esentry

Annual Report 2025

Table of Content

Phalanx Formation – Our Identity

Cybersecurity is not about tools. It is about how people work together when things go wrong.A Phalanx is a formation built for pressure. Each unit covers the next. No one advances alone.

When the line holds, everyone behind it is protected. When it breaks, the cost is immediate.That principle reflects how we work at esentry.

Throughout 2025, as organisations across Africa continued to digitize, security could no longer be approached in silos. Growth introduced complexity. Complexity demanded coordination. Effective protection required teams that understood how their role connected to the whole, a Managed Security Service provider.

Our cyber defense, threat intelligence, cyber offense, security engineering, and customer success teams operated as Phalanx ,one coordinated unit. Intelligence guides decisions.

Human expertise was reinforced with intelligent systems that helped us detect patterns, respond faster, and adapt to attacks that were increasingly automated and AI-driven. Each function remained distinct, but non-independent. Decisions were informed. Actions are deliberate. Responsibility was shared.

This approach shapes how we prepare, respond, and protect the organisations that rely on us. What works today is tested tomorrow, and we adjust. It keeps us effective as environments change and expectations rise.

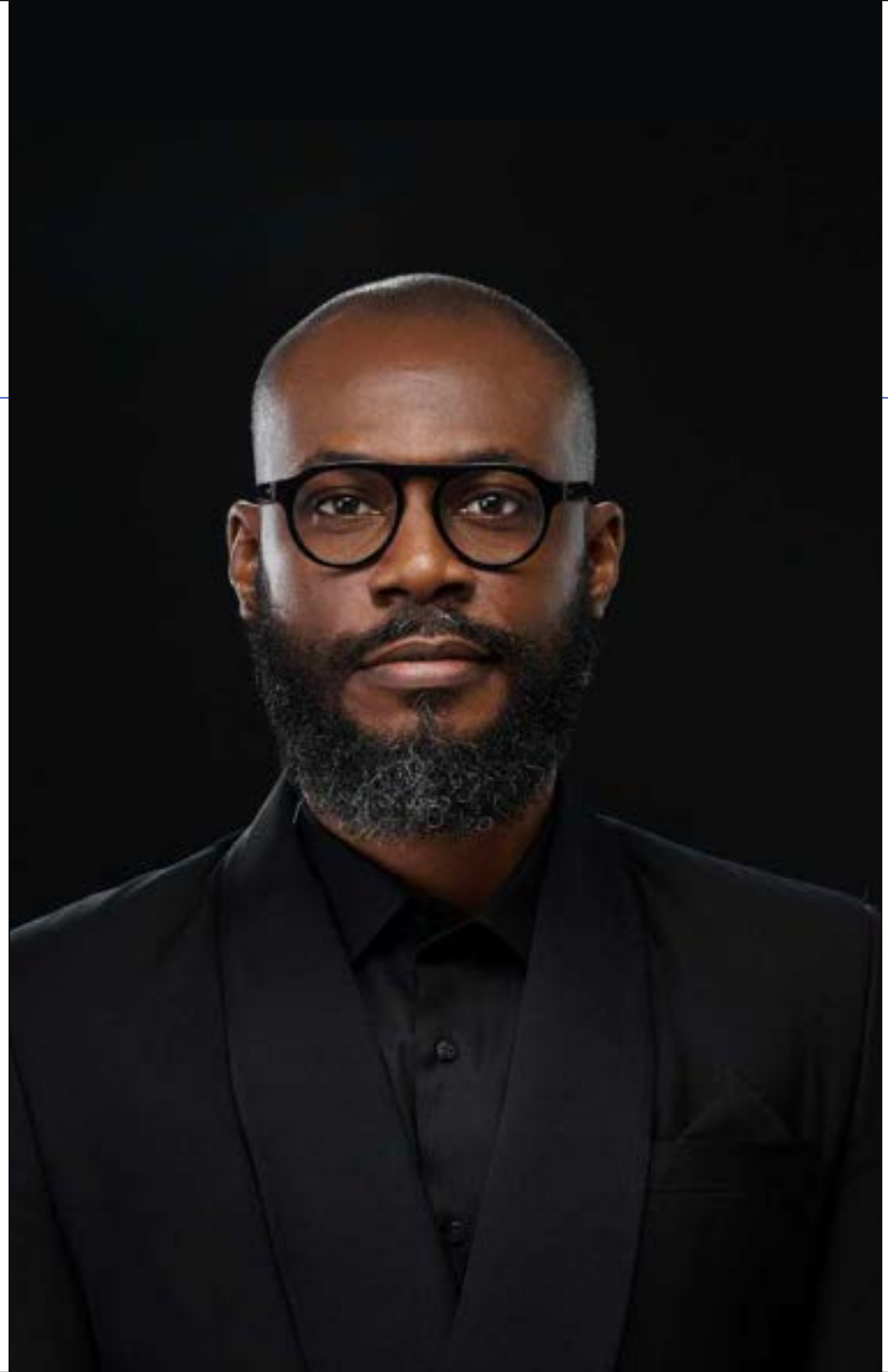
> **This is esentry. Revolutionising the African Cybersecurity Space.**

CBO NOTE

2025 was a year that tested organisations in new ways. As digital adoption across Africa accelerated, systems became more connected, operations moved faster, and decisions carried greater weight. The growing use of artificial intelligence changed how work was done and, in turn, how risk emerged.

Security challenges did not increase simply because defences were absent, but because environments became broader and more complex. Automation reduced reaction time. AI lowered the barrier for attackers and compressed the window for response. In this context, isolated efforts were not enough. What mattered most was how well teams worked together.

At esentry, this reality shaped how we operated throughout the year. Our cyber defense, threat intelligence, cyber offense, security engineering, and customer success teams worked in close coordination, with a shared understanding of responsibility. Every function played its role. Every shield mattered. No single capability stood alone.



This collective approach allowed us to respond with clarity, test what we relied on, and adjust as conditions changed. It reinforced the importance of discipline and structure in delivering security that holds under pressure.

As we move into 2026, our focus remains clear. We will continue to strengthen coordination, evolve alongside emerging technologies, especially AI, and support organisations across Africa as they build and protect digital trust. The environment will continue to change, but our commitment to collective defence remains constant.

Thank you for the trust placed in esentry.

The Threat Landscape
(Setting the Battlefield)

This is where the Phalanx faces the enemy.

The Threat Landscape

The threat landscape in 2025 reflected a clear shift in how and where cyber risk materialized across African organisations. The year was defined by intent. Threat activity showed greater focus, improved coordination, and a growing understanding of African digital environments.

As digital adoption accelerated across the continent, African organisations moved further into the global threat spotlight. Financial institutions, payment providers, lending platforms, healthcare organisations, and technology-driven service providers all experienced increased attention. This was not opportunistic activity driven by novices, but deliberate targeting by organised and experienced threat groups seeking scale, persistence, and reliable returns.

A Broader and More Deliberate Target Set

While financial institutions remained a primary focus, threat activity in 2025 extended well beyond traditional banking. Digital lending platforms, mobile-first financial services, healthcare systems holding sensitive personal data, and organisations supporting critical services increasingly featured in observed incidents.

These sectors shared common characteristics: rapid growth, high data value, operational dependency on digital platforms, and expanding third-party ecosystems. Attackers recognised these conditions and adjusted their target accordingly. The shift confirmed that cyber risk in Africa was no longer concentrated in a narrow set of institutions but distributed across sectors undergoing digital transformation.

