are based on the General Deterrence Theory (Straub and Welke, 1998) that assumes that the subjective probability of detection will decrease the motivation toward malicious actions, and the User and Entity Behavior Analytics (UEBA) scheme (Gartner, 2015) based on the ML to normalize regular activities. This paper proceeds with those, by adapting a model to the

SMEs in Anambra, where there is an uneven adoption of digital, according to Dioha (2022), noting that only 30% of the sample companies have basic security controls in place in response to polling on the use of ICT by Nigerian companies.

Global statistics on insider threats in SMEs indicate they occur at a high rate where, according to Verizon (2023 Data Breach Investigations Report), the percentage of breaches caused by insiders is 19; this number is, presumably, even larger in less developed countries because of weaker protection. The Nigerian Commission of Communication (2021) in Nigeria registers over 500 million losses annually due to cyber-attacks, with the SMEs as a substantial part of them. Early detection models such as the anomaly-based systems of Magklaras and Furnell (2002) were based on rule-of-thumb and although newer ML models, such as those assembled in Liu et al. (2018), can be applied to sequential pattern recognition, it is frequently computationally intensive to SMEs.

This framework fills these gaps with the use of lightweight ML, which is the Random Forest, which is well-known to be robust in unequal datasets which is typical in threat detection (Breiman, 2001). Its extrapolation as realized in real-time monitoring has been recently confirmed by recent applications, including those by Tuor et al. (2017) at Oak Ridge National Laboratory. Mthunzi et al. (2020) emphasize African cultural peculiarities affecting the threats and recommend localized models. The lack of skilled employees poses a threat to Anambra due to its demographic, where the proportion of young people (median age 28) and a high degree of entrepreneurship exists (National Bureau of Statistics, 2022).

Following this introduction is the concept of integrating the old literature with the new, which places the research into a historical context: the recognition of human vulnerabilities, as Anderson (1980) has done, and the most recent approaches in search of solutions to the problem, such as the hybrid models offered by Chattopadhyay et al. (2022), who suggest predicting insiders using models. The goals to find patterns, develop an ML model, test its efficacy, and offer scalable solutions are consistent with the National Cybersecurity Policy (2021) in Nigeria that focuses on SMEs protection.

Increased threat patterns Expanding threat patterns, the classic literature references Parker (1983) in Fighting Computer Crime, which characterized sabotage and espionage, and the recent meta-analyses by Costa et al. (2021) which defined both recent threats as negligent (such as vulnerability to phishing), with others as malicious (such as IP theft). With blurred roles in the SMEs, it is difficult to spot the detection hence the use of features importance of the ML tool in the random forest can reveal important pointers such as atypical login times (Ho et al., 2018).

Specific to the country of Nigeria, research indicates that cyber incidents have been on the increase in the southeast region and this has been attributed to economic disparities (Adedoyin et al., 2019). Anambra has 5 million residents and SME density (1,504 registered in major industries) which makes it an area that has to be filled with specific interventions (State of States, 2023). The research is important to the extent that it offers empirical evidence of local SMEs, allowing the theoretical frameworks of SMEs to be aligned with their practice.

Methodology

The research design will be to develop and test the ML structure methodically and use mixed methods research design to address the needs of capturing quantitatively measured as well as qualitative data. The research is located in the Anambra state with a target of SMEs within the Onitsha, Nnewi and Awka areas being chosen due to their commercial relevance and the representation of a variety of sectors. These places represent more than 60 percent of SME activity in the state, where Onitsha is the trade location, Nnewi is the manufacturing site, and Awka is the service site (Nwanmuoh et al., 2024).

Research design refers to the sequential explanatory approach, according to which quantitative data will inform the development of the model, followed by their qualitative validation (Creswell and Plano Clark, 2017). This enables triangulation thus improving reliability. The conceptual framework incorporates UEBA and Insider Threat Kill Chain (Cole and Ring, 2005), conceptualizes threat as a multi-stage process in form of reconnaissance to exfiltration that can be detected by analyzing ML anomalies.

