KEEPING NETWORKS STABLE: THE 2026 THREAT BRIEF FOR CARIBBEAN TELECOM OPERATORS

STRATOS CYBER INC.

info@stratos-cyber.com

+1 514 299 2015

www.stratos-cyber.com

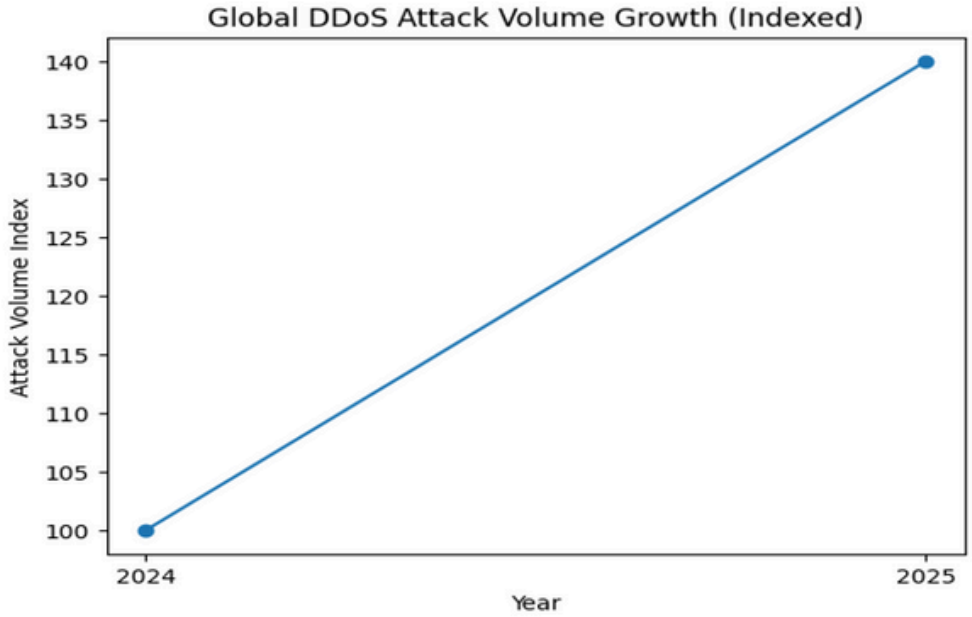
TABLE OF CONTENT

Executive Summary..... 3
The new operating reality..... 5
Ransomware and the IT-to-operations creep..... 7
Fraud and account takeover ecosystems 8
DDoS extortion and availability warfare..... .9
Virtualisation and cloud control plane compromise 10
Legacy signalling and edge exposures 10
Supply chain exposure 11
What the region adds to the equation..... 12
Ten control moves that materially reduce downtime..... 13
Board language: turning cyber risk into uptime..... 16
Conclusion..... 17
References..... 18

EXECUTIVE SUMMARY (1/2)

Telecom resilience once focused on weather, physical damage, and outages. Now, threats have shifted: modern telecom is software-defined and API-connected, with availability dependent as much on control planes as on infrastructure. Many outages now show cyber fingerprints, often manifesting first as instability or degraded service rather than as clear breaches.

Two data points frame operators' reality. First, the global threat environment is not slowing down. Cloudflare reported blocking **8.3 million DDoS attacks in Q3 2025** alone. Attack volume is growing **40% year over year.**



Indexed year-over-year growth based on industry-reported attack volumes, highlighting rising availability pressure on operators.
Source: Cloudflare Threat Reporting (2025)

The company also highlighted a botnet, Aisuru, behind routine hyper-volumetric attacks over 1 Tbps, with peaks at 29.7 Tbps.
Second, ransomware remains a consistent disruption driver. Reporting based on Verizon's 2025 Data Breach Investigations Report (DBIR) notes that ransomware accounted for **44% of breaches**, up from last year. Third-party exposure trends also continue to impact critical infrastructure providers and their vendors.

EXECUTIVE SUMMARY (2/2)

For the Caribbean, these pressures are stronger due to structural conditions, not intent. The region faces tighter specialist talent pools and greater dependence on vendors and integrators. Legacy-to-modern transition footprints are mixed, and outages quickly become public economic or social events. At the regional level, the OAS/IDB 2025 cybersecurity maturity work shows that many countries have strategies. Far fewer have the capacity and coordination to implement them. Only a small subset can protect critical infrastructure.

