EXPRESS COMPUTER

We're moving from reactive cybersecurity to proactive AI-driven defence: Vishal Salvi, CEO, Quick Heal Technologies

As cyber threats rooted in geopolitical tensions continue to escalate, India's critical infrastructure and enterprise landscape face unprecedented challenges. With a marked rise in state-sponsored cyberattacks and disinformation campaigns—particularly from Pakistan—sectors such as defence, healthcare, finance, and telecommunications are increasingly in the crosshairs. In this rapidly evolving threat environment, the need for robust, sovereign cybersecurity solutions has never been more urgent.

In an exclusive conversation with *Express Computer*, **Vishal Salvi, Chief Executive Officer of Quick Heal Technologies Limited,** offers a comprehensive perspective on how India can counter these growing cyber threats through indigenous innovation. Drawing from decades of experience and leadership in the cybersecurity domain, Salvi outlines the strategic role Quick Heal and its enterprise arm, Seqrite, are playing in building national cyber resilience. From leveraging AI-powered platforms like the Seqrite Intelligence Assistant (SIA) to deploying GoDeep.AI, a self-aware malware hunting technology, Salvi shares how the company is helping enterprises transition from reactive defences to proactive threat hunting. He also highlights the measurable impact these innovations have already made, the importance of reducing reliance on foreign cybersecurity solutions, and how a "Made-in-India" approach is positioning Seqrite as a global contender in enterprise security.

How has Pakistan's growing use of cyber weapons, including disinformation and state-sponsored cyberattacks, affected Indian enterprises and critical sectors?
The impact of Pakistan's cyber warfare capabilities on Indian enterprises has been severe and multifaceted. Following recent geopolitical tensions, we witnessed over 150 hacktivist groups targeting Indian critical infrastructure, with daily attack volumes surpassing 50 incidents. These attacks employed sophisticated methods, including malware campaigns and DDoS attacks, targeting Indian defence establishments, government entities, and critical infrastructure.
Pakistani threat actors, including groups like APT36 (Transparent Tribe), Pakistan Cyber Force, and Team Insane PK, have specifically targeted Indian defence establishments and civilian infrastructure, including airports, power grids, transportation services, telecom networks, and financial platforms. The disinformation campaign has been equally damaging, with coordinated efforts involving deepfake videos, fake advisories, and

doctored content flooding social media platforms. This parallel digital warfare has created what we call a “cognitive battlefield” where perceptions are under siege alongside physical infrastructure. The financial sector has been particularly vulnerable, with the RBI issuing high alerts to banks and NBFCs about potential cyberattacks originating from Pakistan.

Which key sectors in India remain most vulnerable to cyberattacks due to the heightened geopolitical tensions, and how can businesses better safeguard them?
The India Cyber Threat Report 2025, prepared meticulously by our researchers at Seqrite Labs, India’s largest malware analysis facility, has identified some key vulnerable sectors during heightened geopolitical tensions. These include healthcare accounting for 21.82% of all cyberattacks, hospitality at 19.57%, BFSI at 17.38%, and education at 15.64%. Critical infrastructure such as banking, telecommunications, energy grids, transportation networks, and government systems have become prime targets. The healthcare sector’s vulnerability is particularly concerning given its mission-critical nature and the tendency to pay ransoms quickly to restore patient care operations.

To better safeguard these sectors, businesses should implement multi-layered defence strategies including behaviour-based threat detection systems that can identify unknown threats beyond traditional signature-based approaches, ZTNA architectures that assume no inherent trust within networks, real-time threat intelligence sharing between organisations and government agencies, regular security audits and vulnerability assessments, particularly for legacy systems integrated with modern technologies. Also, there should be a greater focus on employee training in order to combat sophisticated social engineering and phishing campaigns.

The convergence of operations technology and information technology systems requires specialised protection, especially in manufacturing and energy sectors, where legacy systems create significant security gaps.

How critical is it for India to have cybersecurity firms like Quick Heal Technologies Limited contributing to national resilience through homegrown technologies?
India’s cyber self-reliance has become a matter of national security, particularly given the astounding increase in state-sponsored cyberattacks in recent years. As a homegrown cybersecurity company with over three decades of experience, Quick Heal Technologies Limited plays a vital role in reducing India’s dependency on foreign security solutions. Our significance lies in providing sovereign technology control where homegrown solutions ensure complete control over security policies, data integrity, and compliance with national cybersecurity regulations without foreign dependencies. Through our Seqrite Labs, India’s largest malware analysis facility, we provide crucial insights into region-specific threats and attack patterns. This strategic autonomy means that indigenous cybersecurity capabilities reduce vulnerabilities that could arise from potential backdoors or dependencies in foreign solutions. The economic security aspect involves building domestic cybersecurity capacity, which strengthens the overall digital economy and reduces the outflow of foreign exchange.

