Srinivas L
Joint MD & Joint CEO
63SATS Cybertech

You've highlighted that securing AI systems is now "existential" for enterprises. What unique AI-specific threat models should GCCs prioritise as they scale mission-critical global functions from India?

As AI becomes embedded in mission-critical enterprise operations, the threat landscape expands beyond traditional cybersecurity risks. GCCs must prioritise AI-specific threat models across the entire model lifecycle. These include data poisoning during training, where compromised datasets distort model behaviour; model manipulation or adversarial attacks that influence outputs; and model extraction, where attackers attempt to replicate proprietary algorithms.

Equally critical are risks in AI supply chains, including vulnerabilities in third-party models, libraries, and development frameworks. As enterprises deploy autonomous AI systems, decision integrity and model governance also become central concerns.

For GCCs managing global digital operations from India, securing AI requires strong data provenance controls, continuous model monitoring, secure MLOps pipelines, and robust access governance. Protecting AI is no longer just a technical priority, it is fundamental to safeguarding enterprise decision systems and operational trust.

63SATS has established an advanced SOC with AI-specific threat analysis and rapid incident response. How do you see GCCs leveraging such AI-augmented SOC capabilities to strengthen global resilience and reduce response times?

63SATS enables GCCs to strengthen enterprise-wide cyber resilience through its 24×7 Security Operations Centre. Powered by the 63SATS Cybertech Threat Intelligence Monitoring & Response Command Centre (TiM&RC), the platform delivers AI-driven threat analysis, continuous monitoring, and rapid incident response across distributed global environments. For GCCs that manage critical digital operations for multinational organizations, this capability helps significantly reduce detection and response times while ensuring uninterrupted operations. By integrating predictive threat intelligence with automated defense mechanisms, the framework accelerates cyber defense readiness through a "Shift Left" approach and simultaneously strengthens long-term cyber maturity through "Shift Right."

How are evolving global data regulations impacting cybersecurity frameworks within India's GCCs?

Evolving global data regulations are significantly reshaping cybersecurity frameworks within India's GCCs, pushing them toward more structured, accountable, and globally aligned security models. With regulations such as GDPR, DPDP, and other regional data laws, GCCs must now manage complex cross-border data flows while ensuring compliance with multiple jurisdictions.

This is driving a shift toward data localisation strategies, stronger encryption standards, and stricter access controls. Organisations are re-architecting systems to ensure data sovereignty, while maintaining operational efficiency for global mandates.

There is also a growing emphasis on governance, auditability, and real-time visibility. Compliance is no longer a checkbox exercise, it is becoming a core business enabler. GCCs that can seamlessly integrate regulatory requirements into their cybersecurity architecture will be better positioned to build global trust while continuing to scale AI-driven operations. ■