This brief zeroes in on threat patterns that repeatedly and predictably shatter uptime and service integrity. The imperative is clear: act urgently on control measures that reduce downtime, accelerate stability restoration, and prevent customer harm. Compliance alone is not enough. Only operational continuity matters now.

THE NEW OPERATING REALITY: TELECOM IS SOFTWARE, IDENTITY, AND APIS (WITH TOWERS)

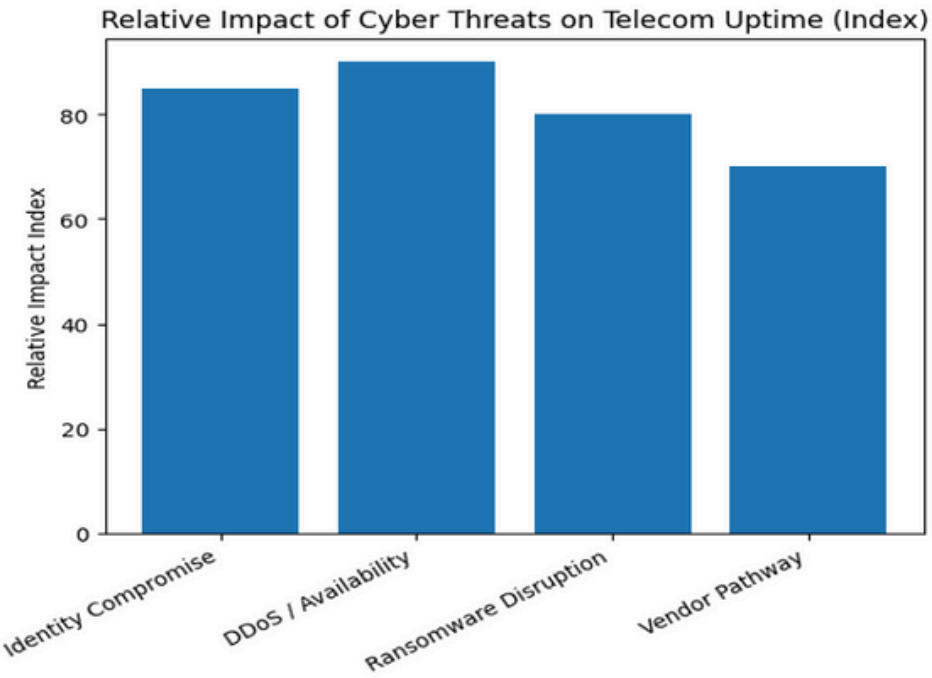
The industry's transformation has been both necessary and profitable. Virtualised network functions, cloud-managed platforms, automated provisioning, partner integrations, self-service customer journeys, and software-defined edge architectures are now normal. The hidden cost is that telecom reliability is increasingly coupled to the integrity of identities, automation pathways, management interfaces, and API ecosystems. When a control plane is misconfigured or a privileged identity is compromised, the blast radius can be immediate and non-linear. The organisation's ability to maintain availability becomes inseparable from its ability to authenticate, authorise, observe, and recover under pressure.

This is why "security" must no longer sit on the sidelines; it is now an urgent, primary input to reliability. When attackers target telecom, they do not need to "hack the tower"-they strike what towers rely on: the systems that issue changes, authenticate operators and vendors, provision services, and expose customer workflows. The consequences unfold swiftly: minutes of instability, hours of disruption, and weeks of remediation backlog-far beyond simple incident tickets.

Industry bodies have been signalling this shift clearly. GSMA's security landscape work positions mobile infrastructure as critical national infrastructure and emphasises cross-industry defensive strategies and supply chain security as central themes. The message is not academic. It is the strategic context for why availability programmes must now include cyber-driven failure modes.

THE NEW OPERATING REALITY: TELECOM IS SOFTWARE, IDENTITY, AND APIS (WITH TOWERS)

Threat patterns that reliably degrade uptime



Not all cyber incidents disrupt operations equally.

Indexed view illustrating relative impact on service stability and recovery effort across common telecom threat patterns.

Sources: GSMA security landscape analysis; Verizon DBIR trend synthesis; operator incident response observations.

