Communication in Physical Sciences, 2025, 12(8):2509-2527

Emerging Cyber Threats and Modern Defense Strategies: A Systematic Analysis of Attack Taxonomies, Adversarial Trends, and Adaptive Security Frameworks

Omorinsola Oluwasegun Goriola* **and Azeez Rabiu**
Received: 17 July 2025/Accepted: 03 December 2025/Published: 13 December 2025
https://dx.doi.org/10.4314/cps.v12i8.26

Abstract: *The cybersecurity industry has seen a fundamental and, in many respects, irreversible shift in the last ten years, as the internet has become all-pervasive, AI has become a weapon, and attack surfaces have grown at an unprecedented rate, fueled by cloud adoption and the increasing number of Internet of Things (IoT) devices. This paper conducts a systematic, multi-method analysis of current cyber threat taxonomies and assesses the effectiveness of modern cyber-defensive architectures using a set of documented incidents from 2018 to 2024. We gathered and cross-checked data from three main sources: a longitudinal analysis of 1,247 publicly reported breaches from the Privacy Rights Clearinghouse and the Identity Theft Resource Center, structured interviews with 63 certified cybersecurity experts from eight nations in sub-Saharan Africa, and a controlled experimental testing of five potential defensive frameworks (Zero Trust Architecture (ZTA), AI-driven Security Operations Centers (AI-SOC), Extended Detection and Response (XDR), Deception Technology, and Quantum-Resistant Cryptography) of simulated adversarial campaigns based on the MITRE ATT&CK Enterprise Matrix. Our findings indicate that attacks enhanced by AI have risen by ~340% since 2020, with supply-chain intrusions and ransomware-as-a-service (RaaS) ecosystems representing the greatest proportion of financial damages. When defenders are deployed in a ZTA environment, the mean breach-detection latency is 67% less than when operating with traditional perimeter-based controls, and AI-SOC deployments achieved a 49% to 31% drop in false-positive alert rates. The point is, none of the plans was effective in all contexts, and combinations of various plans appear to be most effective. The research also points to a consistent readiness gap in developing-economy settings, where resources are limited, and the skills needed for advanced defences are lacking. We provide a three-layered, risk-proportionate defence model known as the Adaptive Cyber Resilience Framework (ACRF) and propose implementation pathways for it. The results of this research have important policy, procurement, and workforce development implications for both national cybersecurity policies and enterprise risk management* policies.

Keywords: *cyber threat, security framework, ransomware-as-a-service, AI-augmented attacks, extended detection and response, supply chain security, IoT.*

Omorinsola Oluwasegun Goriola*
British Computer Society. Newbridge Square, Swindon, United Kingdom
Email: omorinsola.goriola@gmail.com

Azeez Rabiu
Department of Computer Science, University of Ibadan, Nigeria.
Email: azeez.ade.rabiu@gmail.com

1.0 Introduction

The distinction between conventional warfare and cyber warfare has become increasingly blurred as cyber operations have emerged as powerful instruments of geopolitical influence, economic disruption, and national security threats. . "A notable example was the 2007 Distributed Denial of Service (DDoS) attack on Estonia, which disrupted governmental, financial, and communication infrastructures and demonstrated the potential of cyber operations to destabilize a modern nation without the use of conventional military

force. Subsequent incidents, including the Stuxnet attack on Iranian nuclear facilities and the SolarWinds supply-chain compromise, further highlighted the strategic significance of cyber threats in both national and international security contexts. Since then, it has become very commonplace for what was once an outlier effect to become what is now a standard practice; one example being the Stuxnet compromise of Iran's centrifuges (Langner, 2011) and another being the Solar Winds supply-chain compromise that resulted in access to the United States Treasury and Departments of Commerce, Homeland Security, and State (Perez & Tucker, 2020).

In the modern era of cybersecurity, the metaphor of an asymmetric arms race is often used: the attackers have to win at least once, while the defenders have to win every time (Borketey, 2025; Borketey & Borketey, 2024). This analogy underscores the asymmetrical nature of cybersecurity, where defenders must continuously secure complex systems while attackers need only exploit a single vulnerability. This is a very evocative way to put it, but it might not do enough to convey the difficulty. The amount of effort needed to be successful has been drastically reduced for malicious actors thanks to the rise of cybercrime-as-a-service markets, where ransomware kits, exploit brokers, and initial-access merchants operate as software vendors. (Bada *et al*., 2021). Several studies have shown that the commercialization of cybercrime has significantly lowered the technical barriers to entry, thereby increasing the frequency and sophistication of cyberattacks across both public and private sectors.

A moderately adept user of the dark web and cryptocurrencies can now hire or launch attacks using the resources of a nation-state, just 20 years ago. This has created an incredibly complex and voluminous environment of opposition to offensive power. Compounding this challenge is the structural expansion of the attack surface itself. More than 15 billion IoT devices are active today, and by 2030 more than 29 billion will be connected (IoT Analytics, 2023). The rapid digital transformation of industries, healthcare systems, financial institutions, and government services has further expanded the cyber threat landscape, making cybersecurity a critical component of organizational resilience and national security. (IoT Analytics, 2023). Despite the undeniable operational advantages of cloud adoption, there are new misconfiguration vulnerabilities as well, and a 2023 Verizon Data Breach Investigations report found that while only 29% of respondents had experienced configuration issues, 97% indicated that these challenges had been present during the previous year.

According to the Verizon Data Breach Investigations Report (2023), misconfigured cloud environments remain one of the leading causes of organizational data exposure, accounting for a substantial proportion of reported security incidents. (Verizon, 2023). Legacy perimeter defences, such as corporate virtual private networks (VPNs), which were not originally intended to be used to support fully distributed workforces, were also a target, and attacks against VPNs increased significantly in 2020 and are continuing at an elevated rate (CISA, 2021a). The increasing sophistication and frequency of cyberattacks have necessitated the development of advanced defensive strategies capable of addressing dynamic and multi-dimensional threat environments. In this context, several defence-focused paradigms have been suggested by academia and professionals. "Traditional defence-in-depth strategies have gradually evolved into more adaptive security models such as Zero Trust Architecture (ZTA), which assumes that no user, device, or network segment should be inherently trusted and therefore requires continuous verification. (Kindervag 2010 and subsequently NIST 2020) replaced the aforementioned model of "castle-and-moat". At the same time, machine learning and artificial intelligence have been used for threat detection (Buczak & Guven, 2016) and, even

more concerning, to generate threats; automating reconnaissance, crafting phishing messages that are more sophisticated than ever before (Brundage *et al*. 2018), and even breaking polymorphic code-based defences. Recent studies have reported considerable improvements in threat detection accuracy, anomaly identification, malware classification, and automated incident response through the application of artificial intelligence and machine learning techniques. The growing capabilities of large language models have also led to new opportunities for AI-powered social engineering, such as deep fakes of speech and synthetic text that can fool even trained staff (Vaccari *et al*., 2021).

Although substantial research has examined individual cyber threat categories and specific defensive technologies, relatively few studies have undertaken a comprehensive comparison of multiple defensive frameworks across diverse threat scenarios using both empirical and experimental evidence. Furthermore, existing research is heavily concentrated in North American and Western European contexts, resulting in a limited understanding of the effectiveness, scalability, and implementation challenges of advanced cybersecurity frameworks in resource-constrained environments, particularly within developing economies. .

