Quick Heal's Vishal Salvi on India's Cybersecurity Resilience & AI

In an interview with TimesTech, Vishal Salvi, CEO of Quick Heal Technologies Limited, delved into India's growing cybersecurity challenges amid geopolitical tensions. He highlighted the vulnerability of critical sectors, the role of homegrown technologies like SIA and AntiFraud.AI, and how AI is transforming cyber defense. Salvi emphasized Quick Heal's mission to build national cyber resilience through innovative, Made-in-India solutions that are trusted globally.

Read the full interview here:

TimesTech: Which key sectors in India remain most vulnerable to cyberattacks due to the heightened geopolitical tensions, and how can businesses better safeguard them?

Vishal: Our India Cyber Threat Landscape Report 2024, prepared meticulously by our researchers at Seqrite Labs, India's largest malware analysis facility, reveals some key insights regarding the critical sectors in India that face heightened vulnerability amid growing geopolitical tensions. The healthcare sector tops this list, comprising 21.82% of threats detected. This sector houses critical patient data that, if compromised, could have serious national security implications, as we witnessed in the AIIMS cyberattack that exposed sensitive health data of senior government officials and military officers.

Healthcare is followed by hospitality (19.57%), BFSI (17.38%), and education (15.64%), respectively. Apart from these, critical infrastructure, including power grids, transportation systems, and communication networks, continues to face sophisticated threats. The recent Operation Sindoor incident marked a significant escalation in the India-Pakistan cyber conflict, with state and non-state actors collaborating to target key sectors and intensify geopolitical tensions through coordinated digital attacks.

To better safeguard these sectors, businesses need to first and foremost implement comprehensive, multi-layered security frameworks with real-time threat intelligence. Conducting regular security audits and vulnerability assessments can also strengthen the cybersecurity stance. Leveraging AI and

ML-powered solutions for proactive threat detection and enforcing strict access controls through Zero Trust Network Access solutions can be of great help. At the same time, organizations need to invest more in employee cybersecurity awareness training, as human error remains a significant vulnerability.

TimesTech: How critical is it for India to have cybersecurity firms like Quick Heal contributing to national resilience through homegrown technologies?

Vishal: It's absolutely vital. India saw a multifold increase in cyberattacks in recent times, significantly outpacing the global increase. Researchers at Seqrite Labs detected 369.01 distinct malwares in 2024 alone, and the number is expected to increase this year, thanks to the ever-increasing internet penetration. At such a time, our digital sovereignty depends on ironclad indigenous cybersecurity capabilities.

Being a through-and-through 'Made in India' cybersecurity solutions provider, we, at Quick Heal Technologies Limited, understand India's unique threat landscape and can tailor solutions to address specific vulnerabilities in our infrastructure. During international conflicts, when cyberattacks on Indian enterprises rise by leaps and bounds, it's the coordinated efforts between government agencies and cybersecurity firms like ours that keep the damage limited. As the only listed cybersecurity products company in India, we are proud of our contribution to building national cyber resilience.

Our technologies are developed with deep knowledge of both global and India-specific threats, giving us an edge that foreign solutions simply cannot match. In light of the rising incidents of digital fraud, we have also created AntiFraud.AI, our AI-driven fraud detection tool that safeguards users from phishing, deepfake attacks, spam emails, and more. In a bid to make this cutting-edge tool accessible to a greater set of users, we have now adopted a freemium model for AntiFraud.AI, which means that customers now get access to the most advanced features for free.

TimesTech: How can long-standing cybersecurity players like Quick Heal, with deep visibility into India's threat landscape contribute to national resilience against sophisticated cyberattacks?

Vishal: Our three-decades-long leadership in the Indian cybersecurity space has given us unparalleled insights into the evolving threat landscape. Through Seqrite Labs, India's largest malware analysis facility, we have built extensive threat intelligence capabilities that help us identify and neutralize India-specific attacks before they cause widespread damage.

This deep visibility allows us to contribute to national resilience in several ways. First, we provide early warning systems for emerging threats targeting critical sectors. Second, our threat intelligence feeds help strengthen the overall security posture of government agencies and enterprises alike. Third, we actively participate in Indian as well as international organizations such as the DSCI and the NIST NCCoE.

Our patented AI/ML-powered technology GoDeep.AI enables us to detect sophisticated threats, including those from state-sponsored actors targeting India's critical infrastructure. By analyzing millions of threat vectors daily, we are able to predict attack patterns and develop proactive countermeasures that protect Indian organizations against even zero-day vulnerabilities.

We also expanded the shield of safety for our citizens by creating AntiFraud.AI, our AI-driven tool that prevents digital fraud. Like I explained earlier, the tool offers protection from phishing, deepfake attacks, spam emails, etc., preventing unsuspecting users from falling prey to the latest scamming

techniques, which are getting increasingly difficult to detect by the human eye. To further amplify its reach, we recently adopted a freemium model that makes the most advanced features of the tool accessible to users without them having to pay a premium.

TimesTech: How does SIA fit into India's broader national cybersecurity strategy, especially in combating both state-sponsored and hacktivist cyber threats?

Vishal: SIA, our virtual security analyst, represents a significant advancement in India's capabilities to combat sophisticated threats, including those from state actors and hacktivists. Government agencies are prime targets for these attackers, as we have seen with Chinese and Pakistani state-affiliated groups targeting India's strategic assets. Amidst this, SIA augments India's cybersecurity strategy by providing AI-powered threat detection and response capabilities that can operate at machine speed. This is crucial when facing sophisticated adversaries with significant resources. The solution automatically identifies suspicious patterns that might indicate state-sponsored activity or hacktivist campaigns, enabling rapid response before damage occurs.