RANSOMWARE AND THE IT-TO-OPERATIONS CREEP

Ransomware remains a top disruptive force not because attackers are uniquely creative, but because operational environments are uniquely interconnected. Telecom operators run **complex enterprise systems** that feed network operations: identity services, ticketing, remote administration tooling, monitoring, configuration management, and vendor access channels.

Ransomware groups exploit the seams between corporate IT and operational dependencies. What begins as a compromise of credentials, endpoint access, or an unpatched internet-facing system becomes a broader operational constraint because containment actions often require isolation, account lockouts, tooling shutdowns, and change freezes.

Even when network elements remain technically functional, loss of observability and administrative control creates service risk. When the organisation cannot see clearly, it cannot operate confidently, and uptime becomes a gamble.

The global breach landscape continues to reflect ransomware's prominence. Commentary tied to Verizon's 2025 DBIR indicates ransomware's presence in **44% of breaches**, underscoring that extortion-driven disruption remains pervasive rather than exceptional.

For telecom executives, the practical translation is that ransomware response should be treated as a resilience discipline: containment speed and recovery realism are not "security metrics"; they are availability metrics.

FRAUD AND ACCOUNT TAKEOVER ECOSYSTEMS THAT OVERWHELM OPERATIONS

Telecom fraud has evolved into an ecosystem with mature monetisation pathways. Attackers frequently aim for the customer layer: account takeover, SIM swap enablement, call centre manipulation, weaknesses in identity proofing, and insider-assisted workflows. The technical intrusion may be minimal; the operational impact can be significant. Fraud spikes create load on customer operations, retail, support tooling, and escalation chains. They also trigger defensive actions that can degrade customer experience, including forced resets, account holds, and throttling of legitimate activity. At scale, fraud becomes a service-integrity incident that erodes trust and increases churn risk.

This is an uncomfortable message for organisations that treat fraud as a separate function. In telecom, fraud is a cyber-resilience factor because it can consume operational capacity and degrade service confidence at exactly the moment the organisation needs calm execution. When fraud controls are weak, the operator's own customer workflows become an attack surface that attackers can use without ever touching "the network."

DDOS EXTORTION AND AVAILABILITY WARFARE

Distributed denial-of-service attacks have shifted from a nuisance to a form of strategic coercion. DDoS attacks now often degrade service, create reputational pressure, and set the stage for extortion or distraction. The operational issue is not just mitigating traffic, but restoring stability quickly to prevent cascading consequences. DDoS events pull engineers from planned work, introduce emergency change risk, and can degrade services customers need for self-service and support.

The scale and frequency trends are not theoretical. Cloudflare reported blocking **8.3 million DDoS attacks in Q3 2025**, with overall attack volume increasing **40% year over year**. The same report highlighted a **54% quarter-over-quarter** surge in hyper-volumetric attacks, averaging 14 such attacks per day, and noted peaks of 29.7 Tbps. This data matters to telecom leaders because it reframes readiness: the goal is not “we have a scrubbing provider.” The goal is a measurable time-to-stability capability under real pressure.

VIRTUALISATION AND CLOUD CONTROL PLANE COMPROMISE THROUGH MISCONFIGURATION AND IDENTITY

Virtualisation and cloud are not “the problem.” Uncontrolled control planes are the problem. When orchestration layers, management portals, API-driven infrastructure, and privileged identity systems are not tightly governed, compromise becomes disproportionately impactful. Attackers increasingly look for misconfigurations that expose management surfaces, credentials that unlock control-plane access, and weak authorisation paths in API ecosystems. When the control plane is compromised, attackers do not need to break a thousand systems; they can reconfigure them.

For telecom operators adopting cloud-managed network functions and broader platform modernisation, this produces a new failure mode: automation can accelerate the blast radius of both errors and attacks. In that environment, identity governance and configuration validation are not “best practice.” They are for outage prevention.

LEGACY SIGNALLING AND EDGE EXPOSURES WHERE “OLD” STILL BITE

Most operators carry legacy. The risk is not moral failure; it is physics and economics. Older interfaces, transitional gateways, and systems that “still work” can create blind spots where patching is difficult, monitoring is incomplete, and ownership is unclear. Attackers value these systems because defenders avoid them. A legacy component doesn’t have to be exploited at scale to create harm; it only needs to become a persistent foothold, a reconnaissance platform, or a source of operational instability during incident response.

Legacy risk is best approached as a controlled modernisation programme combined with isolation and visibility. Treating legacy as untouchable is how it becomes catastrophic.