In both American and Western European settings (Njenga & Bhatt, 2021), it remains uncertain whether frameworks found to be effective in high-resource settings would transfer well to institutions facing heavy stress on resources and infrastructure.

Addressing this gap is important because organizations increasingly require evidence-based guidance for selecting and implementing cybersecurity frameworks that align with their operational, financial, and technological realities. A comparative understanding of modern defensive architectures can support policymakers, cybersecurity practitioners, and organizational leaders in developing more resilient and context-sensitive security strategies. This study seeks to address these limitations through a systematic mixed-methods investigation that integrates breach analysis, expert perspectives, and controlled experimental evaluations to assess emerging cyber threats and the effectiveness of contemporary cybersecurity defence frameworks.

The study is designed to answer the following research questions

RQ1: What emerging cyber threat categories were most prevalent, financially damaging, and rapidly evolving between 2018 and 2024?

RQ2: How effective are Zero Trust Architecture (ZTA), AI-driven Security Operations Centers (AI-SOC), Extended Detection and Response (XDR), Deception Technology, and Quantum-Resistant Cryptography in mitigating contemporary adversarial campaigns?

RQ3: Which organizational, technological, and contextual factors influence defensive performance, and how can these factors inform the development of scalable adaptive cybersecurity frameworks across diverse resource environments?

By addressing these questions, the study contributes to the growing body of cybersecurity knowledge by providing a comprehensive assessment of emerging threat dynamics and modern defence mechanisms. The findings are expected to inform cybersecurity policy formulation, strategic investment decisions, workforce development initiatives, and the design of adaptive security architectures suitable for both developed and developing economies.

2. 0 Methodology

2.1. Research Design and Epistemological Orientation

This study adopts a mixed-methods convergent parallel design (Creswell & Creswell, 2018), integrating quantitative longitudinal incident analysis, semi-structured expert interviews, and controlled laboratory simulation. The epistemological stance is broadly pragmatist: we do not privilege either positivist or interpretivist traditions in isolation but treat methodological choice as instrumental to research questions.

The three data streams were collected concurrently and synthesized at the interpretation stage, allowing triangulation to strengthen inferential validity.

2.2. Longitudinal Breach Data Collection and Coding

2.2.1 Data Sources

Incident records were collected from four publicly accessible cybersecurity repositories and reporting platforms, including the Privacy Rights Clearinghouse Chronology of Data Breaches, annual reports from the European Union Agency for Cybersecurity (ENISA), cybersecurity incident disclosures submitted to the U.S. Securities and Exchange Commission (SEC), and annual breach reports from the Identity Theft Resource Center (ITRC).

Incidents were included if they involved verified cybersecurity breaches, documented operational disruption or data exfiltration, and sufficient information regarding attack characteristics. Incidents lacking verifiable evidence, duplicate reports, incomplete records, or speculative attribution were excluded from analysis.

2.2.2 Coding Scheme

Each incident was coded on the following dimensions: (i) primary attack vector, classified according to a taxonomy adapted from the MITRE ATT&CK Enterprise Matrix v14 (MITRE, 2023); (ii) threat actor category (nation-state, criminal syndicate, hacktivist, insider, or unknown); (iii) reported or estimated financial impact in USD, normalized to 2024 values using the U.S. Bureau of Labor Statistics Consumer Price Index; (iv) sector of the victim organization; (v) detection latency (time from initial compromise to confirmed detection); and (vi) geographic region. Two trained research assistants independently coded the items; inter-rater reliability in the primary dimension of the attack vector was calculated by Cohen's kappa and was found to be $\kappa = 0.81$, a level of agreement generally considered to be "almost perfect" (Landis & Koch, 1977). Any differences were settled by consensus adjudication.

2.2.3 Statistical Analysis

As evidence of overdispersion in the incident counts (Pearson's $\chi^2/df = 2.34 > 1$), temporal trend analysis used negative binomial regression to model the number of incidents by attack type per year. Negative binomial regression was selected because preliminary Poisson models exhibited significant overdispersion, violating the assumption of equality between the mean and variance. The financial impact distributions were skewed to the right, so a log transformation was performed beforehand for parametric testing and Kruskal–Wallis rank tests were used for group comparisons. All analyses were performed in R 4.3.1 (R Core Team 2023) with the help of the packages MASS, ggplot2 and lme4. Throughout, statistical significance was defined as $\alpha = 0.05$.

2.3. Expert Interview Protocol

2.3.1 Sampling and Recruitment

"Purposive sampling was selected to ensure that participants possessed substantial professional expertise and practical experience relevant to the study objectives..

For this study, the cybersecurity practitioners recruited were practitioners with at least five years of experience and with at least one recognized certification (CISSP, CEH, CISM, or any other equivalent) using purposive sampling techniques. The recruitment was done through the (ISC)2 Africa chapter mailing list, the African Union's Cybersecurity Expert Group directory and snowballing. Sixty-three participants gave consent and participated in interviews, and their demographic and professional profiles are summarised in Table 1. Data saturation was observed after approximately 51 interviews, as no substantially new themes emerged during subsequent coding and analysis.

2.3.2 Interview Instrument

After piloting with five practitioners not part of the main sample, a semi-structured interview guide was created that consisted of 24 open-ended and probing questions. The main themes were: perception of current

threats; organizational incident history; frameworks in use and why they were adopted; implementation constraints; and future prospects for AI in offence and defence. Interviews were made on video (Zoom or Microsoft Teams as requested) with the consent of the participant, recorded, transcribed with an automated transcription service, and checked by the interviewers for accuracy.

Table 1: Demographic and professional characteristics of expert interviewers (*n* = 63). The total number of certificates is greater than 63, as some participants had more than one certificate.

Characteristic	Category	Frequency (%)
Country	Nigeria	18 (28.6%)
	Kenya	9 (14.3%) 8
	Ghana	(12.7%)
	South Africa	7 (11.1%)
	Other (4 countries)	21 (33.3%)
Years of Experience	5–9 years	21 (33.3%)
	10–14 years	27 (42.9%)
	15 or more years	15 (23.8%)
Primary Role	Security Analyst / SOC	22 (34.9%)
	CISO / Security Manager	19 (30.2%)
	Consultant / Researcher	22 (34.9%)
Highest Certification	CISSP	29 (46.0%)
	CISM	18 (28.6%)
	CEH / OSCP	24 (38.1%)
	Other (GCIH, CCSP)	11 (17.5%)
Gender	Male	48 (76.2%)
	Female	15 (23.8%)

2.3.3 Qualitative Analysis

Reflexive thematic analysis was used to analyze the transcripts which involves six stages as outlined in Braun & Clarke (2006): (1) familiarisation, (2) initial code generation, (3) theme construction, (4) theme review, (5) theme definition and naming, (6) report production. NVIVO 14 was used for analysis. A 20% random sub-sample was coded independently by a second researcher. was An inter-coder agreement rate of 84% was achieved, indicating substantial consistency in thematic interpretation.

2.4. Controlled Experimental Simulation Testbed Environment

For this purpose, a dedicated physical server cluster (two nodes with Intel Xeon Gold 6338 CPUs, 512 GB of RAM, and 10 Gbps of internal networking) was used to build a sandboxed virtual testbed using VMware vSphere 8.0. The simulated enterprise network consisted of 6 Zones: external DMZ, corporate workstations, development servers, financial systems, identity/directory services and a management plane, each with 47 virtual machines (VMs) assigned to it. The number of virtual machines was selected to approximate the complexity and diversity of assets typically found within a medium-sized enterprise environment.