From Breaking Systems to Exploiting Trust

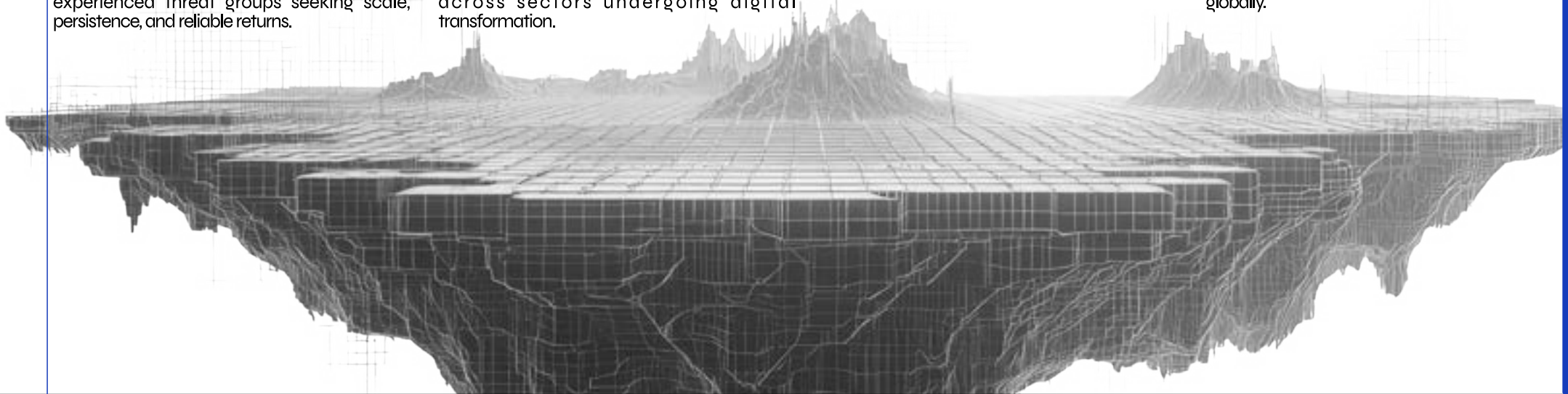
A consistent pattern observed throughout the year was the move away from overt system exploitation toward the abuse of trusted access. Many incidents occurred in environments with functional security controls in place. Attackers succeeded not by bypassing defences outright, but by operating within them.

Compromised credentials, session tokens, and legitimate access paths became central to intrusion activity. This approach reduced noise, delayed detection, and allowed malicious actions to blend into routine operations. As a result, attacks were harder to identify and often progressed further before containment.

Local Threat Actor Maturity

Another notable development in 2025 was the growing sophistication of local threat actors. Activity linked to Nigerian-based groups demonstrated improved operational discipline, deeper understanding of enterprise environments, and effective use of widely deployed platforms.

The arrest of a Nigerian threat actor in December, linked to large-scale abuse of Microsoft 365 environments, reinforced this shift. The case highlighted how cloud identity systems, collaboration tools, and trusted business platforms were increasingly central to attack operations. It also underscored that the threat landscape in Africa now includes capable actors operating both locally and globally.



Automation, AI, and Operational Pressure

Automation and artificial intelligence further altered the scale and precision of attacks. Social engineering, fraud, and impersonation campaigns became more contextual and persistent. Messages reflected local language patterns, timing aligned with business and payment cycles, and activity adapted quickly to defensive changes.

In mobile-dominated and real-time transaction environments, these tactics placed sustained pressure on detection and response capabilities. Attacks were less episodic and more continuous, turning cybersecurity into an operational challenge rather than an isolated technical concern.

Ecosystem Risk and Interconnected Exposure

As organisations deepened their reliance on fintech partners, cloud services, APIs, and third-party platforms, risk increasingly originated outside core environments. In several cases, initial access was traced to partner systems, shared infrastructure, or misconfigured integrations.

This reinforced an important reality observed in 2025: organisational security could no longer be assessed or managed in isolation. The security posture of one entity was increasingly shaped by the maturity and controls of the broader ecosystem it depended on.

Operational Impact and Resilience

Although large-scale disruptive incidents were less visible than in previous years, the operational impact of cyber incidents remained significant. Threat actors demonstrated patience, prioritising persistence and access over immediate disruption. Extended recovery timelines, service degradation, reputational damage, and regulatory scrutiny often proved more costly than the initial technical incident.

These outcomes highlighted the growing importance of operational resilience. Incident response readiness, recovery planning, and the ability to coordinate under pressure became as critical as preventive security controls.

What Changed in 2025

Compared to previous years, 2025 marked a move toward **quieter, more calculated attacks.** Threat groups were better **organised, more collaborative, and more familiar with African operating environments.** Success relied less on exploiting obvious weaknesses and more on **identifying small gaps within increasingly complex systems.**

For defenders, the lesson was clear. Effectiveness depended on coordination. Fragmented security efforts increased risk, while aligned intelligence, defence, engineering, and response reduced it.
This evolving threat environment set the conditions that shaped how esentry operated throughout the year and reinforced the need for a disciplined, coordinated approach to cybersecurity.

Cyber Defense – Holding the Line

Cyber Defense – Holding the Line

This is the front shield of the Phalanx.

In ancient warfare, the phalanx was not defined by individual strength, but by unity, discipline, and unwavering formation. Each shield protected the next, and every movement was deliberate, coordinated, and calm under pressure. Survival depended on structure, trust, and precision.

2025 marked a defining year in the maturity of Cyber Defense Operations. Threat actors demonstrated increased patience, precision, and awareness of defensive controls. In response, the esentry Cyber Defense team operated as a modern digital phalanx, anchored on disciplined execution, clarity of roles, and risk-based decision-making.
Operations were conducted under a 24/7 monitoring model that fused human analyst expertise with automation and AI. This approach strengthened speed and consistency without removing accountability. Our objective remained firm: protect the business, not merely reduce alert volumes.

Key outcomes achieved:

- Sustained availability of critical business systems
- Reduction in high-impact incidents despite increased threat activity
- Increased confidence among stakeholders in our detection and response capabilities

2025 Overview

Q1
Initial Access

- Lumma Stealer campaigns
- Browser data theft
- Credential harvesting
- Persistence establishment

Q2
Escalation Phase

- Ransomware attempts
- Behaviour-based DDoS
- Service disruption
- Lateral movement tactics

Q3
Credential Exploitation

- Valid account abuse
- Insider-related activity
- Targeted ransomware
- Living-off-the-land techniques

Q4
Social Engineering

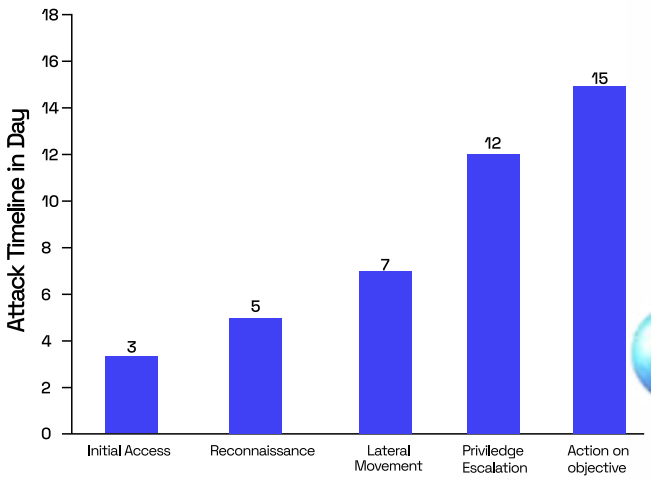
- ClickFix-style campaigns
- Account compromise
- User interaction exploits
- Awareness-based attacks

Critical Finding:

<15Days

Analysis of observed incidents over the reporting period revealed a consistently compressed attack timeline, with threat actors progressing from initial access to operational impact in fewer than 15 days.

Attach Progression Timeline (Days)



As illustrated in the attack progression timeline, adversaries moved rapidly through reconnaissance, lateral movement, and privilege escalation, leaving a narrow window for detection before objectives were achieved.

To address this challenge, structured threat hunting was implemented as a core security control. Operating independently of traditional alert-driven workflows, threat hunting enabled the team to proactively identify malicious activity that evaded automated detection and disrupt attacker progression earlier in the kill chain.

This approach has delivered four key advantages:

Visibility Beyond Automated Detection

Identified valid credential abuse, living- off-the-land techniques, and reconnaissance activity that generated no security alerts.

Proactive Timeline Advantage

Detected intrusions during reconnaissance phase, disrupting attacks before lateral movement or data exfiltration.

Intelligence Generation

Each hunt produced actionable insights, strengthening detection rules and response playbooks with real-world adversary behaviors.

Enterprise-Scale Defense

Systematically examined high-risk areas across complex hybrid environments where sophisticated adversaries operate.