SUPPLY CHAIN EXPOSURE AND VENDOR BLAST RADIUS

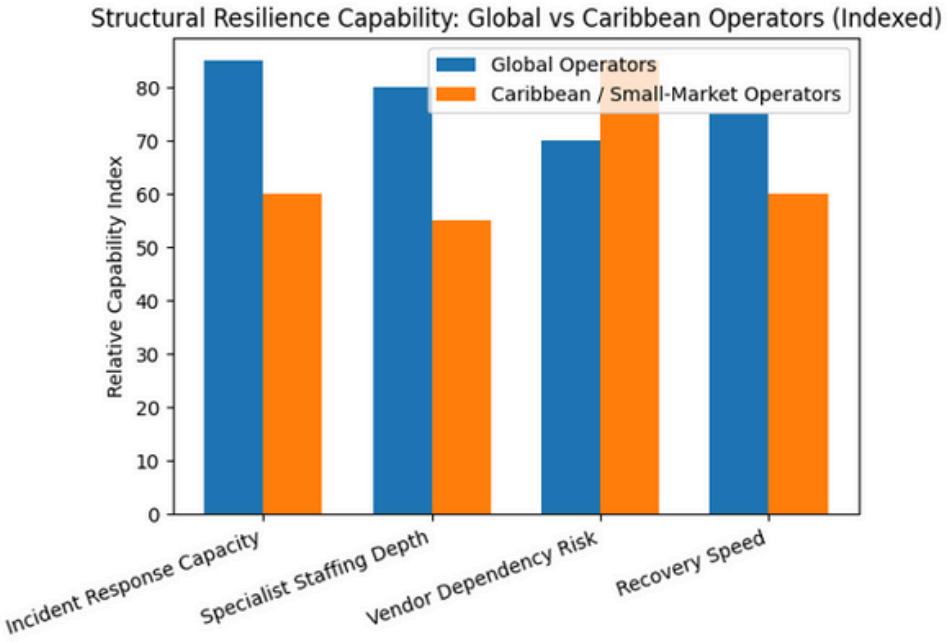
Telecom is always vendor-rich. Equipment providers, managed service partners, integrators, and cloud dependencies are needed. Problems arise when vendor pathways are privileged and persistent. If assurance is assumed rather than proven, and response is slowed by ambiguous contracts or missing telemetry, risk grows. Public focus often centres on extreme supply chain cases. The real danger is more common: a vendor account, remote support channel, trusted update, or outsourced function bypasses internal controls.

This is exactly why formal assurance frameworks exist. 3GPP's Security Assurance Specifications (SCAS) define security requirements and test cases for 5G network functions and related product classes, anchoring assurance to identified threats and assets. Operators do not need to turn SCAS into a marketing slogan. They need to use the underlying logic: no vendor should "touch core functions" without evidence-based assurance expectations, tightly controlled access, and incident-mode revocation capability.

WHAT THE REGION ADDS TO THE EQUATION: CAPACITY GAPS AND CRITICAL INFRASTRUCTURE EXPOSURE

Caribbean operators do not operate in a vacuum. They operate within national and regional ecosystems where cyber maturity varies, and critical infrastructure protection is uneven. The 2025 OAS/IDB cybersecurity maturity work makes a blunt point at the regional level: while many countries have national cybersecurity strategies, far fewer have the capacity, resources, or coordination mechanisms to implement them effectively, and only a small number are equipped to protect critical infrastructure. For operators, this increases the importance of private-sector preparedness, cross-sector collaboration, and practical readiness that does not assume perfect national response capacity.

This is not pessimism. It is strategic realism. Telecom resilience must assume that the first and best response is often internal, coordinated with trusted partners, and executed at speed.



Sources: OAS / IDB regional cybersecurity maturity findings; GSMA critical infrastructure commentary

TEN CONTROL MOVES THAT MATERIALLY REDUCE DOWNTIME(1/3)

The following control moves are designed to map to measurable operational outcomes. They are not presented as compliance checklists. They are presented as availability levers.

The first move is to **treat privileged identity as critical infrastructure**. If privileged access is weak, every other control becomes fragile. Phishing-resistant multi-factor authentication for privileged roles, tighter conditional access, session controls, and a realistic privileged access management approach reduce the likelihood that attackers can operate “legitimately.” The measurement is not whether MFA exists; it is coverage of privileged pathways and evidence of enforced strength.

