Neehar Pathare
MD, CEO and CIO
63SATS Cybertech

How does 63SATS help GCCs build robust cyber defenses through its end-to-end security offerings?

63SATS Cybertech delivers GCCs comprehensive, layered defenses that combine real-time threat intelligence, SOC operations, and cloud-native security tools. For example, a global GCC handling sensitive financial processing can rely on our 47-seater Threat Intelligence & Monitoring Response Centre (TiM&RC) for 24/7 monitoring, instantly detecting lateral movement or credential abuse across their networks.

What makes us stand out is our "customer-first" model – we integrate not only our products but also third-party tools already in use, ensuring seamless, unified protection tailored to the GCC's business model, tech stack, and operational footprint.

How is the company bringing cutting-edge cybersecurity to enterprise environments?

63SATS introduces cutting-edge cybersecurity to GCCs by combining AI/ML-driven anomaly detection, zero-trust frameworks, and advanced EDR/XDR integration. For example, a GCC supporting global supply chain operations can use our automated SOAR (Security Orchestration, Automation, and Response) platform to accelerate threat response – cutting investigation times from hours to minutes.

Moreover, our cloud posture management ensures that as GCCs transition to multi-cloud environments (AWS, Azure, GCP), their configurations remain secure, compliant, and optimized, preventing misconfigurations – a leading cause of modern data breaches – without adding operational burden to their internal security teams.

How are your services tailored to meet the distinct security needs of industries like BFSI, healthcare, and manufacturing?

We recognize that every sector has its own distinct risk landscape. For example, in BFSI GCCs managing transaction processing, we can implement PCI DSS-compliant encryption and real-time fraud detection.

Similarly, for healthcare, we align solutions with industry-specific regulations, while in manufacturing, we address operational risks with tailored security controls. Our approach ensures that each GCC receives a customized security framework aligned with both regulatory requirements and sector-specific threats.

Rather than applying a "one-size-fits-all" defense, we build industry-specific playbooks aligned to compliance, sectoral threats, and business needs – ensuring each GCC operates securely within its regulatory and operational ecosystem.

How does the company support GCCs in handling cyber incidents and strengthening post-attack resilience?

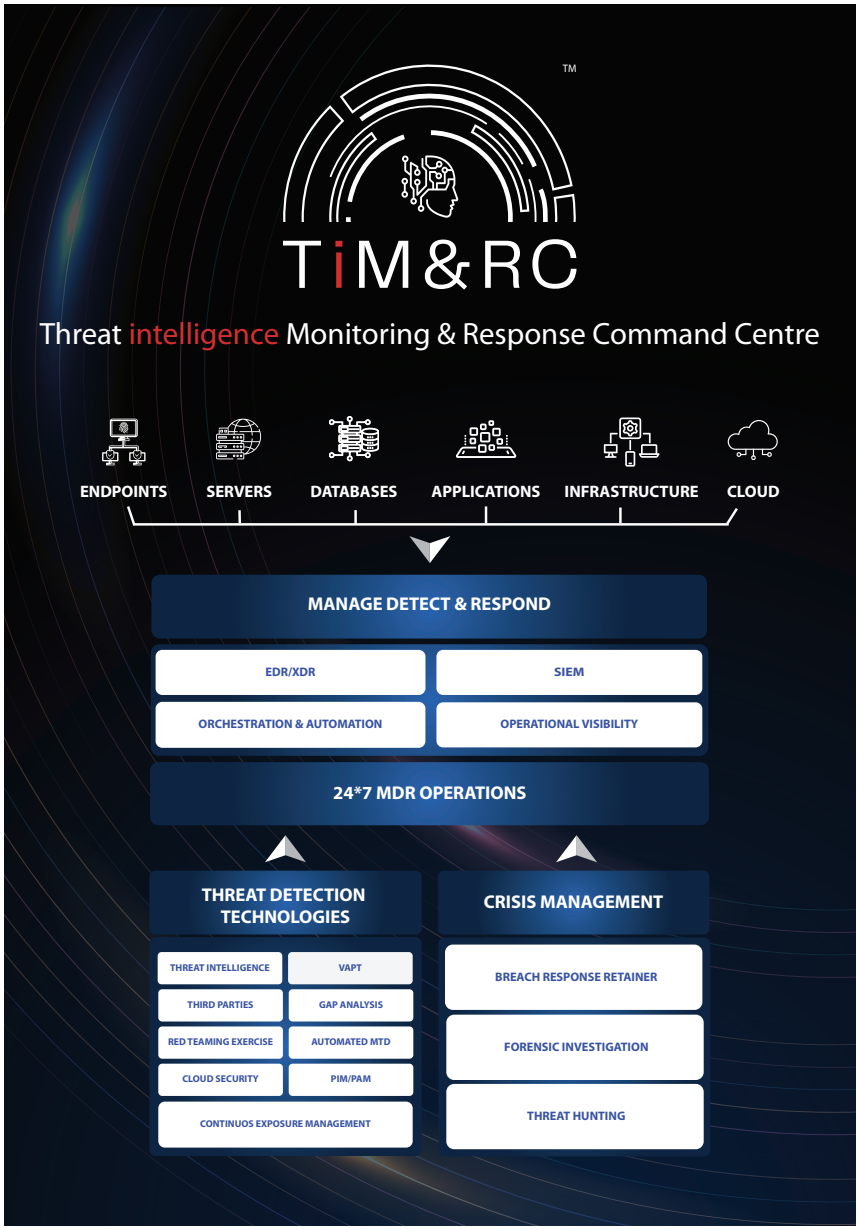
When a GCC experiences a breach – say, a ransomware attack crippling a global HR platform – we swiftly step in with rapid containment through our TiM&RC and specialized forensics lab to uncover entry points and attack paths. But we don't stop at recovery.

We strengthen post-attack resilience by conducting identity audits, rotating machine credentials, tightening IAM controls, and running ransomware simulations to stress-test defenses. For GCCs, recovery isn't just about restoring operations – it's about emerging stronger, smarter, and better prepared for whatever comes next.

As GCCs grow, how does the company ensure their security frameworks scale seamlessly?

As GCCs expand, whether adding new delivery centers in India or across geographies, 63SATS ensures scalable security through modular, API-integrated tools that grow with the enterprise. For example, our identity governance solutions adapt as machine identities multiply (often outpacing human users), ensuring visibility and privilege control across sprawling environments.

We also embed cloud-native security controls that flex across multi-cloud and hybrid setups, preventing gaps as workloads and operations scale. Our centralized dashboards give GCCs a unified security view, regardless of how many regions, clouds, or services they add.



What emerging cyber risks do you foresee for GCCs, and how is the company preparing to address them?

Emerging risks for GCCs include AI-powered social engineering, deepfake scams targeting executive teams, and machine identity exploitation. For example, we've seen attackers use synthetic audio to impersonate GCC leadership, tricking staff into wire transfers. We are already delivering deepfake detection tools, advanced behavioural analytics to flag unusual access patterns, and machine identity governance to close the fastest-growing attack surface – where ad hoc service accounts often go unmanaged. In India's rapidly digitizing landscape, we help GCCs secure not just systems but business continuity and national digital sovereignty against increasingly sophisticated, multi-layered threats.