For government entities safeguarding critical infrastructure and sensitive data, SIA provides continuous monitoring and analysis that would otherwise require vast human resources. This aligns perfectly with the NCIIPC's efforts to strengthen India's cybersecurity posture through comprehensive frameworks and sector-specific protection measures. By combining advanced AI with deep threat intelligence from our Seqrite Labs, SIA helps address the cybersecurity skill shortage while providing enterprise-grade protection against the most sophisticated threat actors targeting India's national interests.

TimesTech: How does SIA represent a "transformative leap" that bridges the gap between human intelligence and Generative AI?

Vishal: SIA represents the convergence of human expertise and advanced artificial intelligence in a way that completely reimagines cybersecurity operations. Traditional security approaches either relied heavily on human analysts who couldn't scale to match the volume of threats or used rule-based automation that lacked adaptability. SIA bridges this gap.

What makes SIA transformative is its ability to learn continuously from our vast threat intelligence database while applying contextual understanding to security incidents. It goes beyond just detecting threats based on signatures by understanding the narrative behind attack patterns. When analyzing potential incidents, SIA incorporates the specialized knowledge of our security experts with the pattern-recognition capabilities of AI.

For security teams overwhelmed by alerts, SIA acts as a trusted advisor that can prioritize threats based on their potential impact, provide actionable remediation steps, and continuously learn from new attack vectors. This human-AI partnership allows security teams to focus on strategic decisions while SIA handles the complex analysis of threats at machine speed.

TimesTech: What sets GoDeep.AI apart as a "self-aware malware hunting technology" powering SIA?

Vishal: GoDeep.AI is truly revolutionary as a malware hunting engine because it combines multiple advanced technologies that work in harmony to create what we call "self-awareness" in threat detection. Its Cloud-Based Deep Learning Module grants our malware hunting engine the power to learn and remember virtually every malware threat in history, storing this comprehensive knowledge in a centralized cloud. At the same time, its Advanced Behavior Detection System continuously

monitors and tracks activities performed by each program running on a computer. Any program displaying behavior similar to known malware is immediately blocked, even if it uses novel techniques to evade traditional detection.

The DNA Scan capability of GoDeep.AI is another breakthrough. It's a boot-time scan that can identify and fix critical system files that have been infected, proving effective even against zero-day attacks while consuming minimal system resources. But perhaps the most important feature is GoDeep.AI's Seed Analysis, which can identify a threat's origination, potential impact, and characteristics before it activates. This predictive capability, combined with multilayered defense mechanisms, enables SIA to stop threats that other solutions simply cannot detect.

TimesTech: How does SIA reinforce Seqrite's positioning as a "Made-in-India" solution for global enterprise cybersecurity?

Vishal: SIA stands as a prime example of our commitment to developing world-class cybersecurity solutions with Indian innovation at their core. As the enterprise arm of Quick Heal Technologies Limited, Seqrite has consistently demonstrated that homegrown technology can compete with and often exceed global alternatives.

Our position as the first and only Indian company to collaborate with the U.S. Government on its NIST NCCoE's Data Classification project underscores the international recognition of our capabilities. SIA further reinforces this positioning by leveraging our unique understanding of both global and India-specific threat landscapes to deliver comprehensive protection.

Today, over 30,000 enterprises across 70+ countries trust Seqrite with their cybersecurity infrastructure. As our latest innovation, SIA combines the best of Indian engineering talent with cutting-edge AI to create a truly global offering. By developing such sophisticated technologies domestically, we aim to not just protect Indian organizations but also to position India as a cybersecurity leader on the world stage.

TimesTech: As AI becomes integral to cybersecurity, how do you see Seqrite leveraging advancements in AI to stay ahead of evolving cyber threats in the coming years?

Vishal: There's no doubt in the fact that the cybersecurity landscape is undergoing a profound transformation in today's increasingly digitized world. AI is acting like a double-edged sword, simultaneously becoming both a powerful defensive tool and a dangerous weapon in the hands of attackers. In our India Cyber Threat Landscape Report 2024, which we prepared in association with DSCI, we shared our predictions for AI to be used to develop highly sophisticated phishing campaigns using deepfake technology and personalized attack vectors in 2025, making them harder to detect.

At Seqrite, we have adopted a two-pronged approach to leverage such AI advancements. On one hand, we are continuously enhancing our detection capabilities by teaching our AI systems to identify AI-generated threats. Our systems are capable of identifying the subtle indicators of deepfakes and AI-crafted phishing attempts that might fool human analysts. On the other hand, we continue to focus on predictive security, where our AI systems anticipate attack vectors before they emerge. This involves training our models on vast amounts of threat data to identify patterns that precede major attack campaigns. Our Data Lake has a rich dataset exceeding 100 TB, which is leveraged for training & validating our machine learning models. On the retail side, the freemium model of our AntiFraud.AI tool ensures optimal protection against spam emails, deepfake attacks, and phishing.

Looking ahead, we continue to invest heavily in adversarial AI research, which essentially means teaching our systems to think like attackers to better defend against them. We are also exploring quantum-resistant encryption to prepare for future threats, aligning with India's quantum encryption migration strategies. I'm confident that in the coming time, Seqrite will continue to stay ahead of evolving cyber threats, protecting our customers not just against today's challenges but tomorrow's as well.