The second move is **to shrink the management plane attack surface** until it becomes boring. Operators should know, with confidence, where management interfaces are reachable, who can access them, and how quickly access can be revoked. External reachability of management surfaces should be the exception and should be monitored as a leading indicator of outage risk.

The third move is t**o adopt an operationally authorised containment-first model for ransomware and identity compromise**. Many organisations fail here not because they lack technical capability, but because they lack pre-agreed authority. Containment must be fast, and speed requires governance that empowers isolation actions without improvisation.

TEN CONTROL MOVES THAT MATERIALLY REDUCE DOWNTIME(2/3)

The fourth move is **to convert DDoS readiness into a stability discipline** measured by time-to-stability. The reality of cloud-scale DDoS makes clear that attacks will happen and that scale can be extreme. Operators should measure whether instability windows are shrinking, whether escalation paths work, and whether post-event tuning is systematically applied.

The fifth move is **to treat APIs as tier-one production assets**, not developer conveniences. Critical BSS/OSS and partner APIs should be inventoried, strongly authenticated, rate-limited, and monitored for abuse signals. The measurement is the proportion of critical APIs that have enforceable controls and actionable telemetry.

The sixth move is **to harden the control plane for virtualisation and cloud** by combining baseline configuration validation with least-privilege identity governance. In fast-moving environments, drift is inevitable; the goal is to detect dangerous drift quickly and correct it before it becomes exploitable.

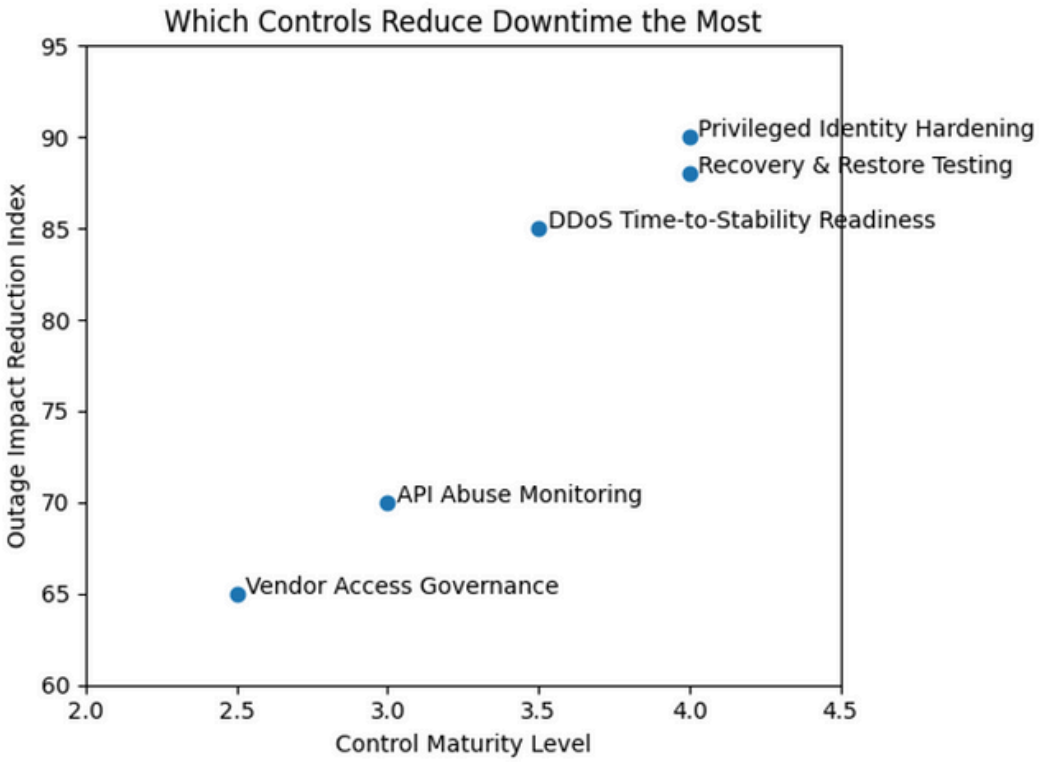
The seventh move is **to govern patching based on exposure and exploitability** rather than abstract severity scoring. Patch latency for internet-facing services is a direct predictor of compromise probability, and compromise probability is a direct predictor of disruption.