Together, these reinforced a proactive, intelligence-driven approach to security shifting the SOC from a reactive posture to one capable of anticipating and disrupting threats before they could escalate.

By combining structured threat hunting with targeted automation and deep visibility, the team not only reduced attacker dwell time but also strengthened overall situational awareness, ensuring that defenses remained adaptive, resilient, and aligned with the unique risks faced across the enterprise.

The SOC Dashboard

Security Operations Center Overview

All system Operational

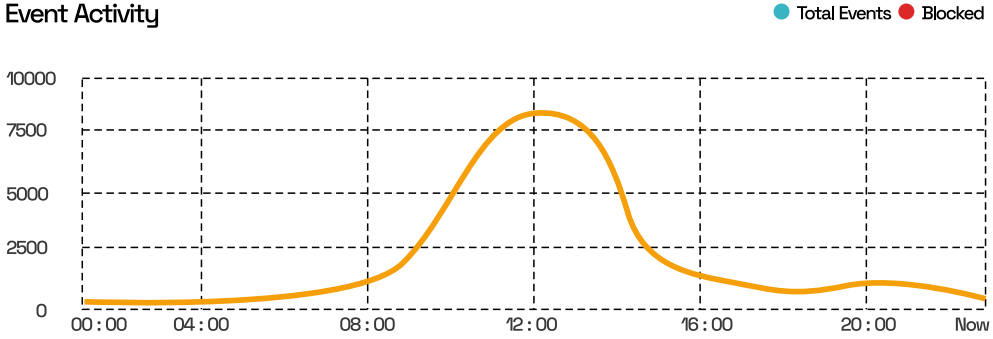
3

Search

- Dashboard
- Threat Intel
- Alerts
- Monitoring
- Reports
- Settings

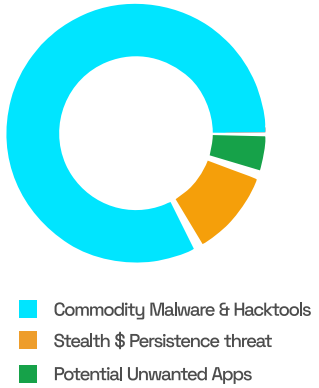
15k+	3.5M+	31B+	6	4
BLOCKED ATTEMPTS	ALERTS GENERATED	EVENT PROCESSED	DFIR CASES	SECTORS AFFECTED

Event Activity



EDR Telemetry Detection

Reputation and Behavioral Analysis



Recent Alerts

1 Active

ID	TYPE	SOURCE	SEVERITY	TIME	STATUS
ALT - 001	Malware Detected	Endpoint-WS-047	SEVERITY	2 min ago	Active
ALT - 002	suspicious login	Auth-server-02	high	15 min ago	investigating

Business-Impact-Driven Incident Handling: Protecting What Matters Most
2025 DFIR Incident Review: Protecting Critical Operations

Throughout 2025, the SOC responded to six significant attacks across key sectors, including Telecommunications, Financial Services, Health Care, and Logistics.

What stood out during these incidents was not simply the volume of alerts, but the speed, sophistication, and diversity of techniques used by the attackers.

Each incident was approached with a business-impact-driven mindset, assessing potential operational disruption, trust erosion, and sensitive data exposure to prioritize response actions.

The SOC's proactive and deliberate approach ensured that resources were focused on what truly mattered, enabling containment and mitigation while maintaining business continuity across affected sectors.

Sector	Initial Access Vector	Primary Threat	Key Techniques Observed	Containment & DFIR Actions	Business Impact
Telecommunications	Phishing Email	Credential Harvesting	Credential theft, mailbox access, account misuse	Account isolation, forced password reset, email rule cleanup	Moderate
Telecommunications	Exposed Web Service	RCE	Unauthorized script execution, persistence via startup tasks	Application cleanup, endpoint hardening, service access review	Moderate
Financial Services	Malicious Email Attachment	Infostealer	Credential harvesting, browser data exfiltration	Endpoint isolation, IOC-based hunting, credential resets	High
Financial Services	Misuse of Valid Credentials	Insider Threat	Unauthorized access, privilege misuse, lateral movement	Access revocation, audit review, privilege restriction	High
Health Care	Exposed RDP Service	Ransomware	Network exploitation, password dumping, service creation	Immediate isolation, validation of critical services	Critical
Logistics	Malicious Web Download	PUA	External reconnaissance, persistence mechanisms	Endpoint remediation, application control enforcement	Moderate

Incident Case : Healthcare Ransomware Deployment

Attack Timeline and Technical Analysis
Phase 1: Initial Access & Persistence

Weakness Exploited: Inadequate network segmentation and monitoring

What the SOC Saw First

The threat actors gained initial access through compromised credentials and quickly deployed a Remote Monitoring and Management agent immediately after establishing RDP access. This confirmed intent to persist, not just explore.

Observed RMM Deployment Commands:

```
RMM Agent Installation (chrome remote desktop variant observed)
msiexec.exe /I [redacted].msi"/quiet/norestart ADDLOCAL=ALL
Persistence via Scheduled Task
msi" /quiet /norestart ADDLOCAL-ALL
schtask/create /tn [redacted]" /tr
"C:\ [redacted]/ [redacted] /[redacted].exe" /sc onstart/ru SYSTEM
```

The Story Behind the Installation

It started like any routine alert in the Security Operations Center, but something subtle caught the analyst's eye. msiexec.exe a legitimate Windows installer was running, but unusually, it executed with the flags /quiet /norestart and ADDLOCAL=ALL. There were no pop-ups, no user prompts, just silent execution installing all components. At first glance, it looked like a standard IT deployment, but something didn't sit right.

The MSI-based deployment suggested the use of commercial or enterprise-grade tooling, not a typical malware dropper. This wasn't accidental; it was precise and intentional.
Digging deeper, the team realized the attackers had deliberately chosen this trusted remote access tool to achieve multiple objectives:

- **Evade detection:** The use of a legitimate installer allowed it to bypass AV and EDR signatures.
- Blend in: By mimicking normal administrative activity, the operation stayed under the radar.
- Maintain control: The tool enabled persistent, long-term remote access to the environment.

Discovery & Reconnaissance

```
Network Discovery

net view /all/domain
net view \\[redacted]-[redacted]-[redacted]01
nltest /domain_trusts

Active Directory Enumeration

net group "Domain Admins" /domain
net group "Enterprise Admins" /domain
net group [redacted] [redacted] " /domain
net localgroup administrators

Domain Controller Identification
nltest /dclist: [redacted] [redacted].local
set logonserver echo %logonserver%

System Information Gathering
systeminfo | findstr /B /C:"Domain"
wmic computersystem get domain

User and Session Enumeration
query user net user /domain
net user /domain | findstr /I " [redacted] [redacted] [redacted]
```

Discovery & Reconnaissance Activity

During the investigation, the SOC noticed a sequence of commands indicative of reconnaissance within the network. The attackers were methodically mapping the environment and gathering intelligence on user privileges, domain controllers, and system configurations.

Network Discovery:

The attackers used commands like net view /all /domain and net view \\<host> to enumerate available hosts and shares. Additionally, nltest /domain_trusts was leveraged to identify trusted domains, providing insight into potential lateral movement paths.

Active Directory Enumeration:

Commands such as net group "Domain Admins" /domain and net group "Enterprise Admins" /domain were executed to enumerate high-privilege groups. This allowed the attackers to identify accounts with administrative rights that could be targeted for privilege escalation.

Domain Controller Identification:

Using tools like nltest /dclist:<domain> and echo %logonserver%, the attackers identified the primary domain controllers within the environment key targets for further compromise and persistence.

System Information Gathering:

The attackers gathered system-level information with commands like systeminfo, findstr /B /C:"Domain", and wmic computersystem get domain. This provided a detailed view of host configuration and domain membership, aiding in lateral movement planning.

User and Session Enumeration:

Finally, the attackers enumerated user accounts and sessions using query user /domain and net user /domain | findstr /i "<username>". This step allowed them to identify active users, their privileges, and potential targets for compromise.

