Neehar Pathare
MD, CEO & CIO
63SATS Cybertech

With GCCs emerging as AI powerhouses, how are you securing AI models, data flows, and autonomous operations effectively?

As GCCs evolve into global engineering and AI innovation hubs, cybersecurity architecture must move from perimeter protection to model-centric and data-centric security. Our focus is on securing the entire AI lifecycle, from data ingestion and model training to deployment and autonomous decision environments.

We are strengthening architectures through zero-trust frameworks, secure data pipelines, and continuous model monitoring to guard against data poisoning, model manipulation, and supply-chain vulnerabilities. Equally important is embedding security by design into AI development workflows so that protection scales alongside innovation.

India's GCC ecosystem is operating at global scale, and with that comes systemic responsibility. Our approach is to combine advanced threat intelligence, automation, and resilient infrastructure so that high-autonomy digital operations remain both secure and trusted in an increasingly AI-driven world.

What core security foundations do GCCs need to build an "impenetrable cyberdome," and how does your platform strengthen that journey?

To achieve what we describe as an "impenetrable cyberdome," GCCs must first build security as an architectural foundation rather than an operational layer. This requires a combination of zero-trust identity frameworks, real-time threat intelligence, unified visibility across cloud and on-premise environments, and strong protection for data, APIs, and AI workloads. Just as important is the ability to detect and respond to threats at machine speed through automation and continuous monitoring.

At 63SATS, our platform is designed to help organizations move from fragmented security tools to a cohesive, intelligence-driven defense architecture. We integrate advanced analytics, automated threat detection, and resilient infrastructure protection to create a secure operating environment. The objective is not only to defend systems, but to enable GCCs to innovate and scale globally with confidence.

With GCCs leading global cyber mandates, how can your platform help them mature into full cyber command centers across detection, response, assurance, and secure AI?

GCCs are uniquely positioned to evolve from support functions into global cyber command centers that oversee enterprise-wide security operations. Our approach is to partner with GCCs by strengthening four foundational pillars: advanced detection, rapid response, continuous assurance, and secure AI operations.

We help establish integrated security operations environments that combine real-time threat intelligence, AI-driven monitoring, and automated incident response to manage risks at global scale. Equally important is embedding assurance frameworks and governance models that provide visibility across cloud, data, supply chains, and digital infrastructure. As enterprises increasingly deploy AI across core operations, GCCs must also secure models, data pipelines, and decision systems. Our role is to provide the technology architecture, engineering expertise, and operational frameworks that enable GCCs to operate as resilient, intelligence-driven cyber command centers for the global enterprise. ■