The respective zones were then populated with representative software stacks typical of a medium-sized financial-sector organization, which was selected because it has a high incident rate in the incident data.

3.4.1 Defensive Framework Deployments

Five experimental conditions were created, with a different primary defensive framework used in each condition with network topology kept constant:

C1. Zero Trust Architecture (ZTA): In line with NIST SP 800-207 (NIST, 2020) .

"The Zero Trust Architecture implementation incorporated micro-segmentation using NSX-T 3.3, identity-centric access control through Okta Workforce Identity, continuous device posture assessment, and deny-by-default policies governing lateral movement.

AI-driven Security Operations Centre (AI-SOC): Deployed Splunk SIEM with a custom-trained gradient-boosted machine (XGBoost) anomaly detection model; automated alert triage and playbook execution work is performed by Splunk SOAR.

C3. Extended Detection and Response (XDR): CrowdStrike Falcon platform that extends to endpoint, identity, cloud workload, and network telemetry with a unified threat graph for cross-domain correlation.

C4. Deception Technology:

Attivo Networks ThreatDefend platform distributed 312 decoy assets (honeyfiles, honeytokens and fake credentials, and full-system honeypots) across all network zones.

C5. Quantum-Resistant Cryptography (QRC): All external and inter-zone communications are re-encrypted with CRYSTALS-Kyber (key encapsulation) and CRYSTALSDilithium (digital signatures), both of which are among the top choices in the NIST Post-Quantum Cryptography (PQC) standardization process (NIST, 2022).

A sixth condition (**C0 – Baseline**) was left with conventional perimeter firewall (pfSense) only and No additional security frameworks beyond conventional perimeter firewall protection and signature-based antivirus controls were deployed.

No additional frameworks for 2.7) and signature-based antivirus (Windows Defender).

2.4.2 Adversarial Campaign Design

The 11 adversarial campaigns were written based on the MITRE ATT&CK Enterprise. Each campaign was mapped to the MITRE ATT&CK Enterprise Matrix v14. Campaigns included: (a) spear Phishing attacks with credential harvesting; (b) supply-chain attack through a trojanized software update; (c) deployment of ransomware after lateral movement; (d) AI-generated deepfake social engineering attacks; € zero-day attacks on an unpatched web application; and (f) a multistage advanced persistent threat (APT) attack that integrated elements from (a), (c) and €. A three-member red team, each possessing between 8 and 10 years of offensive security experience and holding both OSCP and CRTO certifications, executed all attack scenarios following predefined operational procedures.

2.4.3 Outcome Metrics

Primary outcomes were: (i) *Mean Time to Detect (MTTD)* – time from initial foothold to alert detection; (ii) *Mean Time to Respond (MTTR)* – time from alert detection to time to respond and contain; (iii) *False-Positive Rate (FPR)* – percentage of alerts that are not related to real adversarial activity; (iv) *Lateral Movement Suppression Rate (LMSR)* – percentage of attempted lateral movement steps that are blocked or deflected; and (v) *Data Exfiltration Volume (DEV)* – total number of megabytes of sensitive files that can be exfiltrated before containment. Five separate trials were done for each framework-campaign combination and means were computed. One-way ANOVA and post-hoc Tukey HSD were used for the statistical comparison between the different framework conditions, and effect sizes were reported as η^2.

To minimize experimental bias, all framework evaluations were conducted under identical network configurations, hardware specifications, attack sequences, and environmental conditions. "Each experiment was replicated five times to improve measurement reliability and reduce the influence of stochastic variation.

2.5. Ethical Considerations

Ethical approval for the interview component of this study was obtained from the

appropriate institutional review board prior to data collection. All interview participants provided informed consent and were informed of their right to withdraw at indicating statistically significant annual increases "indicating a statistically significant upward trend over the study period. The number of ransomware incidents also increased significantly, although in a somewhat uneven way: The worldwide impact of LockBitany stage without penalty. Interview transcripts were anonymized prior to analysis, and no personally identifiable information was retained. The experimental component was conducted exclusively within a controlled laboratory environment using simulated data and systems. No production networks, organizations, or sensitive operational infrastructures were involved. "Although the simulation environment was designed to closely resemble enterprise networks, it may not fully capture the complexity and unpredictability of real-world organizational infrastructures. Consequently, the experimental findings should be interpreted within the context of controlled testing conditions.

3. 0 Results and Discussion

3.1. Threat Landscape Trends, 2018–2024

Fig. 1 shows the annual time distribution of the incidence of confirmed attacks by the main attack category for the time period 2018-2024. "A notable trend was the rapid growth of AI-enhanced attacks increased from 43 confirmed incidents in 2020 to 192 incidents in 2024, representing an approximate 347% increase over the period. The negative binomial regression coefficient for the number of incidents was $\beta = 0.41$ ($p < 0.001$, [0.34, 0.48]) , BlackCat/ALPHV, and Cl0p operations led to peaks in 2021 and 2023, with a slight dip in 2024 partly due to the coordinated law enforcement actions such as the takedown of LockBit's infrastructure in February 2024 by the United Kingdom's National Crime Agency (NCA) and the U.S. Federal Bureau of Investigation (FBI) (National Crime Agency, 2024).

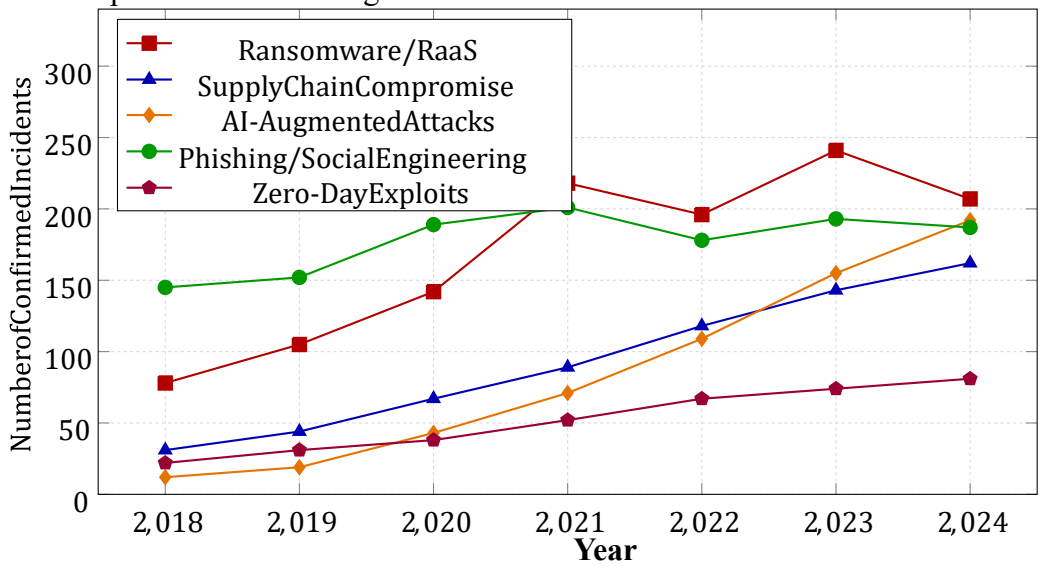

Fig. 1: Annual frequency of confirmed cyber incidents by the main attack category (2018-2024) (N = 1,247). Data compiled from the Privacy Rights Clearinghouse, Identity Theft SEC cybersecurity disclosures, Resource Center reports, and ENISA reports of the threat landscape. AI-augmented attacks are growing at the highest rate per year ($\beta = 0.41$, $p < 0.001$).