The observed activity reflected a controlled and intentional reconnaissance phase conducted after initial compromise. The sequence and timing indicated that the attacker had already achieved sufficient access and was now focused on understanding the environment well enough to operate at scale.
Rather than exhibiting exploratory or opportunistic behavior, the actions demonstrated a clear effort to reduce operational risk before advancing the intrusion.

The attacker prioritized situational awareness of the domain structure, privilege boundaries, and control points that would influence the success of subsequent attack stages.

This phase materially increased the attacker's confidence in navigating the environment. By establishing clarity around where administrative control could be obtained and how systems were interconnected, positioning themselves to move laterally with precision, avoiding unnecessary exposure, and target assets capable of amplifying impact.
From the investigation, the absence of disruptive or overtly malicious actions during this stage indicated that the attacker was operating with a broader objective in mind rather than pursuing immediate exploitation. This level of restraint shows a deliberate and disciplined approach, typically associated with intrusions aimed at large-scale disruption or financial monetization, rather than opportunistic data theft.

Our analysis also determined that this activity did not trigger effective security intervention. The reconnaissance activity closely resembled legitimate administrative behavior, allowing the attacker to complete environmental mapping without interruption. As a result, the attacker was able to significantly reduce the effort required for subsequent privilege escalation and to position the environment for coordinated deployment of malicious payloads in later phases of the attack.

These activities are consistent with postcompromise reconnaissance commonly associated with ransomware operations, where attackers map the environment prior to lateral movement and privilege escalation. The scope and sequence of the enumeration suggest intent to identify critical assets, privileged users, and potential propagation paths to maximize impact. This behavior significantly increased the attacker's ability to deploy ransomware across multiple systems and highlights a failure in early detection of anomalous administrative command usage within the domain.

Key Observations from DFIR Operations

Attackers used a variety of initial access methods, from phishing emails and exposed RDP endpoints to compromised third-party services.

Techniques included both common tools and sophisticated methods, such as credential harvesting, lateral SMB movement, API abuse, registry persistence, and WMI-based persistence.

The business impact ranged from moderate to critical, highlighting the importance of prioritizing incidents based on operational relevance rather than technical severity alone.

Rapid containment, endpoint isolation, and verification of critical operations were essential to maintain continuity and minimize disruption.

Lessons Learned and Public Guidance

- Proactive threat hunting and continuous monitoring are essential to detect attackers using legitimate tools and credentials
- Business-context awareness allowed the SOC to prioritize threats and allocate resources effectively.
- ·Stakeholder communication during active incidents is as critical as technical mitigation, helping maintain trust and operational stability.
- ·Public cybersecurity advice includes maintaining strong credentials, enabling multi-factor authentication, monitoring unusual activity, training personnel on phishing risks, and preparing legitimate tool abuse.

Threat Intelligence – Seeing Beyond the Shield

Threat Intelligence – Seeing Beyond the Shield

This is the eyes and foresight of the Phalanx

In 2025, the Threat Intelligence team provided early visibility into how adversaries were operating, where they were shifting, and what that meant for organizations across Africa. By maintaining sustained awareness of threat actor activity and tracking changes within underground ecosystems, the team translated fragmented signals into clear, actionable intelligence that guided defensive posture, informed strategic decisions, and strengthened coordination across the organization.

This intelligence function served as the forward view of the formation, ensuring decisions were based not on assumptions or headlines, but on what was actively unfolding in the threat environment.

Threat Vector Highlights

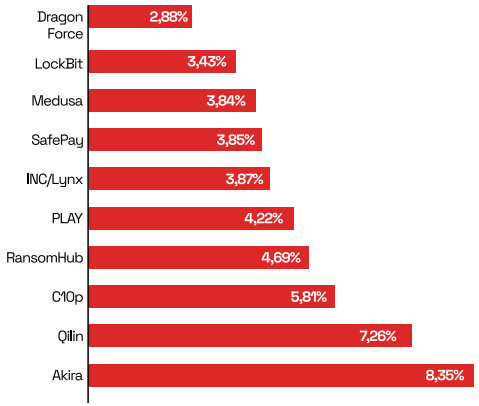
Threat Vector	Key Characteristics	Evolution in 2025
Phishing & SocialEngineering	AI-generated content (80% of attacks) •Phishing-as-a-Serviceplatforms •Multi-channel (email,Teams, SMS)	Hyper-personalized using LLMs;ClickFix and device code phishing emerged

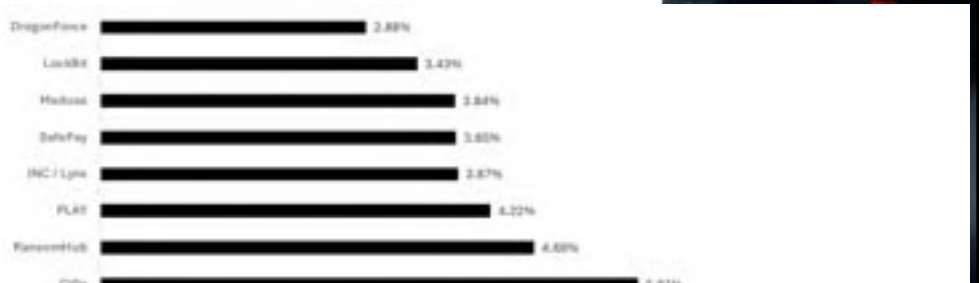
Threat Vector	Key Characteristics	Evolution in 2025
Ransomware	Median demand: $115,000 •64% refused to pay •Avg cost: $5.08M (withoutpayment)	Ransomware-as-a-Service (RaaS); targeting hybrid cloud; exfiltration-firststrategies

Threat Vector	Key Characteristics	Evolution in 2025
Vulnerability Exploitation	Weaponization within days of disclosure •Web-facing applicationsprimary target	75 zero-days in 2024; rapid exploitation cycle

Threat Vector	Key Characteristics	Evolution in 2025
Identity-BasedAttacks	Token theft bypassing MFA •Oauth abuse •Workload identity targeting	Shift from credentials to session tokens; targeting machine identities

Threat Vector	Key Characteristics	Evolution in 2025
Supply Chain Compromises	•Third-party software vulnerabilities •Malicious browser extensions •Open-source repositorypoisoning	Coordinated campaigns; ecosystem-wide propagation





