Srinivas L
Joint MD & Joint CEO
63SATS Cybertech

GCCs operate at massive scale with distributed teams and workloads. How do you help them translate cybersecurity strategy into consistent, day-to-day operational execution?

Cybersecurity strategy must ultimately serve and align with business objectives. To translate this into consistent day-to-day execution, we combine expert-led consulting with a robust portfolio of solutions and services. Our approach integrates advanced tools and OEM platforms to strengthen the overall security architecture, while also embedding governance and operational discipline into daily workflows. This ensures that cybersecurity is not just a strategic intent, but a continuously enforced practice across distributed teams and environments.

We further drive measurable outcomes through defined KPIs, regular audits, and continuous improvement frameworks that enhance accountability and long-term resilience.

Many GCCs still approach security reactively. How is 63SATS helping them move toward continuous assurance and real-time readiness across global operations?

A reactive approach is no longer viable in today's threat landscape, especially with advancements such as Claude Mythos, and other AI-driven attack models. At 63SATS, we enable organizations to shift toward a proactive and resilient posture through our next-generation SOC, which delivers real-time threat detection, analysis, and response across global operations.

Beyond technology, our teams focus on the continuous evolution of cybersecurity frameworks, helping GCCs anticipate risks, strengthen defences, and embed readiness into everyday operations. This ensures a move from reactive response to continuous assurance, aligned with the dynamic nature of modern cyber threats.

We also leverage predictive intelligence, automation, and cross-functional collaboration to ensure faster decision-making, reduced response times, and sustained cyber resilience at scale.

As GCCs increasingly become the first line of defense for global enterprises, what operational capabilities do they need to own internally versus relying on external partners?

As part of our engagement model, we enable GCCs to strike the right balance between in-house capabilities and external expertise. Core functions such as governance, risk ownership, and critical decision-making should remain internal to ensure accountability and alignment with business priorities.

At the same time, we provide managed services where our specialists operate as an extension of their teams, supporting day-to-day security operations and resilience. We also actively participate in due diligence processes and offer leadership roles such as vCISO and vDPO. While these experts are part of our organization, they operate with complete integrity and act in the best interests of the client, ensuring strong oversight, compliance, and operational excellence, enabling scalability, faster response times, proactive risk mitigation, and sustained alignment with evolving regulatory and cybersecurity landscapes. ■