The sample size involves employees and managers of 50 SMEs, who are stratified randomly to be proportionate to sectors, 20 retail, 15 manufacturing, 15 services. It is estimated that there are 350,000 SME workers in the state of Anambra (SADI Journal, 2023). It has samples of 250 employees, 60 managers and 25 owners which are calculated using the Yamane formula of finite populations at 95 percent confidences.

The demographics of participants in the study represent the workforce in Anambra: 65 per cent of females and 35 per cent of males; age breakdown 20 per cent below 25, 70 per cent between 25-45, 10 per cent above 45; education level 20 per cent primary level, 55 per cent secondary level, and 25 per cent tertiary level; occupations are practical according to the sectors, 40 per cent are in sales and 30 per cent in production with 30 The FCs are most ethnically Igbo (95 percent) and the average tenure is 4 years (SD=2.5), with a monthly earnings ranging between N50,000-N150,000 (National Bureau of Statistics, 2022).

The gathering of primary data is complex. The threat behaviors are measured through quantitative data with the use of structured questionnaires, where a Likert-scale is applied to such items as frequency of unauthorized access (Cronbachs alpha=0.87). Given face-to-face to reduce bias with results of 310 responses (response rate 95%). The logs on the system of 30 agreeing SMEs record 100,000+ entries on login, file and transfers within three months. Semi-structured interviews provide qualitative data that address contextual aspects that have been transcribed and coded into themes.

Python Data analysis Data analysis will be performed with ML supervised using Random Forest (scikit-learn) (Pedregosa et al., 2011). These are login frequency, access pattern, volume of transfers; labels based on simulated threats and the comments of the experts. Split of dataset: 70/ 30 training/ testing. Measures: accuracy, recall, precision, F1-score. Thematic coding is applied in NVivo in qualitative analysis.

The ethical procedures are informed consent, anonymity, and IRB approval at Anambra State University. This allows privacy especially those related to sensitive logs.

Development of the framework is based on feature engineering, grid search hyper-parameter optimization, and cross-validation to avoid overfitting. It is anticipated that the results would be an 85 percent-plus accurate model, which would work in SME on low-end hardware.

Results

The confined rates of insider threats according to the quantitative data of the questionsnaires indicate common insider threats patterns: 45% were those employees who observed unauthorized data sharing, 30% reported suspicious logins and 25 percent observed attempts of file exfiltration. The economic motivations (60%), and lack of training (50%) were pointed out by the managers as the main drivers. It recorded system logs with average logins/user daily of 5.2 (SD=2.1), and uncharacteristic results of 15 percent of the sessions being above baselines.

Table 1

Demographic characteristics.

Characteristic	Frequency (n=335)	Percentage (%)
Gender: Male	218	65
Gender: Female	117	35
Age: <25	67	20
Age: 25-45	234	70

Age: >45	34	10
Education: Primary	67	20
Education: Secondary	184	55
Education: Tertiary	84	25
Sector: Retail	134	40
Sector: Manufacturing	100	30
Sector: Services	101	30
Income (N/month): <50,000	100	30
Income: 50,000-100,000	168	50
Income: >100,000	67	20

The Random Forest model, which was trained using 70,000 logs, had accuracy, precision, recall and F1-score of 88, 85 and 90, and 87 respectively. The top rankings on the feature importance feature were obtained on login frequency (0.25), file access (0.22), and transfer volume (0.18).

Table 2

Model Performance Metrics.

Metric	Value (%)
Accuracy	88
Precision	85
Recall	90
F1-Score	87
AUC-ROC	92

Qualitative aspects are "workplace dissatisfaction" (said by 80% of the owners) and resource constraints (70%), which are associated with quantitative anomalies ($r=0.42$, $p<0.01$).
Use in 10 pilot SMEs lowered the number of incidents detected by 35 and false positives were 5.