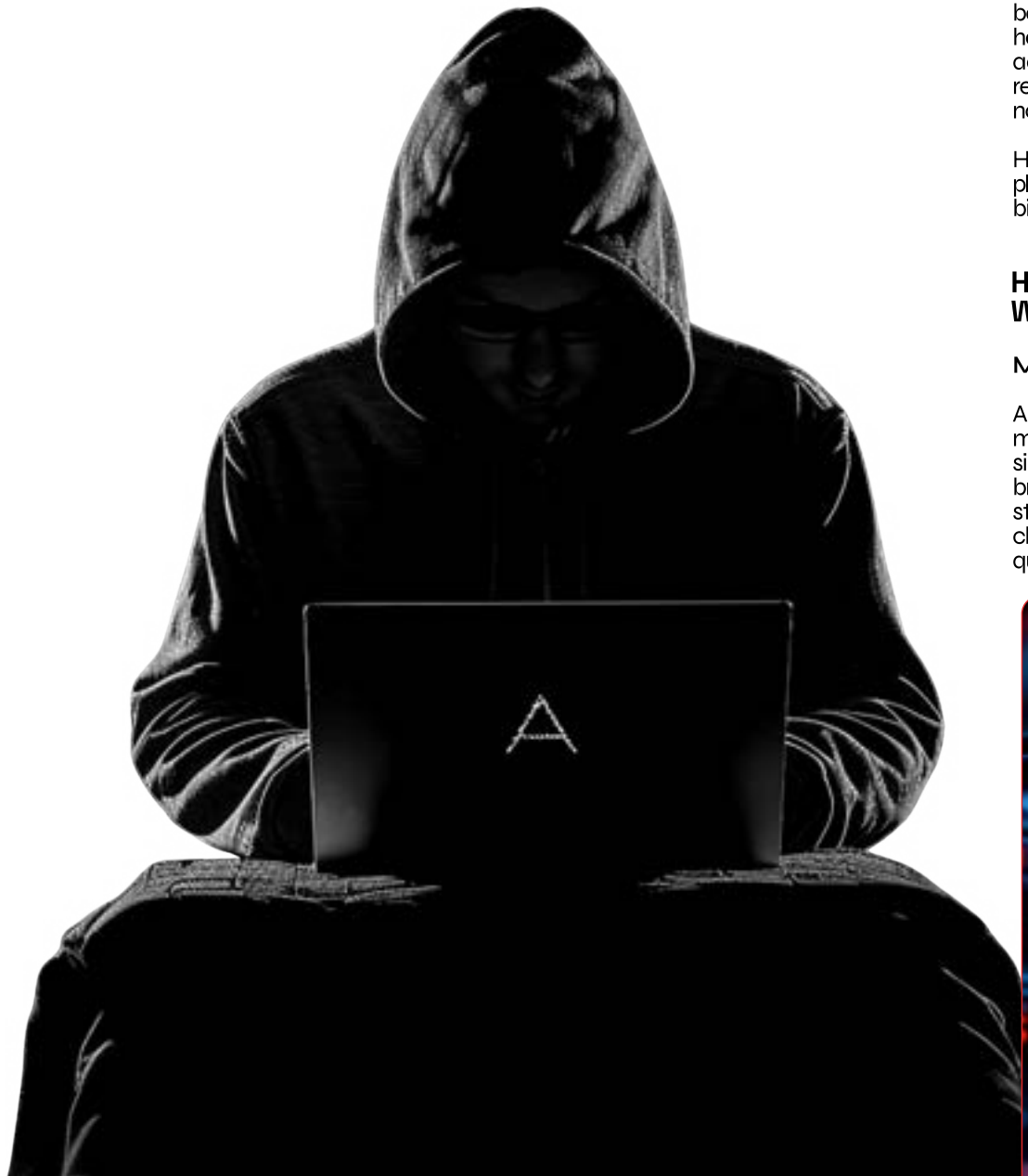
A Sneak into the Dark Web

Public administration was the most exposed sector on the Dark Web at 12.85%, ascending from third place in 2024. Ransomware activity during the reporting period remained highly fragmented, with no single group maintaining long-term dominance. Instead, the landscape continues to reflect a competitive criminal economy, where multiple actors operate simultaneously, adapt quickly, and capitalize on shifting opportunities.

Akira emerged as the most active ransomware group in this period, accounting for 8.35% of observed activity. Its sustained presence suggests operational maturity and consistent access to victims, rather than reliance on short-lived campaigns. Closely following is Qilin (7.26%), which continued to expand its footprint, indicating growing confidence and possible recruitment of new affiliates.

Mid-tier actors such as Clop (5.81%), RansomHub (4.69%), and PLAY (4.22%) collectively represent a significant portion of activity. These groups demonstrate a recurring pattern seen across the ransomware ecosystem: rapid adaptation, aggressive monetization strategies, and a willingness to change tools and tactics to remain relevant.

The remaining share is distributed across actors including INC/Lynx, SafePay, Medusa, LockBit, and DragonForce, each contributing between 2.88% and 3.87%. While individually smaller, these groups collectively reinforce a critical insight risk does not concentrate around a single threat actor. Instead, organizations face exposure from a broad pool of capable adversaries operating at varying levels of sophistication



Major Breaches & Incidents in 2025

By 2025, cyber breaches stopped being background noise and started reading like headlines you couldn't ignore. They unfolded across sectors and countries, each one reinforcing the same truth: compromise was no longer easy to hide.

Here's how the year's most visible breaches played out, listed clearly, but woven into the bigger story they collectively tell.

Healthcare: When Patient Trust Was the First Casualty

M-TIBA (Kenya)

A health-tech platform holding sensitive medical and insurance records saw its data siphoned and published on Telegram. The breach was significant not just for what was stolen, but for where it appeared, open channels designed for maximum visibility, not quiet monetization.

Telecommunications: Prime Targets, Public Fallout

Cell C (South Africa)

Customer data surfaced on dark-web leak sites, attributed to the **RansomHouse** extortion group. This followed the now-familiar playbook: **steal first, publish fast, pressure publicly.**

MTN Group (South Africa & Ghana)

Breaches affecting tens of thousands of subscribers forced cross-border disclosures and regulatory scrutiny. Telecom infrastructure once quietly monitored was now openly exposed.

Telecom Namibia

After refusing to pay ransom, attackers leaked billing data linked to government officials. What began as a cyber incident quickly escalated into a political and reputational crisis.

Critical I: Digital Attacks, Physical Consequences

South African Weather Service (SAWS)

Systems were knocked offline, disrupting aviation and maritime forecasts. This wasn't about data theft it was about real-world operational impact.

Municipal Systems in Otjiwarongo (Namibia)

Local government services were taken offline mid-year, reinforcing how cyberattacks increasingly affect citizens directly.

Eskom Online Vending System (South Africa)

A breach tied to fraud rather than ransomware enabled the generation of illegitimate electricity tokens, reportedly costing the utility billions. It showed how cybercrime is evolving beyond encryption and extortion into systemic abuse.

Regulatory & Enforcement Responses

Reporting Rules Toughened

Several African countries tightened breach notification requirements, forcing organizations to disclose and detail cyber incidents within strict windows including Algeria's 5-day rule, Kenya's 48–72-hour reporting timeline, and South Africa's online breach-log submission process.

Law Enforcement Actions

INTERPOL coordinated arrests of 1,209 cybercriminals across 18 African countries, a major pan-regional effort against organized cybercrime.

Fines & Penalties

Nigeria's Data Protection Commission fined MultiChoice ₦766 million (≈ $528 000) for inadequate data protection signaling stricter regulatory enforcement.

What These Breaches Tell Us

- Exposure became the strategy, not the by-product
- Critical services joined the target list, not just data-rich enterprises
- Public disclosure replaced quiet containment
- Regulatory pressure and arrests closed the gap between cybercrime and consequence

Critical Vulnerabilities

CVE	Vulnerability	Impact	African Context
CVE-2025-53770, CVE-2025-53771	Microsoft SharePoint RCE	Web shells, persistence, lateral movement	Nigerian government parastatals, banks running outdated SharePoint
CVE-2025-53786	Microsoft Exchange Hybrid Privilege Escalation	Mailbox access, exfiltration	Nigerian fintechs, Ghanaian payment processors (BEC-style compromises)
CVE-2025-20333, CVE-2025-20362	Cisco Firewalls	Unauthenticated RCE (~50K devices vulnerable)	Many unpatched despite available patches
CVE-2024-20376	Cisco IOS / IOS-XE SNMP	Unauthenticated remote DoS/RCE	ISPs, telecoms, critical infrastructure

CVE	Vulnerability	Severity	Impact
CVE-2025-49827	CyberArk IAM authenticator bypass	CVSS 9.1	Cloud providers, DevOps, SaaS, financial services
CVE-2025-49828	CyberArk RCE	High	Secrets management compromise
CVE-2025-6000	HashiCorp Vault Plugin-catalog RCE	CVSS 9.1	DevOps pipelines, CI/CD
CVE-2025-5999	HashiCorp Vault Privilege Escalation	High	Vault infrastructure compromise
CVE-2025-61882	Oracle E-Business Suite	Critical	CIOp ransomware exploitation; data exfiltration, ransom
CVE-2025-42957	SAP S/4HANA	Critical	Full system control; manufacturing, supply chain, retail, finance

Throughout 2025, threat intelligence matured beyond the collection of isolated indicators. Intelligence efforts increasingly centred on verified victim disclosures, attacker behaviour patterns, and the measurable impact of incidents across organisations and sectors. This shift provided clearer insight into how extortion models evolved, how attacks against critical services intensified, and how data exposure itself became a primary instrument of pressure.

What emerged over the year was a connected threat environment. Breaches were rarely standalone events; they were part of coordinated campaigns that moved across industries, regions, and digital ecosystems. Understanding these linkages allowed intelligence to move from retrospective reporting to proactive guidance, strengthening preparedness, and decision-making across the organization.

