**Neehar Pathare**
MD, CEO & CIO
63SATS Cybertech

### What strategic shifts are you prioritizing to help enterprises stay ahead of rapidly evolving cyber threats?

At 63SATS Cybertech, we recognize cybersecurity is no longer just a technology function but a core business imperative. As threats grow more sophisticated, our focus is on helping organizations shift from reactive security to a proactive, intelligence-driven, resilience-led approach.

A key priority is integrating AI and automation into security frameworks for faster detection, response, and predictive threat management. We are also advancing zero-trust architectures and strengthening cloud and data security to support evolving digital transformation.

Equally important is embedding cybersecurity into enterprise strategy, aligning it with risk management, compliance, and business continuity. Our approach focuses on building cyber resilience, enabling organizations to both prevent attacks and recover quickly. Through advanced technology, domain expertise, and strong partnerships, we help organizations stay ahead of emerging threats while enabling secure, sustainable growth.

### How do you balance modernizing internal technology with delivering cutting-edge cybertech solutions in areas like AI-driven threat detection, cloud security, and zero-trust?

Balancing internal technology modernization with delivering advanced cybersecurity solutions is central to my role as CIO. At 63SATS Cybertech, we follow a "build, secure, and scale" philosophy, using our own environment as a live testbed before deploying solutions for clients.

We focus on modernizing our infrastructure with AI-driven security, cloud-native architectures, and zero-trust frameworks. This strengthens our resilience while providing real-world insights into what works at scale, enabling us to design practical, effective solutions. At the same time, we remain deeply client-centric. Our investments in AI-led threat detection, advanced analytics, and cloud security are aligned with evolving risks and business needs. Close collaboration between internal teams and client delivery ensures faster feedback and continuous improvement.

This dual approach helps us stay ahead of emerging threats while delivering scalable, robust solutions grounded in real operational experience.

### How is 63SATS Cybertech shaping its product and service roadmap to address the distinct needs of different sectors?

The cyber risk landscape varies across sectors such as BFSI, manufacturing, and government, each with distinct threats, regulations, and priorities. At 63SATS Cybertech, our roadmap follows a sector-specific approach, ensuring solutions are tailored, scalable, and aligned with industry needs.

In BFSI, where data sensitivity and compliance are critical, we focus on advanced threat detection, fraud prevention, and strong data protection to support secure customer experiences.

In manufacturing, the convergence of IT and OT creates new vulnerabilities. We address this by securing industrial systems, protecting connected assets, and ensuring business continuity.

For government and public sector organizations, we prioritize protecting critical infrastructure, strengthening data sovereignty, and building resilient security architectures. Across sectors, we integrate AI-driven intelligence, cloud security, and zero-trust models to enable proactive risk management and secure digital transformation. ■