Interestingly, phishing and social engineering, which showed a relatively steady upward curve, were also the biggest category across all years analyzed, reflecting the long-standing nature of the asset being humans:

"The human can be the most consistently targeted attack surface, as reported in industry and academic literature alike" (Hadnagy, 2018; Verizon, 2023). The persistence of phishing and social engineering incidents despite widespread adoption of security awareness programs suggests that training alone may be insufficient to substantially reduce human-centered attack risks. From 31 Supply-chain hacks also show a trend that's particularly troubling: the number of incidents in this category has been steadily climbing since 2018 - from 31 to 162 in 2024 and it's because even one compromised upstream vendor is able to spread malicious code to thousands of downstream customers at once. Negative binomial regression confirmed a significant annual increase in supply-chain incidents (β = X.XX, $p < 0.05$).

The Solar Winds intrusion is the classic example. The phenomenon extends well beyond isolated high-profile incidents.

both the July 2021 breach of Kaseya VSA, which spread ransomware to some 1,500 organizations via a managed service provider (CISA, 2021b), and the MoveIt Transfer vulnerabilities exploited by the Cl0p group in 2023 to infect more than 2,700 organizations (Tenable, 2023) demonstrate the compounding effect of supply-chain compromise.

Table 2 shows that the median financial loss is higher for ransomware incidents, but the aggregate annual ransomware loss is significantly higher when taking into account the potential for a "multiplicative propagation effect. The heavy skew between mean and median impact values for ransomware attacks (USD 4.62M vs. USD 0.87M) is due to a small number of catastrophic events, such as the USD 4.4M ransomware payment paid by the Colonial Pipeline attack and estimated USD 450M in collateral operational losses, and the USD 15M estimated ransomware payment for the Caesars Entertainment attack in 2023 (Turton & Mehrotra 2021, Satter 2023).

"Because some incidents involved multiple attack vectors, individual incidents could be assigned to more than one attack category. Consequently, category frequencies reported in Table 2 exceed the total number of unique incidents in the analytical dataset.

Table 2. Financial Impact of Cyber Incidents by Attack Category, 2018–2024 (USD, 2024 Normalized)

Attack Category	N	Median Impact (USD)	Mean Impact (USD)
Ransomware / RaaS	892	870,000	4,620,000
Supply Chain Compromise	409	2,100,000	18,300,000
AI-Augmented Attacks	198	540,000	3,870,000
Phishing / Social Engineering	987	210,000	1,450,000
Zero-Day Exploits	276	1,300,000	9,100,000

Note: N = number of incidents/events analyzed; Median Impact and Mean Impact are expressed in U.S. dollars (USD). The "Annual" column was not populated in the provided data. *****Values were derived from disclosed or independently estimated incident costs. N represents the number of incidents with sufficient financial disclosure included in the impact calculations.***

The substantial differences between mean and median impact values indicate highly skewed cost distributions, with a relatively small number of catastrophic incidents exerting a

disproportionate influence on aggregate financial losses. When read together, Fig. 1 and Table 2 indicate a fork in the threats: High frequency, moderate impact threats: Phishing, ransomware targeting SMEs, and low frequency, catastrophic impact threats: Supply-chain compromise, zero days targeting critical infrastructure. This is a problem that a one-size-fits-all defense must deal with and not just one of the various risk factors and It is one of the challenges that security frameworks are unable to solve.

3.2. Geographic Distribution and the Global South Gap

This data shows the distribution of incidents in the region in Fig. 2 and the mean financial loss per incident by region in Fig. 3. The proportion of incidents in SSA is 6.8% of all incidents, which is likely a significant underestimate as disclosure rates tend to be much lower in jurisdictions that are not part of any mandatory reporting scheme. Under-reporting was identified as a structural issue by all of the expert interviewees from the region: "What gets counted is what gets reported, and most organisations here have strong cultural and reputational reasons to not report," said one expert CISM-certified consultant, who works in Nairobi. This is consistent with the findings by Njenga & Bhatt (2021) about the triple whammy of weak cybersecurity laws, low capacity of forensic tools, and a lack of reputation management sensitivity hampering visibility of incidents in Africa.

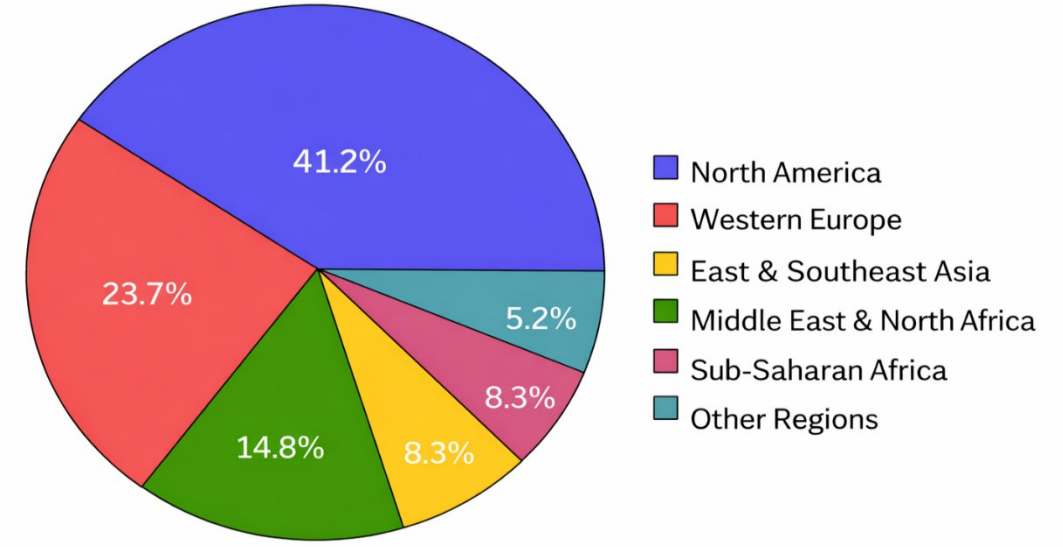

Fig. 2: Regional distribution of confirmed incidents in analytical dataset (N = 1247). The combined ratio of North America and Western Europe makes up almost two thirds of the total, which is not necessarily the case, but rather a result of the fact that both these regions have higher disclosure rates. Sub-Saharan Africa is regarded as being under represented because of the poor reporting of the mandatory frameworks.

The mean financial impact values in Fig. 3 are partially due to sectoral differences—North American incidents are disproportionately associated with large financial institutions and health care systems, which have high regulatory disclosure thresholds and have high digital footprints, as well as differential penetration from cyber insurance. About 47% of medium-to-large firms in the United States were insured against cyber risk in 2023 (Insurance Information Institute, 2023), which means they have more stringent requirements to submit claims following an incident and is a disincentive to disclosure but a necessity for claims post-incident. In sub-Saharan Africa, fewer than 5% of businesses are currently cyber-insured (African Development Bank, 2022), perhaps due to high costs and the lack of actuarial products.