As 2025 closed, these insights reinforced the need for intelligence that is continuous, contextual, and closely integrated with defensive and strategic functions — a foundation that will remain critical as the threat landscape continues to accelerate into 2026.


Cyber Offense –
Testing the Formation

Cyber Offense – Testing the Formation

Purposeful Testing in Real Environments

Cyber Offense exists to challenge assumptions. In 2025, the team focused on simulating real-world attack behaviour across client environments to identify weaknesses that could not be detected through passive monitoring alone.

Rather than testing isolated controls, engagements were designed to mirror how capable threat actors operate in practice. This meant chaining weaknesses, abusing trust relationships, and moving deliberately through systems to understand how attacks would realistically unfold.
Each engagement was conducted with a clear objective: reveal how attackers could gain access, remain undetected, and expand their reach if left unchallenged.

Scope of Engagements

Cyber Offense operations in 2025 spanned multiple sectors and high-value systems, including:

- Investment and financial web platforms handling sensitive transactions
- Internal enterprise applications within major financial institutions
- External web applications supporting payment switching and interconnectivity
- Messaging-integrated payment and transaction platforms

While many of these environments appeared secure at first glance, testing consistently showed that attackers do not experience systems the way architecture diagrams suggest. Security weaknesses often emerged at the intersections between applications, identity systems, and business logic.

What Testing Revealed

Across engagements, recurring patterns emerged. Vulnerabilities were rarely isolated issues. Instead, they formed attack paths when combined with trust assumptions, legacy components, or overly permissive access.

In one engagement, authentication mechanisms relied heavily on assumptions about client behaviour. By carefully replaying requests and adjusting execution timing, it became clear that trust, rather than cryptographic strength, was the weakest link. Addressing that single issue required changes across multiple teams and workflows.

This pattern was repeated across environments: small gaps, when chained together, created meaningful exposure.

Key Offensive Findings and Outcomes

The table below summarises representative findings from 2025 engagements and the defensive outcomes they enabled.

Cyber Offense Findings and Defensive Impact

Offensive Finding	What Was Demonstrated	Defensive Outcome
OTP flow weakness	Potential account takeover through authentication abuse	Bank-wide redesign of OTP and authentication policies
Legacy component exploitation	Remote code execution risk via outdated libraries	CI/CD hardening and legacy component patching
Session chaining and credential reuse	Account takeover and lateral movement	MFA enforcement and session management controls
Insecure cross-origin trust	Unauthorised data submission via external pages	Strict origin validation and request filtering

These findings were not theoretical. Each was demonstrated in controlled conditions to show real impact, allowing remediation efforts to focus on controls that materially reduced risk.

Measured Impact

While individual client details remain confidential, the outcomes of Cyber Offense activity were clear:

- Attack paths identified and eliminated
- Control gaps closed across multiple environments
- Faster detection and containment during real incidents
- Reduced recurrence of previously observed weaknesses
-

Each engagement shortened the feedback loop between testing and improvement, strengthening resilience over time.

Looking Ahead

As attacker techniques continue to evolve, Cyber Offense will remain focused on learning faster than adversaries. The goal is not disruption for its own sake, but insight that informs stronger design, better detection, and more confident response.

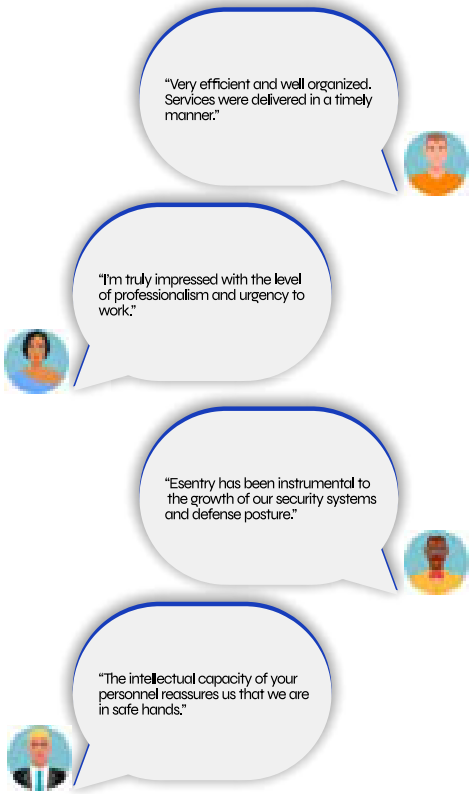
By deliberately testing assumptions and exposing how systems behave under pressure, Cyber Offense ensures organisations are prepared not for hypothetical threats, but for the realities of modern attack behaviour.

Customer Success – The Center of the Phalanx

Customer Success – The Center of the Phalanx

Where security execution becomes customer confidence.

What Our Customers Told Us in 2025



These voices reflect a consistent experience across engagements : one defined by clarity, reliability, and trust.

Turning Technical Security Into Trust

Customer Success sits at the center of esentry's operations, ensuring that technical security work consistently translates into confidence for our customers.

Acting as the bridge between customers, technical teams, and leadership, the team ensures clear communication, timely updates, and active risk management ,both during routine operations and high-pressure incidents.By aligning security outcomes with business priorities, Customer Success enables informed decision-making, operational continuity, and long-term trust.

Customer Satisfaction Snapshot (January – December 2025)

CSAT Performance

Q1: 100%	Q2: 98%
Q3: 95%	Year-end average: ~90%

Customer Advocacy

Net Promoter Score increased from 65 (Q1) to 73 (Q4)

Engagement Effectiveness

- 90% of customer queries resolved within agreed timelines
- Sustained confidence despite increased operational complexity

In 2025, Customer Success evolved beyond service delivery into a strategic trust function,focused on strengthening long-term resilience rather than short-term fixes.

Security Engineering

Security Engineering

From Insight to Resilient Architecture

Security Engineering is where foresight becomes structure. In 2025, the focus shifted from deploying more tools to strengthening how environments were designed, connected, and controlled.

Across multiple client environments, a recurring pattern emerged. Security challenges were rarely caused by the absence of controls, but by complexity. Overlapping tools created blind spots. Excessive alerts masked real threats. Identity and access controls often extended beyond their intended purpose.

As adversaries became more deliberate and patient, these weaknesses were increasingly exploited. The role of the Security Engineering team throughout the year was to simplify, harden, and align security architectures so that defenses worked together rather than in isolation.

Identity and Insider Risk in Focus

One of the most persistent challenges observed in 2025 was insider-related risk. In many cases, this did not involve malicious intent, but access that outlived its relevance.

Broad administrative privileges were retained after role changes. Dormant accounts remained active. Third-party vendors held persistent access beyond operational necessity. These conditions created silent but significant exposure.

The team addressed this through architectural controls rather than reactive fixes. Periodic access reviews reduce excessive privileges. Dormant accounts were identified and removed through continuous monitoring. Vendor access was redesigned using segmented network architecture, ensuring access was limited strictly to required systems. In one instance, compromised vendor credentials enabled lateral movement across a flat network. Architectural reviews identified the exposure early, and segmentation controls were implemented to contain and prevent recurrence.

Visibility Where It Matters

Several incidents reinforced the importance of unified visibility. Sensitive data was observed leaving environments through legitimate channels such as email, bypassing traditional perimeter controls. In another case, an employee attempted to install unapproved software containing hidden malware.

These events were contained not through reactive response alone, but through prior engineering decisions. Centralised telemetry across endpoints, cloud platforms, and network layers provided full visibility across the attack chain. Application control policies prevented unauthorised execution, while contextual monitoring ensured activity that appeared legitimate in isolation was flagged as risky.

Reducing Noise, Strengthening Detection

Many environments entered 2025 overwhelmed by alert volume. Thousands of alerts were generated daily, diluting analyst focus and delaying response.

The team addressed this through deliberate SIEM optimisation. Detection logic was refined, correlation rules were tuned, and alert thresholds were aligned to observed threat behaviour rather than generic severity scores. User and Entity Behaviour Analytics (UEBA) rules surfaced identity misuse and insider anomalies more effectively.