Discussion

The discussion of the results obtained in this research gives strong grounds to the effectiveness of the described machine leaning system based on the Classification Forest in insider threat detection of small and medium enterprises (SMEs) in Anambra State, Nigeria. With a 88% accuracy, 85% precision and recall of 90 percent and F1-score of 87 the model has shown high performance in substrating the results on the basis of flagging abnormal behaviors using the features of login

frequency, patterns of file accesses and volumes of data transfers. Other metrics are quite consistent with the latest findings in insider threat detection where Random Forest algorithms have continued to report good outcomes when dealing with unbalanced datasets, which is characteristic of cybersecurity deployment (Sharma et al., 2025). The high recall rate, in especially, is essential to reduce cases of costly falses in insider threats, wherein anomalies remained undetected may result in profound data theft or sabotage, and inadequate cybersecurity knowledge and attitude (refer to the larger scale location into malicious insider threats) make a person vulnerable in developing economies (Deloitte Nigeria, 2025). The socio-economic aspect of the SME labor in Anambra is evidenced by demographic correlations of lower education levels with a high level of negligence ($r = -0.35$) and the lack of higher education as well as primary, secondary education with the majority of the SME workforce (70% of their ages are 25-45). This is similar to findings on African SMEs, in which insufficient resources and skillset limit the mitigation of the threats (Mugwagwa et al., 2024). These threats are further contextualized by qualitative themes of workplace dissatisfaction and resource constraints in accordance with the reports on the world that insider-related cases are usually a result of the irresponsible or discontented employee instead of those who are completely malicious (Ponemon Institute, 2025).

The performance of the framework to a large extent is better than most of the conventional rule based systems which fail to cope with the change in threats within the constraints of limited resources. Recent comparative studies prove the superiority of Random Forest over such alternatives as SVM or Isolation Forest in data protection scenarios, especially with the addition of feature selection methods (Sharma et al., 2025). To improve the level of theoretical alignment with more established frameworks such as the Insider Threat Kill Chain (Cole and Ring, 2005), the framework will be enhanced with the concept of User and Entity Behavior Analytics (UEBA), which means its light weight design ensures that it can be practically applied even in the case of SMEs characterized by limited computational capacities because of budget limitations (Onatuyeh et al., 2025). The strategy is ideal in detecting stages of the threat process, reconnaissance to exfiltration, and provides a way of baselining normal behaviors that detect deviations. This is especially applicable in the SMEs where the fact that some of the roles overlap erases any distinct role, and hence UEBA becomes essential in monitoring everything holistically (Securonix, 2024). The application of the model in practice is confirmed by pilot deployment with a reduction in incidents by 35 per cent and low false positives (5%), which is supported by behavioural analytics implementations highlighting the importance of constant learning to implement adaptive detection (Splunk, 2025).

But, restraints need to be realized. The fact that self-reported questionnaire data will be used can be associated with some response bias, whereas the data can be restricted to 30 SMEs to create system logs, which can limit the generalizability. Dependencies in networks when collecting data

may also impact scalability in places that do not have reliable connectivity, which is one of the most frequent problems in Nigeria (National Bureau of Statistics, 2022). Moreover, a labeled nature of the anomaly in the model presupposes the labelled anomalies that might not reflect the new threats when the model is not retrained. These problems are noted recently, where gaps in the datasets and the complexity of the models are identified as obstacles in real-world use (Alzaabi and Mehmood, 2024).

Nevertheless, without these, the framework will enhance context-driven cybersecurity research in Nigeria, which will address gaps in regional studies where SMEs incur final cyber losses in the wake of digital transformation (Deloitte Nigeria, 2025). There is inclusivity through its use of local data and accessibility of cheap tools such as scikit-learn, unlike global solutions which are usually configured to larger businesses. The value of mixed methods can be established with correlations between qualitative data and quantitative anomalies ($r = 0.42$), which prove useful to consider the contextual nuances, including cultural factors affecting threats in the African context (Mthunzi et al., 2020).New techniques, including federated learning as a privacy-preserving multi-SME cooperation or federated learning and deep learning hybrid approach, should be implemented in the future (Roy and Chen, 2024). Communication intent-based threats can be further identified by integrating natural language processing in sentiment analysis, which has been used in recent studies (Al-Shehari et al., 2024). AI generated threats would enhance resilience in scaling to include the growing relevance of generative tools (Cybersecurity News, 2025).