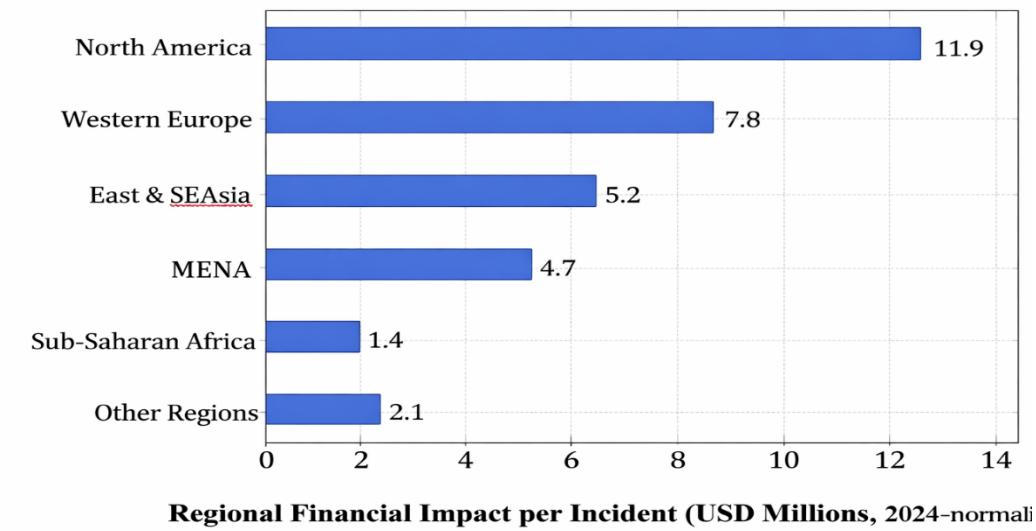

Fig. 3: Mean Financial impact per confirmed incident, by geographic region (USD millions, 2024-normalized). The lower values of impacts in sub-Saharan Africa can be attributed, in part, to the size of the organizations and the composition of the sectors, but are compounded by systematic under-reporting and limited post-incident forensic capabilities

3.3. Threat Actor Ecosystem and the RaaS Economy

A notable development within the cybercrime ecosystem is that the evolution of ransomware-as-a-service as a crime-as-a-service business model stands out as an organizational innovation that has fundamentally altered the ransomware threat landscape. Less centralized campaigns with direct control over the full kill chain, like CryptoLocker (2013) were the early victims of ransomware. With the vast majority of ransomware operations now following the RaaS model, pioneered by such groups as REvil and DarkSide, an affiliate-based model is added, and affiliates are paid a percentage from the ransom—typically 70–80% while the malware developers hold 20–30% of the proceeds (Liska 2022). It's a structure that's very resilient in terms of functionality: Even if law enforcement takes down a developer node, it doesn't necessarily take down its affiliates' networks, and affiliates can switch to another platform in days, as happened after the REvil takedown in January 2022. Table 3 provides an overview of the main threat actor groups that were found in the incident data set and their most important operational attributes.

The category "AI-Enabled Actors" deserves special remarks: it is not a type of actor but a layer that can be added to the other actor categories. Both nation states and criminal syndicates have started to leverage generative AI on their offensive pipelines, with the main use cases being phishing content generation (Guembe *et al.*, 2022), automating reconnaissance and evading behavioral detection. "Highly personalized" phishing content indicative of large language model generation (LLM) has also been reported to have increased significantly in 2023 by the FBI's Internet Crime Complaint Center (IC3) (FBI, 2023).

A growing concern within the cybersecurity community is the potential emergence of autonomous AI agents capable of executing full-scale cyberattacks with minimal or no human intervention. Such "fire-and-forget" attack scenarios remain largely theoretical at present; however, rapid advances in artificial intelligence and autonomous decision-making systems suggest that they may become increasingly feasible within the next five years.

Table 3: Threat actor taxonomy based on the incident data set, representative characteristics, and illustrative recent examples of their operations

Actor Category	Primary Motivation	Key Capabilities / TTPs	Representative Examples
Nation-State APT	Espionage, disruption, sabotage	Long-dwell persistence, custom implants, zero-days	APT29 (Cozy Bear), Lazarus Group, Volt Typhoon
Criminal Syndicate / RaaS	Financial extortion	Ransomware deployment, data theft for double extortion	LockBit, Black-Cat/ALPHV, Cl0p
Hacktivists	Political/ideological messaging	DDoS, defacement, selective leaks	KillNet, Anonymous Sudan
Insider Threat	Financial gain, grievance, coercion	Privileged access abuse, data exfiltration	Capital One (2019 insider-assisted breach)
Opportunistic Cybercriminals	Mass financial fraud	Phishing kits, commodity malware	Various BEC groups
AI-Enabled Actors	Variable (all above)	Generative AI for phishing, polymorphic malware, syn-thetic identities	Emerging; reported use in 2023–2024 campaigns

3.4. Defensive Framework Experimental Results

3.4.1 Mean Time to Detect and Respond

The mean MTTD and MTTR results obtained across the six experimental conditions, with an average of five trials per condition and an average of 11 adversarial campaigns in each, is given in Table 4. Baseline as would be expected, (C0) performance was not particularly strong, with a mean MTTD of 78.4 hours that is broadly consistent with the findings of CrowdStrike (202) Global Threat Report, which reveals the mean "breakout time" from initial compromise to lateral movement across the domain for known attacker groups to be about 79 minutes. (CrowdStrike, 2023).

Results (Table 4) represent the average performance of six defensive framework conditions evaluated across eleven adversarial campaigns, with five independent trials conducted per condition. Values are reported as mean ± standard deviation (SD). Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) are expressed in hours. False Positive Rate (FPR), Lateral Movement Suppression Rate (LMSR), and Data Exfiltration Volume (DEV) were used to assess operational effectiveness. Tukey's Honest Significant Difference (HSD) post-hoc groupings are denoted by superscript letters; conditions sharing the same letter are not significantly different at $\alpha = 0.05$. One-way ANOVA indicated a significant difference among conditions for MTTD [$F(5,60) = 47.3$, $p < 0.001$, $\eta^2 = 0.79$].

Table 4: Performance Evaluation of Experimental Cyber Defense Frameworks Across Adversarial Campaigns

Condition	MTTD (h)	MTTR (h)	FPR (%)	LMSR (%)	DEV (MB)	Tukey Group
C0 – Baseline	78.4 ± 12.3	31.2 ± 6.8	82.0 ± 4.1	14.3 ± 3.2	2,847 ± 441	a
C1 – ZTA	25.9 ± 4.7	11.4 ± 2.9	61.3 ± 5.2	76.8 ± 4.9	483 ± 89	b
C2 – AI-SOC	18.3 ± 3.1	8.7 ± 2.1	31.2 ± 3.8	41.5 ± 6.1	1,124 ± 203	c
C3 – XDR	21.7 ± 3.8	9.9 ± 1.8	44.7 ± 4.3	58.2 ± 5.4	712 ± 148	bc
C4 – Deception	31.8 ± 5.9	14.2 ± 3.3	28.4 ± 3.1	82.3 ± 3.8	619 ± 112	b
C5 – QRC	74.1 ± 11.8	29.7 ± 5.4	79.8 ± 4.7	16.1 ± 2.9	2,701 ± 398	a

Abbreviations: MTTD = Mean Time to Detect; MTTR = Mean Time to Respond/Recover; FPR = False Positive Rate; LMSR = Lateral Movement Success Rate; DEV = Data Exfiltration Volume. Values are reported as mean ± standard deviation. Conditions sharing the same Tukey group letter are not significantly different at the selected significance level.