Building Defense in Depth

Engineering efforts followed a defense-in-depth approach, ensuring no single control carried the burden alone. Layered mechanisms were implemented across identity, network access, detection, and response.
Key initiatives included:

- Refinement of Managed Detection and Response (MDR) architectures to support scale
- Elimination of legacy authentication protocols and enforcement of continuous verification
- Re-architecture of privileged access using just-in-time workflows
- Rationalisation of overlapping security tools to improve clarity and efficiency
- Centralised telemetry providing end-to-end visibility across environments
-

In one client environment, ten overlapping security tools were consolidated into six purpose-built solutions, reducing operational overhead while improving detection and response speed.

Speed Through Intentional Automation

Automation supported consistency and speed throughout 2025. SOAR playbooks were implemented for routine incidents such as phishing, policy violations, and known indicators of compromise.

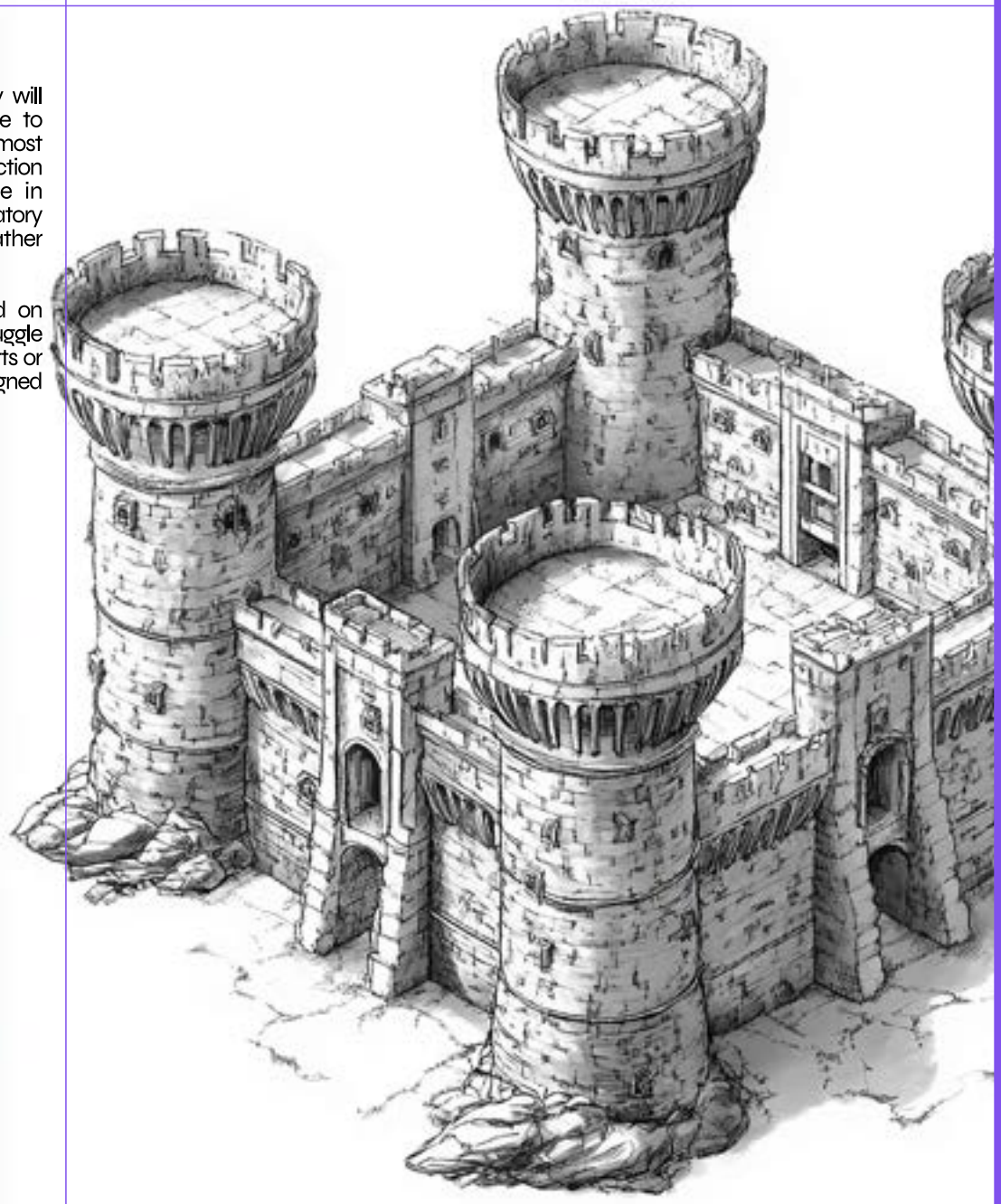
Automated containment and documentation reduced response time for low-complexity incidents from an average of 45 minutes to under 90 seconds. Analysts recovered hundreds of hours each quarter, redirecting effort toward complex investigations and threat analysis.

Automation enhances decision-making. It did not replace it.

Looking Ahead to 2026

As organisations move into 2026, security will continue to shift from reactive response to intentional design. Identity will remain the most targeted attack surface. AI-driven detection and response will play a greater role in managing scale and complexity. Regulatory requirements will shape architecture rather than sit alongside it.

Security Engineering will remain focused on building environments where attacks struggle to gain traction, not because of louder alerts or more tools, but because systems are designed to anticipate and absorb pressure.



Emerging Threats 2026

We're past the point of incremental change. The cyber threat landscape has fundamentally restructured itself. After tracking this acceleration through 2024 and 2025, what we're seeing now isn't just , is different. In kind, and not just degree.

The adversaries we're tracking have figured something out that many defenders haven't: you don't need to be bigger or better funded to win. You need to be faster, more distributed, and willing to burn everything down if the economics don't work out. They've industrialized their operations while simultaneously decentralizing their infrastructure. They're using our own AI tools against us while we're still figuring out governance policies.

This is what we're seeing in the data, in the incidents we're responding to, and in the conversations we're having with organizations struggling to stay ahead of the curve.

What Changed Between 2024 and 2025

Amazon reported blocking roughly 100 million potential threats per day at the start of 2024, a figure that surged to about 750 million daily by mid-year, signaling a rapid escalation in automated and high-volume attack activity. Ransomware groups that carried out only five major attacks annually a decade ago were now executing 20–25 attacks per day, contributing to approximately 3,100 reported ransomware incidents in 2024. DDoS attacks rose by 46%, reinforcing the pattern of sustained compounding growth rather than isolated spikes.

The upward trajectory intensified even further in 2025. Between January and September, 4,701 confirmed ransomware incidents were tracked, a 34% increase compared to the same period in 2024. By October, the number of victim organizations exposed on dark-web leak sites climbed to 6,330, representing a 47% year-over-year surge. The momentum continued into November, which alone recorded 727 attacks, marking a 22% increase over the previous year. Measured together, these figures show a progression between attack waves and their high success volume rates each year.

The financial impact closely mirrors this operational trend. The average cost of a data breach reached $4.88 million in 2024, a 10% from 2023, while average ransomware payments quintupled to approximately $2 million per incident. As both attack frequency and success rates rise in parallel, analysts now project that cybercrime will cost the global economy $10.5 trillion annually, effectively positioning it as the world's third-largest economy. As attack scale and velocity increase, economic damage escalates at an equally aggressive pace.

Why 2026 Is Different

Every year, someone publishes a report saying, "this will be the worst year for cyber threats yet." Usually, they're right by default; things have been getting worse for a long time. But 2026 represents something more specific than just another bad year.

The attackers have systematized their approach. They operate without centralized leadership structures that law enforcement can dismantle. They scale using artificial intelligence that doesn't get tired, doesn't make mistakes, and learns faster than human defenders. They've built economic models that survive even when major operations get disrupted. And they've learned to blend criminal, geopolitical, and economic motives in ways that make attribution nearly meaningless.

Meanwhile, defenders are dealing with tool sprawl, chronic skills shortages, expanding attack surfaces across cloud and identity environments, increasingly complex supply chains, and regulatory requirements that often lag behind the threats they're meant to address.