On the whole, the research will be relevant to the computer science community by showing that it is possible to create a scalable, cost-efficient, and machine learning-based solution, which is specific to the needs of developing-world SMEs and helps to close detection gaps where the existing perimeter defense would break down.

Conclusions and Recommendations.

To sum up, the present study manages to design and confirm a new machine learning model based on the use of the Random Forest that can be implemented to detect insider threats among SMEs in the state of Anambra with high performance indicators and realistic threat counts reduced in the pilot stage. The study fills the major gaps in localized cybersecurity solutions because it determines the most common patterns by means of empirical data and situates them with the context of the socioeconomic realities of Nigeria. The lightweight architecture of the framework, as well as the combination of behavioral analytics, is in accordance with UEBA paradigms and provides better detection of anomalies that managing traditional tools miss, especially in resource-limited contexts (IBM, 2025; CrowdStrike, 2025). Findings confirm its usefulness on curbing risks in the view of increasing insider risks within the African continent where SMEs are increasingly

costs and vulnerable (Deloitte Nigeria, 2025; Ponemon Institute, 2025). This contribution is not only important as it advances the insider threat research in the field of computer science, but also fosters digital resilience that enables sustainable economic growth in Nigeria and national cybersecurity policies.

Some solutions include complex implementation and policy recommendations. SMEs need to be encouraged to implement simple ML-based surveillance systems, which will be enhanced by periodic exhaustion of employees on the culture of cybersecurity and the minimization of cases of negligence (Mugwagwa et al., 2024; SentinelOne, 2024). The exposure can be further restricted with the use of least-privilege access controls, as well as data loss prevention (Resolver, 2025). Regulators and policymakers, including the Nigerian Communications Commission and National information technology development agency should offer subsidies or incentives to SMEs to adopt cybersecurity such as low-cost UEBA frameworks and awareness creation (Deloitte Nigeria, 2025). Working with managed security service providers might also address the problem of skills gaps, so that the outsourced monitoring can be adapted to local threats. Further studies should also consider academic studies that use hybrid models that combine federated learning and explainable AI to increase the level of trust and adaptation in different African settings (Alzaabi and Mehmood, 2024; Roy and Chen, 2024). To help with the wider usage models, setting national insider threat standards and anonymized data. Finally, a holistic manner of integrating technology and education with policy will enable the SMEs to fight insider threats successfully to achieve cybersecurity maturity in the long run.

References

Adedoyin, A., et al. (2019). Cyber incidents in southeastern Nigeria. Journal of African Cybersecurity, 5(2), 45-60.

Al-Mhiqani, M. N., et al. (2020). A review of insider threat detection: Classification, machine learning. Applied Sciences, 10(15), 5208.

Al-Shehari, T., Al-Razgan, M., Alfakih, T., Alsowail, R. A., & Pandiaraj, S. (2024). Enhancing insider threat detection in imbalanced cybersecurity settings using the density-based local outlier factor algorithm. IEEE Access, 12, 45678-45689.

Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access, 12, 30907-30927.

Ambalavanan, V. (2020). Cyber threats detection and mitigation using machine learning. Handbook of Research on Cyber Crime.

Anderson, J. P. (1980). Computer security threat monitoring and surveillance. Technical Report, James P. Anderson Co.

Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5-32.

Cappelli, D., et al. (2009). Insider threat study: Illicit cyber activity in the information technology and telecommunications sector. CERT Program.

Chattopadhyay, P., et al. (2022). Hybrid models for insider prediction. IEEE Transactions on Information Forensics and Security, 17, 1234-1245.

Cole, E., & Ring, S. (2005). Insider threat: Protecting the enterprise from sabotage, spying, and theft. Syngress.

Costa, D. L., et al. (2021). Meta-analysis of insider threats. Computers & Security, 104, 102199.Creswell, J. W., & Plano Clark, V. L. (2017). Designing and conducting mixed methods research. Sage.

CrowdStrike. (2025). What is user and entity behavior analytics (UEBA)? CrowdStrike Cybersecurity Resources.

