Neehar Pathare
MD, CEO & CIO
63SATS Cybertech

As GCCs increasingly own global systems and platforms, how do you view their role evolving from execution centers to enterprise-wide digital control towers—and how is 63SATS preparing for that shift?

We partner with Global Capability Centers (GCCs) across the data and software lifecycle, providing support from design to deployment. Our governance specialists ensure security is embedded at every stage, not treated as an afterthought.

As GCCs evolve into critical hubs, strong internal controls are essential to avoid concentration risks and single points of failure. We work with organizations to strengthen these frameworks, while our technology helps mitigate insider threats.

We also enable a holistic cybersecurity approach by validating the entire ecosystem, including third-party partners, against best practices, ensuring resilience and end-to-end security integrity.

Additionally, our continuous monitoring, threat intelligence, and AI-driven analytics empower GCCs to proactively detect, respond, and adapt to cyber risks.

From a CIO's perspective, how should GCCs architect security into their platforms from day one, rather than layering it later as a compliance requirement?

In system development, we begin at the requirement definition stage by outlining security expectations alongside the business case—ensuring security is a core criterion from the outset. As design is finalized, we incorporate threat modeling to identify and address vulnerabilities.

During development, modules undergo testing through SAST and DAST techniques to ensure code and application-level security. We also enforce strict segregation of SATS data from system data, maintaining integrity and minimizing risk across the lifecycle.

Post-development, we conduct rigorous validation, including penetration testing and secure code reviews, before deployment. Continuous monitoring, patch management, and incident response mechanisms further ensure systems remain resilient against evolving threats.

What architectural or platform-level decisions should GCC leaders make today to ensure long-term cyber resilience as business complexity and autonomy increase?

It is essential to clearly segregate operational requirements from evolving security requirements, ensuring that both grow in tandem. A structured pipeline must be in place to consistently uphold the availability, integrity, and confidentiality of data as operations scale.

From a strategic standpoint, planning must account for scalability, elasticity, and future feature needs. For instance, when building AI platforms, robust security controls must be embedded into the development of LLMs from the outset. Given that GCCs manage significant volumes of global data, they must also address a wide range of regulatory compliance obligations, while carefully considering the ethical implications of data usage and profiling. ■