Five Threat Predictions for 2026

Prediction One: The Ransomware Business Model Is Breaking (And That Makes It More Dangerous)

Here's the counterintuitive part: ransomware is becoming less profitable for attackers. Payment rates have dropped sharply. Organizations are refusing to negotiate. Backup and recovery capabilities have matured. Insurance companies are getting smarter about what they'll cover. Law enforcement operations continue fragmenting the major syndicates.
So attackers are adapting.

In 2026, ransomware operations will start with compromised credentials, not malware. They'll buy initial access from brokers rather than conduct their own reconnaissance. They'll use AI to select victims based on likelihood of payment and operational vulnerability. They'll move faster, reducing dwell time from weeks to days or even hours. And critically, they'll prioritize maximum disruption over clean encryption and recovery.

What this means in practice: many victims won't even be offered a chance to recover quietly. The goal is to be leverage through chaos, not negotiated settlement.

Operations will be designed to cause immediate, visible damage that forces a response before defenders can even assess what's happened.

This model is more dangerous precisely because it's less economically rational. When attackers have less to lose, they're willing to cause more damage. When they're not planning for long-term reputation management, they'll burn bridges and scorched earth becomes the default.

Prediction Two: Identity Infrastructure Is Collapsing Under Its Own Complexity

If there's one single point of failure that defines 2026, it's identity.

Modern organizations run on cloud identities, single sign-on platforms, API credentials, automated service accounts, and third-party integrations. Non-human identities already vastly outnumber human users in most environments. Credentials from historic breaches continue circulating in underground markets. Social engineering bypasses even well-implemented technical controls. MFA fatigue and helpdesk impersonation remain embarrassingly effective.

The result: attacks increasingly look like normal activity. Logs show legitimate access. Security teams can't distinguish abuse from authorized usage. The line between insider threat and external compromise becomes meaningless.
In 2026, most major breaches will begin with valid credentials. Not stolen through malware. Not cracked through brute force. Just... valid. Obtained through phishing, purchased from brokers, extracted from legacy breaches, or socially engineered from helpdesk staff.

We're not ready for this. Most organizations still treat authentication as a binary state you're either authenticated or you're not. But in 2026, that model fails completely. Continuous authentication, behavioural analysis, risk-based access controls; these aren't optional anymore.

Prediction Three: AI Becomes the Battleground (And Everyone Loses Data in the Process)

Let's separate the AI hype from what's actually happening.

On the defensive side, we're finally seeing operationally meaningful deployments. Real-time behavioral detection is replacing static signatures. Automated triage and response systems are reducing dwell time. AI-assisted SOC operations are helping us scale limited human talent. Organizations with mature AI-driven security programs are showing consistently faster containment, lower breach costs, and reduced operational downtime.

But attackers have the same tools. They're generating flawless phishing messages in any language. They're cloning voices and writing styles with frightening accuracy. They're automating negotiation and extortion communications. They're building malware that adapts its behaviour dynamically to evade detection. They're training models to mimic legitimate user behaviour.

The bigger risk, though, might be self-inflicted. Organizations are uploading sensitive data into public AI platforms. They're deploying AI tools without governance frameworks. They're training models on proprietary information without understanding where that data goes or how it gets reused. They're creating shadow AI infrastructure that security teams don't even know exists.

In 2026, many significant data breaches won't involve hackers at all. They'll be the result of employees using AI tools in ways that seemed convenient at the time but that fundamentally misunderstood the data handling implications.

Prediction Four: Supply Chain Compromise Becomes the Primary Attack Vector

Direct attacks on hardened targets are becoming less cost-effective for sophisticated adversaries. So, they're pivoting.

Instead of attacking you, they attack your software vendors. Your managed service providers. Your cloud platforms. Your SaaS integrations. Your open-source dependencies. This strategy offers broader reach, lower effort, higher impact, and significantly reduced detection risk.

You'll be breached without being directly attacked. You'll inherit risk from partners you trust but can't fully control. Your security controls won't matter if the software you're running is compromised at the source.

The challenge isn't technical we know how to do supply chain security. The challenge is economic and organizational. Verifying every dependency, monitoring every vendor, assessing every integration it doesn't scale with current resource models. And attackers know that.

Prediction Five: Critical Infrastructure Attacks Merge with Geopolitics

In 2026, the line between cybercrime and cyber warfare effectively disappears.
State-sponsored groups are planting long-term access in critical infrastructure not for immediate disruption, but for strategic leverage. Attacks will be timed around elections, conflicts, economic stress points. Criminal groups will operate with tacit state tolerance, providing plausible deniability for operations that serve geopolitical objectives.
The targets remain energy, water, transportation, healthcare, financial services. But the objective isn't always immediate chaos. Sometimes it's just demonstrating capability. Sometimes it's gathering intelligence. Sometimes it's pre-positioning for future contingencies.
What makes this particularly difficult is that detection doesn't equal prevention. By the time you find the access, they've achieved their objective which might have been just proving they could get in.

Why 2026 Feels Different

Even compared to 2025, 2026 will feel heavier. Not because any single attack will necessarily be unprecedented, but because the cumulative weight of constant pressure, faster attack cycles, longer recovery times, instant public exposure, increasing regulatory penalties, and compounding trust erosion will fundamentally change how organizations experience cyber risk.

Incidents will trigger executive accountability, legal action, customer churn, and market confidence loss in ways that purely technical failures never did. The reputational damage will outlast the technical recovery. The regulatory scrutiny will persist long after the forensics are complete.

This is the year when cyber risk stops being something that IT handles and becomes something that defines business strategy.

What Success Looks Like in 2026

The defining mistake of 2026 will be overconfidence in prevention.

Organizations that survive; really survive, not just barely hold on will have accepted that breaches are inevitable. They'll focus on detecting earlier in the attack lifecycle. They'll protect identity as critical infrastructure. They'll design systems for failure and recovery, not just for optimal operation. They'll practice disruption scenarios regularly, not just during annual tabletop exercises.

They won't try to prevent every attack. They'll try to limit impact, survive disruption, and maintain trust.

The balance of power is still tilted toward attackers in terms of speed and tactical creativity. But defenders are gaining ground in resilience, detection capabilities, recovery processes, and strategic awareness.
Victory in 2026 isn't about perfect security. It's about being able to take the hit and keep operating.

Immediate Priorities (Q1–Q2 2026)

Deploy AI-powered defences for real-time anomaly detection and automated response. Implement phishing-resistant MFA and continuous authentication across all access points.

Begin migration to quantum-resistant cryptography for sensitive systems. Map and secure your supply chain dependencies. Harden critical systems with network segmentation and zero-trust architecture.

Medium-Term Shifts (2026–2027)

Move from prevention-focused to resilience-focused security models. Shift from perimeter defense to identity-centric security. Replace compliance checkbox exercises with adaptive risk management. Build proactive threat hunting capabilities and predictive modeling.

Organizational Changes

Embed cybersecurity expertise at board and executive levels. Integrate security across IT, development, operations, and business units. Invest in continuous learning and realistic simulation exercises.

Investment Priorities

High-impact investments include AI-driven security platforms, zero-trust architecture, automation and orchestration, and comprehensive threat intelligence. Cost-effective quick wins include phishing-resistant MFA deployment, network segmentation, automated patch management, and targeted security awareness training.

Sector-Specific Considerations

Healthcare organizations need to prioritize network segmentation for medical devices and maintain treatment continuity during incidents. Manufacturing must secure operational technology environments and protect intellectual property. Educational institutions should focus on foundational email and network security despite budget constraints. Financial services require advanced fraud detection and strict access controls.

Final Assessment

We're not going to prevent every breach in 2026. We're not going to stop every attack. We're not going to catch every adversary.

What we can do is build organizations that can absorb the impact, recover quickly, and maintain the trust of customers, partners, and regulators. We can make ourselves harder targets. We can increase the cost and complexity for attackers. We can reduce our dwell time and limit our blast radius.

The threat landscape in 2026 will be defined by speed, scale, and sophistication that most organizations aren't prepared for. But preparation is still possible. The window is closing, but it hasn't closed yet.

The question isn't whether you'll face a significant cyber incident in 2026. The question is whether you'll still be operating normally the day after it happens.

Contact Us

services@esentry.io

212/214 Herbert Macaulay Way.
Yaba, Lagos, Nigeria