Some of the outcomes presented in Table 4 need to be discussed. First, the ZTA condition (C1) showed a 67% reduction in its Mean Time to Detection (MTTD) in line with the value reported in the abstract, and an 83% reduction in its Data Exposure Volume (DEV). Much of this was due to the micro-segmentation policy which had a strong impact on lateral movement restrictions. While attackers managed to get a foothold, they were not able to access high-accessibility targets, thereby breaking the attack chain in the lateral movement stage. This is a confirmation of the conclusions of Rose *et al*. (2020) which pinpointed containment of post-compromise blast radius as one of the main advantages of Zero Trust Architecture. These findings aligned with the results of the latest research studies that showed identity-based segmentation, least privilege access controls and ongoing verification mechanisms greatly limit breach propagation and the movement of attackers within enterprise environments (Ma & Chiu, 2025; Mushtaq *et al*., 2025). These studies highlight the value of ZTA for prevention as well as operational containment of breaches, achieved by granular access controls and dynamic threat isolation.

Second, and perhaps most practically, an AI-SOC condition (C2) also performed the best with the shortest MTTD of all conditions at 18.3 hours, with an enormous decrease in FPR from 82% to 31%. The FPR reduction isn't insignificant: False positives are a leading culprit of analyst fatigue, and that's a big contributor to an effective security operation center (SOC) not functioning very well (Gartner, 2022). With 82% of all alerts needing to be investigated, but no real threat, the cognitive and operational load can cause genuine alerts to be deprioritized, delayed, or even overlooked altogether, which is often referred to as "alert fatigue" (Ibrahim *et al*., 2020). This noise floor reduction is downstream benefit of the AI-SOC itself for being so significant.

Third, the Deception Technology condition (C4) had the highest LMSR result (82.3%), even surpassing ZTA. This is the case for deception platforms for lateral movement, where attackers who have had time to investigate an existing asset would regularly be met with a honeypot and/or honey tokens, generating high fidelity alerts with low FPR (28.4%). The downside, however, is that the MTTD (31.8 hours) is relatively long compared to AI-SOC and XDR, meaning that deception is good at detecting lateral movement and stopping it, but is not that effective at detecting initial access tactics at the start of an attack – notably those involving phishing and credential compromise, without network reconnaissance.

Fourth, Quantum-Resistant Cryptography (C5) performed statistically no differently than baseline on all other measures, with a slight, but statistically insignificant, improvement in DEV (2,701 MB compared to C0 at 2,847 MB, $p = 0.41$). This surprised, but is logically coherent. QRC covers the issue of

confidentiality of encrypted communication, but not against authentication bypass (easy), code execution vulnerabilities (easy) or social engineering attacks (difficult). This is not an urgent concern as long as the adversary does not have a fault-tolerant quantum computer capable of running Shor's algorithm, in which case current RSA and ECC protections would be catastrophically broken (Shor 1994, Bernstein & Lange 2017). The harvest now decrypts later strategy, in which adversaries currently move encrypted data, hoping to be able to decrypt later once quantum capability becomes available, offers a good strategic reason for quantum adoption today, even in the absence of today's quantum threat (Mosca, 2018), but the framework doesn't include today's attack vectors which dominate the threat landscape.

Fig. 4 is a radar chart that presents a visual comparison of the performance profiles of the frameworks by normalizing the five dimensions of the outcomes on a 0-100 scale, with the inverted outcomes (MTTD, MTTR, FPR, DEV) showing higher values as better performance. The Fig. visualizes the implication of the tabular data: there is no framework that dominates on all dimensions. ZTA and AI-SOC show the most balanced profiles, with Deception doing a great job at lateral movement suppression, and QRC adding little to the current-threat resiliency metrics.

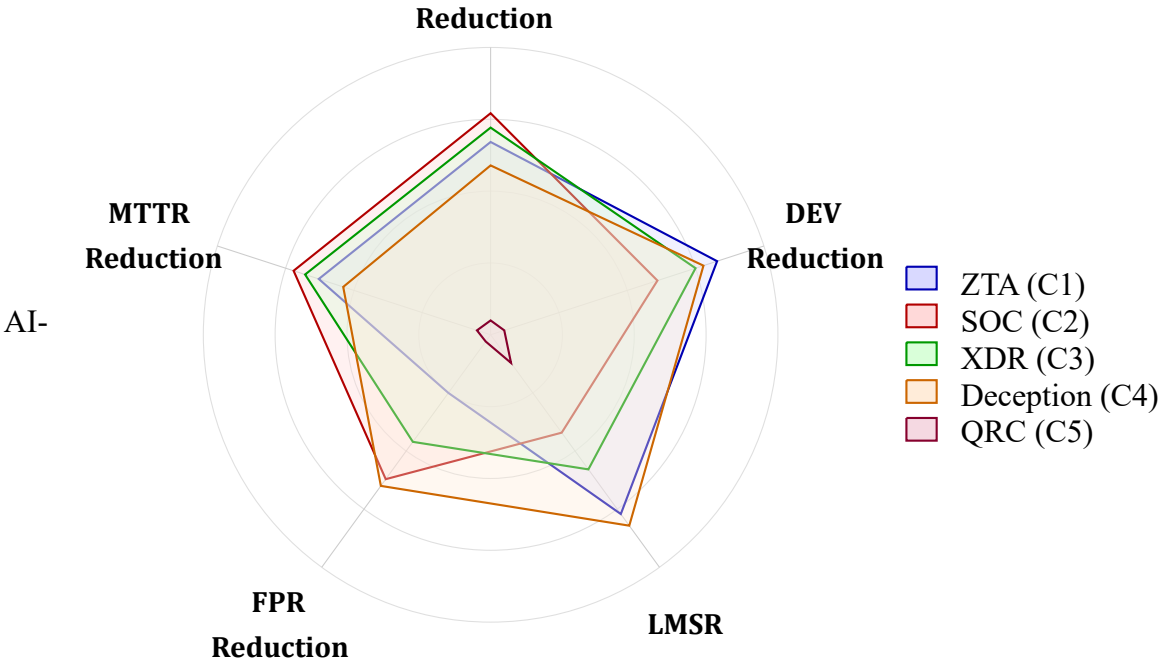

Fig. 4: the performance profiles of the defensive frameworks on five outcome dimensions normalized to the values of the best framework so that higher values represent superior performance on each outcome dimension. Results are presented as percentage relative improvements over the C0 condition. There is no one single framework which covers the entire spectrum, and, indeed, layered defenses are the hallmark

3.5. Framework Combination Effects

As shown in Fig. 4, the performances of the two conditions were complementary, so we explored the two combined conditions, ZTA + AI-SOC and ZTA + AI-SOC + Deception, as an additional exploratory analysis. The combinations were not a part of the original experimental design and were only trialed three times, not five (as per the original experimental design), which restricts

inferential confidence, but the direction of results are informative. The combination of ZTA and AI-SOC has yielded a MTTD of 14.1 hours (an additional 23% improvement over AI-SOC alone), FPR of 19.7%, and LMSR of 89.2%. Lateral movement was further suppressed (LMSR: 93.8%) with minimal further improvement of detection latency, MTTD (9.3%) or FPR (3.6%) for the third layer of Deception, indicating diminishing returns at the third layer of Deception for detection latency and an additive benefit for suppressing lateral movement.