The eighth move is **to treat fraud as a joint resilience mission** across security, customer operations, and risk functions. Fraud monitoring signals should be operationalised and connected to security monitoring so that account takeover campaigns are detected as quickly as denial-of-service events.

TEN CONTROL MOVES THAT MATERIALLY REDUCE DOWNTIME(3/3)

The ninth move is **to operationalise vendor assurance** through evidence and access control, not through paperwork. SCAS-aligned expectations are useful precisely because they clarify security requirements and testing expectations for network functions. The measurement is vendor coverage and the speed at which vendor access can be disabled during incidents.

The tenth move is **to make recovery realistic** through tested restoration, including the restoration of monitoring and control capabilities, not just data. Backup confidence without restoration testing is optimism with a budget line.



Source: Stratos Cyber analysis based on telecom incident response engagements, industry incident reporting (GSMA, Verizon DBIR), and operational resilience assessments across carrier environments.

BOARD LANGUAGE: TURNING CYBER RISK INTO UPTIME, REGULATORY EXPOSURE, AND CAPEX/OPEX DECISIONS

Boards do need clarity in decision-making that ties technical realities to business outcomes. The simplest translation model is that cyber risk is now a service stability risk, which becomes a customer trust risk, which becomes a financial and regulatory risk. When a telecom outage happens, the public does not separate cause categories. The outcome is what matters: downtime, degraded access, and lost confidence.

The board-level discussion should therefore centre on a small set of **outcome-oriented questions**:

- Are we reducing the probability of control-plane compromise by hardening privileged identity and management access?
- Are we reducing time-to-containment when identity compromise occurs?
- Are we reducing time-to-stability when DDoS or availability attacks occur, given that DDoS volume and scale trends remain intense?
- Are we governing vendor pathways as potential blast-radius multipliers, consistent with industry emphasis on supply chain security and assurance?
- And are we funding controls that measurably reduce downtime hours rather than funding controls that only improve audit comfort?

This is the CAPEX/OPEX point that matters. Resilience spending should be justified as outage-cost prevention and stability acceleration. When the organisation tracks containment speed, stability speed, patch latency for exposed systems, and recovery success rates, it develops an investment model that boards can understand without becoming security specialists.

CONCLUSION

This brief is intentionally practical. It assumes that operators cannot pause modernisation, cannot avoid vendors, and cannot magically staff every specialised role overnight.

It also assumes a reality that the data supports: attack volume, extortion-driven disruption, and availability-focused pressure are not edge cases; they are part of the operating environment.

The strategic question is therefore not whether incidents will occur, but whether the operator can compress impact, maintain stability, protect customer trust, and recover with discipline.

Telecom resilience in 2026 is not a slogan. It is the quiet competence to keep services stable when identity is attacked, APIs are abused, vendors become pathways, and traffic becomes a weapon.

REFERENCES

1. GSMA, “Mobile Telecommunications Security Landscape 2025” and related industry updates on defensive strategies and supply chain emphasis (https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2025)
2. Cloudflare, “2025 Q3 DDoS Threat Report,” including quarterly and year-over-year DDoS volumes and hyper-volumetric attack observations. (https://blog.cloudflare.com/ddos-threat-report-2025-q3)
3. Verizon, “2025 Data Breach Investigations Report” reporting, including ransomware prevalence trends and payment dynamics. (https://www.verizon.com/business/resources/reports/dbir/#2025DBIRNR)
4. Barr Advisory analysis citing Verizon 2025 DBIR on third-party involvement trends. (https://www.barradvisory.com/resource/takeaways-2025-verizon-dbir/)
5. OAS/IDB, “Cybersecurity Report 2025: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean,” including regional institutional capacity observations and critical infrastructure preparedness.
6. 3GPP, Security Assurance Specifications (SCAS) overview and assurance logic for 5G network functions.

WHY STRATOS CYBER –
WE EMPOWER SMES WITH RESILIENCE

Stratos Cyber supports organizations that require measurable cybersecurity outcomes under practical operating constraints. Our delivery model integrates exposure reduction, continuous monitoring and response, governance alignment, and readiness validation so that security activity translates into verified posture improvement.

📩 Contact us to schedule a strategic briefing.

info@stratos-cyber.com

+1 514 299 2015

www.stratos-cyber.com