Cybersecurity News. (2025). Insider threats in 2025: Detection and prevention strategies. Cybersecurity News.

Deloitte Nigeria. (2025). Nigeria's cybersecurity outlook 2025. Deloitte Nigeria Perspectives.

Dioha, I. J. (2022). ICT usage in Nigerian firms. Nigerian Journal of Technology, 41(3), 567-578.ENISA. (2020). Threat landscape for SMEs. European Union Agency for Cybersecurity.

Gamachchi, A., & Boztas, S. (2017). Graph-based ML for user behavior analytics. Proceedings of the Australasian Computer Science Week.

Gartner. (2015). Market guide for user and entity behavior analytics. Gartner Research.

Ho, T. K., et al. (2018). Random Forest for anomaly detection. Data Mining and Knowledge Discovery, 32(4), 1023-1045.

IBM. (2025). What is user and entity behavior analytics (UEBA)? IBM Think Topics.

Liu, L., et al. (2018). Deep learning for sequential pattern recognition. IEEE Transactions on Cybernetics, 48(8), 2463-2475.

Magklaras, G. B., & Furnell, S. M. (2002). Insider threat prediction tool: Evaluating the insider threat. Computers & Security, 21(1), 62-73.

Mthunzi, S. N., et al. (2020). Cultural nuances in African cybersecurity. International Journal of Information Security, 19(5), 567-578.

Mugwagwa, A., Bhero, E., & Chibaya, C. (2024). Cybersecurity strategy: Future proof cybersecurity for small to medium enterprises in South Africa. International Journal of Research in Business and Social Science, 13(5), 123-145.

National Bureau of Statistics. (2022). Socioeconomic statistics: Anambra State. NBS Nigeria.

Nigerian Communications Commission. (2021). Annual report on cyber threats. NCC.

Nwanmuoh, E. E., et al. (2024). ICT contribution to SME growth in Anambra. Journal of Business Management, 12(1), 34-45.

Onatuyeh, E., et al. (2025). Cybersecurity and business survival in Nigeria: Building customer's trust. African Journal of Applied Research, 11(1), 882-895.

Osho, O., & Onoja, A. D. (2015). Cybercrime impacts on Nigerian businesses. African Journal of Computing & ICT, 8(4), 1-10.

Parker, D. B. (1983). Fighting computer crime. Scribner.Pedregosa, F., et al. (2011). Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12, 2825-2830.

Ponemon Institute. (2025). Cost of insider risks report 2025. Ponemon Institute.Resolver. (2025). 6 strategies for mitigating insider threats. Resolver Blog.

Probst, C. W., et al. (2010). Insider threats in cybersecurity. Springer.

Roy, K. C., & Chen, G. (2024). GraphCH: A deep framework for assessing cyber-human aspects in insider threat detection. Cybersecurity, 8, 17.

SADI Journal. (2023). Population estimates for Anambra SMEs. SADI Journal of Economics and Social Sciences.

Securonix. (2024). User and entity behavior analytics (UEBA) solutions for threat detection. Securonix Products.

SentinelOne. (2024). A guide to insider threat mitigation for small businesses. SentinelOne Platform.

Sharma, R., Sherje, S. N., Sharma, S., Ahuja, K., Marathe, V., & Birari, D. R. (2025). Machine learning for insider threat detection in cybersecurity—A comparative analysis. In Innovations in communication networks: Sustainability for societal and industrial impact (pp. 343-355).

Springer.Splunk. (2025). Splunk user and entity behavior analytics (UEBA). Splunk Products.

State of States. (2023). SMEs rankings: Anambra. Kingmakers.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(4), 441-469.

Tuor, T., et al. (2017). Deep learning for unsupervised insider threat detection. Proceedings of the Machine Learning Research.

UNDP. (2021). Cybersecurity awareness in Africa. United Nations Development Programme.

Verizon. (2023). Data breach investigations report. Verizon.Wood, B. (1999). An insider threat model for adversary simulation. SRI International.

Yuan, S., et al. (2023). Random Forest ensembles for threat detection. Cybersecurity Journal, 6(2), 89-102.