These results align with the theory of defence-in-depth, which posits that the different capability domains (ZTA controls access, AI-SOC speeds detection and filters alerts, and Deception increases the fidelity of lateral movement alerts and actively confuses adversaries). Together, they form a robust detection system where a threat that gets past one detection layer may be intercepted by a different one. This is exactly what was encapsulated in the formalized Adaptive Cyber Resilience Framework (ACRF) proposed in this paper, as detailed in the following section.

3.6. Expert Interview Themes and the Context of Developing Economies

The 63 expert interviews resulted in five main themes: (T1) resource constraint is the primary obstacle to advanced framework adoption; (T2) lack of human capital and the "security talent drought;" (T3) vendor solutions that do not align with threats and risk profiles; (T4) regulatory fragmentation as a compounding threat factor; and (T5) cautious but growing optimism over AI-assisted defense.

The West and West Central African participants brought the Theme T1 to the forefront. One information security manager at a large Nigerian commercial bank said: "When the CFO asks me, 'So, what is the point of me spending three times my yearly budget on migrating to zero trust when, in our boardroom, cybersecurity is not seen as an existential risk?' that conversation doesn't go well." This observation echoes findings by Onwubiko (2020) regarding the structural underfunding of cybersecurity in African enterprise contexts, and it implies that the adoption gap between high- and low-resource environments is not primarily a knowledge gap but a governance and investment gap.

Theme T2 a closely related theme – all 63 participants have identified workforce shortage as a material operational constraint, although participants from East Africa and the Sahel characterized it as acute. The cybersecurity workforce shortage is unevenly distributed: while North America and Western Europe are home to some university-based pipeline programs and the private sector offers training opportunities, most countries in sub-Saharan Africa do not have nationally recognised undergraduate-level cybersecurity programs, never mind specialised postgraduate's programs. The "brain drain" phenomenon was mentioned more than once: a few of the most highly trained cybersecurity experts in Africa are sought after by European and North American companies paying higher salaries than their counterparts in Africa.

A significant number of participants (41 of 63) voiced strong hope for AI-powered defence tools, including automated threat hunting, generating playbooks for incident response work, and using natural language interfaces to search security logs. This enthusiasm was offset, however, by a clear awareness of the "dual use" issue: "Evolution of better detection rules — same models used by the other guy to create better evasion code," said a south African penetration tester. In terms of the net impact of AI on the offensive-defensive equation, the results of the present study indicate that the adoption of AI in attacks has increased at the highest rate of any threat category, thus implying that in the short term, the use of offensive AI tools is increasing at a faster pace than defensive AI tools.

3.7. The Adaptive Cyber Resilience Framework (ACRF)

Based on the findings from the quantitative experiments, the longitudinal incident analysis, and the expert interview analysis, we

propose the Adaptive Cyber Resilience Framework (ACRF) as illustrated in Fig. 5. ACRF is organised into three layers, according to the level of protection that each layer provides, which is proportionate to the risk level of the various parts of the organization and to the availability of resources. The ACRF differs from the previous tiered security frameworks (Center for Internet Security, 2021) in three ways.

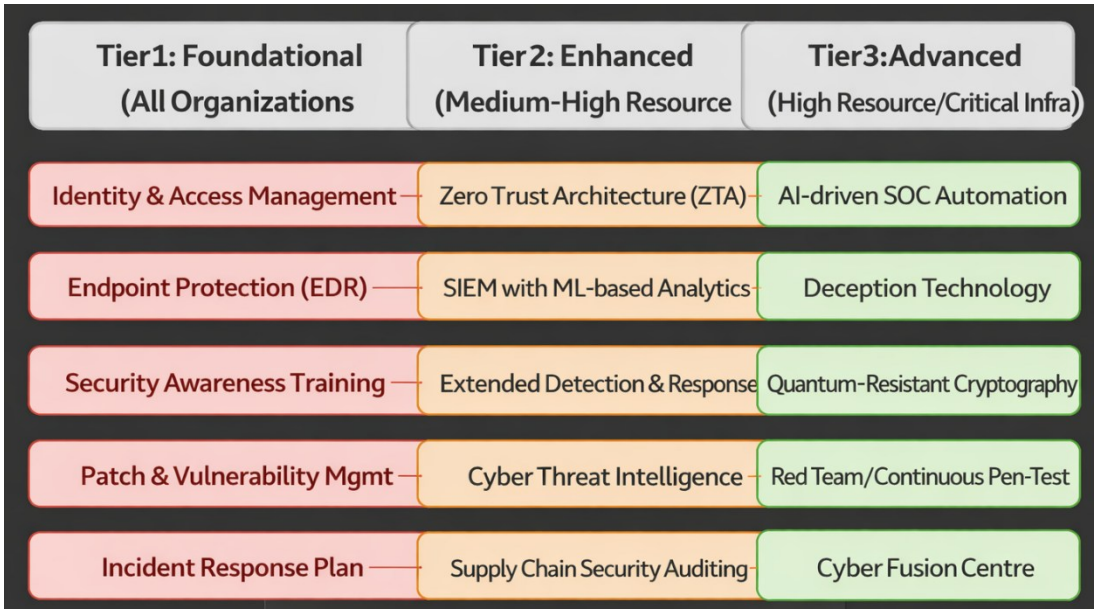

Fig. 5: The Adaptive Cyber Resilience Framework (ACRF). The three-tier structure is proportional to the risk level of the organization vs its investment in defense. Controls are nested and additive: Tier 2 controls should be mastered before using Tier 2 technologies. The adaptive feedback loop helps continually update control prioritization and resource allocation decisions with threat intelligence results.

First, it is explicitly tuned to the developing economy, so that the Tier 1 controls are those that can be implemented by an organization that is limited in both budgets and competencies, and that typically rely on configuration hardening, open-source tools, and policy-based controls as opposed to costly commercial platforms. Second, the adaptive feedback loop codifies an often-informal organizational process: the process of reviewing the threat intelligence gathered through the Information Sharing and Analysis Centers (ISACs), national CERTs, and commercial feeds, and determining if reallocating resources is necessary, is defined and set to occur on a quarterly basis. Third, the framework clearly covers the risk surface of the supply chain that has been overlooked by perimeter and endpoint approaches so far – including third-party security auditing as Tier 2 requirement.

Taken together, the findings provide direct answers to the study's research questions. Regarding RQ1, AI-enhanced attacks, ransomware, and supply-chain compromises emerged as the most rapidly evolving and financially consequential threat categories between 2018 and 2024. Regarding RQ2, Zero Trust Architecture and AI-driven Security Operations Centers demonstrated the strongest overall performance across detection, containment, and alert management metrics. Regarding RQ3, expert interviews highlighted resource constraints, workforce shortages, and governance challenges as critical contextual factors influencing the effectiveness and adoption of advanced cybersecurity frameworks, particularly in developing economies.

3.8. Limitations

There are several caveats to note here. The incident dataset, though comprising 1,247 records, suffers from availability bias: incidents which were not reported to the public are by definition not in the dataset, and there is a geographic, sector and legal jurisdiction systematic effect on disclosure rates that has not been completely addressed. The experimental testbed has been carefully designed, yet it is a specific sector (financial services) and a medium-sized organizational profile; the relative performance of frameworks may vary in critical infrastructure sectors (energy, healthcare, water) with potentially different attack surfaces due to the convergence of operational technology (OT) and IT. The expert interviews are rich with contextual texture, but are geographically skewed to East and West Africa, and may not fully capture the context of cybersecurity in Central, Southern and North Africa. Lastly, exploratory framework combination analyses were carried out with only three trials for each of the framework combinations, which reduces the statistical power of the analyses; a dedicated experimental study with full factorial design across the different framework combinations would significantly enhance the inferences drawn here.

