VOLUME 2, ISSUE 2 | APRIL 2026

Tech Disruptor media.com

techdisruptormedia.com techdisruptormedia

Scan and Explore Full Magazine

63SATS CYBERTECH SECURING ENTIRE AI LIFECYCLE FROM DATA INTEGRITY TO MODEL VALIDATION

NEEHAR PATHARE

MD, CEO and CIO
63SATS Cybertech

A BRAND OF BNG
bharatnetworkgroup.com

INTERVIEW

63SATS CYBERTECH SECURING ENTIRE AI LIFECYCLE FROM DATA INTEGRITY TO MODEL VALIDATION

Neehar Pathare, MD, CEO and **CIO, 63SATS Cybertech**, tells **Aishwarya Saxena** why the moment an organisation stops assuming the intruder is already inside is the moment it becomes genuinely vulnerable

What inspired the positioning of 63SATS as a "Cyber Security Force" for enterprises and governments?

Think of the traditional approach to security like a fire department, they are world class at putting out fires, but they only arrive after the smoke appears. Positioning 63SATS as a Cyber Security Force (CSF) represents a shift from being a "firefighter" to being a "specialized defense unit".

In a world where digital threats are constant, you cannot afford to be reactive. We operate with a "defense-oriented" mindset, focusing on continuous monitoring and rapid response. Much like a physical security force patrolling a perimeter, we use real-time threat intelligence to stop intruders before they breach the gates. For our partners in government and enterprise, this means we aren't just a vendor they call during a crisis; we are a strategic partner integrated into their daily operations to ensure their systems remain resilient and their data stays trusted.

Having transitioned from core IT leadership roles into cybersecurity, what

> When we build new technology, we don't "add on" security at the end; we frame it in from the very first line of code

mindset shift was required?

In traditional IT leadership, the goal is "Performance and Uptime". You want the engine to run smoothly, efficiently, and fast. However, in cybersecurity, the starting assumption is much darker: the "engine" is already under attack, and the intruder might already be inside the cabin.

The shift required is moving from a "Reliability" mindset to a "Resilience" mindset. It's no longer enough to build a strong wall; you have to think like the person trying to climb over it. This means embedding security into the very DNA of an organization from how a server is configured to how an employee handles an email. At 63SATS, we "stress-test" this mindset using Red Teaming, where we simulate real-world attacks to find gaps before a malicious actor does.

With AI increasingly embedded in enterprise systems, how do you mitigate risks like data poisoning and adversarial attacks?

AI is a double-edged sword. It's incredibly powerful, but its "brain" is only as good as the data its fed. Data poisoning is like someone slipping "false memories" into an AI's education, causing it to make dangerously wrong decisions.

To mitigate this, we secure the entire AI Lifecycle.

Data Integrity: We verify the "purity" of the data at the very first stage to prevent manipulation.

Model Validation: We treat the AI model like a black box that needs constant inspection to ensure it hasn't been tampered with or developed "biases".

Zero-Trust for AI: We apply Zero-Trust principles, meaning no input is trusted by default. Every interaction with the AI must be verified, and we use our own AI-driven detection to spot patterns of "adversarial attacks" that a human might miss.

How does your use of frameworks like MITRE ATT&CK enhance your ability to simulate real-world attack scenarios?

In the past, security testing was often a "checkbox" exercise. Did you lock the door? Did you close the window? Frameworks like MITRE ATT&CK allow us to move beyond checkboxes to Adversary Emulation.

Think of MITRE ATT&CK as a massive, globally updated encyclopedia of every move a "burglar" has ever used. Instead of

just looking for a "weak lock," we map out the entire "heist". We can simulate how an attacker would move through a network, what they would try to steal, and how they would try to hide their tracks. This gives organizations a clear map of not just their weaknesses, but their gaps in detection and recovery, providing actionable insights to harden their defenses effectively.

With increasing reliance on third-party vendors and SaaS tools, how do you embed supply chain security into modernization strategies?

Modern businesses are "interconnected." When you use a third-party software or a cloud service, you aren't just buying a tool; you are opening a door into your house for a stranger. Supply chain risk is the danger that this "stranger" (the vendor) might have their own security flaws that lead back to you.

At 63SATS, we treat supply chain security as a non-negotiable part of digital transformation.

Lifecycle Assessment: We don't just vet a vendor when they sign a contract; we monitor them continuously.

Extended Zero-Trust: We extend our security perimeter to include these external tools. Every time an external tool tries to talk to your internal systems, it must be authenticated, authorized, and verified. This allows companies to scale and innovate without worrying about "hidden" risks lurking in their ecosystem

> **We can simulate how an attacker would move through a network, what they would try to steal, and how they would try to hide their tracks**

As MD, CEO, and CIO simultaneously, how do you balance business growth, technology innovation, and security governance?

People often see security as a "brake" on a car, it slows you down. I see it as the reason you can drive at 100 mph with confidence. Balancing these roles requires understanding that they are all interconnected drivers of success.

Growth is built on trust: You cannot grow a business if your customers don't trust you with their data.

Innovation requires "Security- by Design": When we build new technology, we don't "add on" security at the end; we frame it in from the very first line of code.

Governance as a blueprint: Governance provides the rules of the road, allowing us to scale responsibly while staying compliant with global standards.

By integrating these, security becomes a business enabler rather than a constraint. It gives an organization the "Digital Sovereignty" to evolve and compete on a global stage, knowing their foundation is rock-solid.

editor@thefoundermedia.com