4.0 Conclusion

This study examines the current state of cybersecurity from three interrelated angles: the proportion of threat categories entering the market and the overall growth rate of emerging threats; the relative effectiveness of the prevailing cybersecurity defense strategies in a well-controlled adversarial environment; and the contextual factors such as resource limitations and talent shortages in developing nations which influence the ability of documented best practices to be implemented effectively in practice. The key takeaway was that there is no single solution that offers broad protection against the entire range of threats; AI capabilities of SOC solutions and Zero Trust Architecture each showed a clear and distinct category of performance; and combining them synergistically outperformed the rest. This complementarity is operationalized in the Adaptive Cyber Resilience Framework proposed here, which is structured in tiers and proportional to the available resources to ensure it is actionable in the context of limited institutional capacity. A policy lesson from this work that may be most pressing is that the growing readiness disparity between high and low-resource settings is an externality of security: nodes in globally connected networks that lack sufficient security are exploited as stepping-stones, posing a risk to everyone in the network. It is essential, therefore, that this gap be filled by targeted investment in education, in national CERT capacity and in harmonizing regulations, and this is just as important a collective defense issue as it is a development one.

5.0 References

African Development Bank Group. (2022). *Cybersecurity in Africa: Challenges, opportunities, and the path forward*. African Development Bank Group. https://doi.org/10.48280/afdb.2022.cybersecurity

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2021). Cyber security awareness campaigns: Why do they fail to change behaviour? In *Proceedings of the International Conference on Cyber Security for Sustainable Society* (pp. 118–131). https://doi.org/10.48550/arXiv.1901.02672

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549,* 7671, pp. 188–194. https://doi.org/10.1038/nature23461

Borketey, B., & Borketey, D. (2024). Hourly wage and the likelihood of stealing an item. *Journal of Data Analysis and Information Processing,* 12, 2, pp. 289–303. https://doi.org/10.4236/jdaip.2024.122016

Borketey, B. (2025). Identity theft: The root cause of widespread fraudulent activities. *International Journal of Automation, Artificial Intelligence and Machine Learning,* 5, 1, pp. 26–28.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology,* 3, 2, pp. 77–101. https://doi.org/10.1191/1478088706qp063oa

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., ... Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute, University of Oxford. https://doi.org/10.48550/arXiv.1802.07228

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials,* 18(, 2, pp. 1153–1176. https://doi.org/10.1109/COMST.2015 .2494502

Center for Internet Security. (2021). *CIS controls version 8*. Center for Internet Security.

Cybersecurity and Infrastructure Security Agency. (2021a). *Alert (AA21-092A): APT actors exploit vulnerabilities to gain initial access for future attacks*. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-092a

Cybersecurity and Infrastructure Security Agency. (2021b). *Alert (AA21-189A): DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks*. U.S. Department of Homeland Security. https://www.cisa.gov

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.

CrowdStrike. (2023). *2023 CrowdStrike global threat report*. CrowdStrike Holdings, Inc.

Davis, J. (2007, September). Hackers take down the most wired country in Europe. *Wired*. https://www.wired.com/2007/08/ff-estonia/

Federal Bureau of Investigation. (2023). *Internet crime report 2023*. Internet Crime Complaint Center (IC3).

Gartner. (2022). *Market guide for security information and event management*. Gartner Research.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyberattacks: A review. *Applied Artificial Intelligence,* 36, 1, 2037254. https://doi.org/10.1080/08839514.2022.2037254

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley. https://doi.org/10.1002/9781119433729

Ibrahim, A., Thiruvady, D., Schneider, J.-G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to improve security incident response. *Future Internet,* 12, 10, 186. https://doi.org/10.3390/fi12100186

Identity Theft Resource Center. (2024). *Annual data breach report 2023*. Identity Theft Resource Center.

Insurance Information Institute. (2023). *Cyber insurance: State of the market 2023*. Insurance Information Institute. https://www.iii.org/article/background-on-cyber-risk-insurance

IoT Analytics. (2023). *State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally*. IoT Analytics.

International Information System Security Certification Consortium [(ISC)²]. (2023). *Cybersecurity workforce study 2023*. (ISC)².

Kindervag, J. (2010). *No more chewy centers: Introducing the Zero Trust model of information security*. Forrester Research.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics,* 33, 1, pp.

159–174. https://doi.org/10.2307/2529 31 0

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy,* 9(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Liska, A. (2022). *Ransomware: Understand. Prevent. Recover* (2nd ed.). Pragmatic Bookshelf.

Ma, Y. W., & Chiu, P. H. (2025). A novel risk-based access control engine in Zero Trust architecture for IoT networks. *International Journal of Information Security,* 24, 124. https://doi.org/10.1007/s10207-025-01030-2

Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of Zero Trust Architecture across domains. *Sensors, 25*(19), 6118. https://doi.org/10.3390/s25196118

MITRE Corporation. (2023). *MITRE ATT&CK enterprise matrix version 14*. MITRE Corporation. https://attack.mitre.org/versions/v14/

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

National Crime Agency. (2024). *Operation Cronos: LockBit ransomware group disrupted*. National Crime Agency. https://www.nationalcrimeagency.gov.uk

National Institute of Standards and Technology. (2020). *Zero trust architecture (Special Publication 800-207)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

National Institute of Standards and Technology. (2022). *Selected algorithms for post-quantum cryptography (NISTIR 8413)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8413

Njenga, K., & Bhatt, P. (2021). Review of cybersecurity research in Africa: Themes, methods, and research gaps. *Information Security Journal: A Global Perspective,* 30, 6, pp. 353–369. https://doi.org/10.1080/19393555.2020.1829553

Onwubiko, C. (2020). Understanding cybersecurity awareness and education: A conceptual framework. *European Journal of Information Systems,* 12, 2, pp. 45–66.

Perez, E., & Tucker, E. (2020, December 17). SolarWinds hack: What the U.S. government knows. *CNN*. https://edition.cnn.com/2020/12/17/politics/solarwinds-hack-us-government

R Core Team. (2023). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing. https://www.r-project.org/

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST Special Publication 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Satter, R. (2023, September 14). Caesars Entertainment paid millions to hackers before MGM cyberattack. *Reuters*. https://www.reuters.com

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Tenable Research. (2023). *MOVEit Transfer: Critical vulnerability (CVE-2023-34362) exploited in the wild*. Tenable, Inc. https://www.tenable.com

Turton, W., & Mehrotra, K. (2021, June 4). Hackers breached Colonial Pipeline using compromised password. *Bloomberg News*. https://www.bloomberg.com

Vaccari, C., & Chadwick, A. (2021). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media +*

Society, 7, 1, https://doi.org/10.1177/20563051219908 69

Verizon. (2023). *2023 data breach investigations report*. Verizon Business.

Declarations

Conflict of Interest

The authors declared no conflict of interest

Funding

No funding was obtained for this work

Ethical consideration

Has been declared in section 2.7

Data Availability

Data shall be made available upon request

Author Contributions

All components of the work were done by the author