Our collaboration with the US government’s NIST NCCoE Data Classification project demonstrates that Indian cybersecurity companies can compete globally while maintaining sovereignty. Also, our Made-in-India approach ensures that critical national infrastructure is protected by solutions developed with a deep understanding of local threat landscapes and regulatory requirements. The recent surge in cyberattacks during geopolitical tensions

underscores why nations need indigenous cybersecurity ecosystems that can respond rapidly to evolving threats without external dependencies.

How does SIA fit into India's broader national cybersecurity strategy, especially in combating both state-sponsored and hacktivist cyber threats?
SIA addresses a critical gap in India's cybersecurity infrastructure by democratising advanced threat detection and response capabilities. Given that thousands of alerts overwhelm security teams daily, leading to slower response times and increased human error risk, SIA's AI-powered automation becomes strategically important.

In the context of state-sponsored and hacktivist threats, SIA provides accelerated incident response by enabling security analysts to instantly navigate critical incidents and find related threats, matched IOCs, and associated playbooks. Teams can investigate sophisticated APT campaigns and hacktivist activities using conversational queries rather than complex technical interfaces. The system remembers conversations and provides real-time context, crucial for tracking persistent campaigns by groups like APT36 or hacktivist collectives. By automating routine tasks, SIA allows skilled cybersecurity professionals to focus on advanced threat analysis rather than manual correlation work.

This aligns with the NCIIPC's objectives of protecting critical infrastructure through coordinated, technology-enhanced approaches. SIA's ability to provide instant, actionable insights supports the rapid response requirements necessary when dealing with geopolitically motivated cyber campaigns targeting Indian assets. With over 5,842 hacktivist attacks last year targeting the Indian cyber space and over 150 hacktivist groups observed in 2023 alone targeting Indian entities, the scale of threats requires the kind of intelligent automation that SIA provides.

How does SIA represent a "transformative leap" that bridges the gap between human intelligence and generative AI?
SIA combines the analytical capabilities of experienced security professionals with the processing power and pattern recognition of generative AI. This transformation occurs through conversational intelligence, where, unlike traditional security tools that require specialised query languages and technical expertise, SIA enables natural language interaction with complex security data. This democratises threat hunting capabilities across team members with varying technical backgrounds.
The system maintains contextual memory and learning by retaining the last three contextual queries within each session and storing up to 10 recent sessions per analyst. This creates a continuous learning environment where human insights enhance AI capabilities, while AI augments human decision-making speed and accuracy. SIA provides pre-defined prompt questions tailored to help analysts initiate investigations quickly, while allowing for dynamic follow-up queries. This bridges the gap between structured automation and flexible human reasoning.
Unlike traditional AI tools that operate in isolation, SIA maintains a session history that analysts can revisit, pin, and rename for recurring investigations. This creates institutional memory that combines human expertise with AI processing capabilities. The transformative aspect lies in SIA's ability to make advanced cybersecurity analysis accessible to broader teams while amplifying the effectiveness of expert analysts. It represents the evolution from reactive security operations to proactive, AI-enhanced threat hunting that leverages both human intuition and machine intelligence.

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

GoDeep.AI stands out as our proprietary advancement in AI-powered malware detection, distinguished by its self-learning and adaptive capabilities. The technology's self-aware nature stems from deep learning with historical memory, where GoDeep.AI learns and remembers every historical malware threat, storing these learnings in a centralised cloud infrastructure. This creates an evolving knowledge base that continuously improves detection accuracy based on past encounters.
The system provides predictive detection capabilities where the AI algorithm works in conjunction with behavioral detection technology to monitor and track program activities in real-time. This enables the system to identify and block programs with suspicious behavior patterns, even for threats that have never been encountered before, providing true zero-day protection. GoDeep.AI integrates artificial intelligence, deep learning, behavioral detection, and predictive analytics into a unified detection engine. This comprehensive approach ensures that malware cannot easily evade detection by exploiting single-point vulnerabilities.
Unlike traditional signature-based systems that rely on known threat databases, GoDeep.AI evolves in real-time as it encounters new attack vectors. This self-awareness allows the system to anticipate emerging threats rather than simply reacting to them. The cloud-based learning model enables rapid knowledge distribution across all protected endpoints, ensuring that threat intelligence discovered at one location immediately benefits the entire network. This self-aware malware hunting capability is particularly crucial in today's threat landscape, where polymorphic malware, fileless attacks, and advanced persistent threats require intelligence that can adapt faster than traditional security measures.

What measurable improvements in incident response time or analyst productivity have early users of SIA reported?
The first version of SIA was launched in May, and we have already started seeing improvements in analyst productivity of approximately 20% in incident response. SIA is now an assistant to the SOC analyst, helping them analyse the event faster and more efficiently. With future improvements, we would be moving upwards in productivity and efficiency improvements, not replacing the analyst but making them wiser and smarter in their decision-making and actions.

How does SIA reinforce Seqrite's positioning as a "Made-in-India" solution for global enterprise cybersecurity?
SIA is in line with Seqrite's commitment to developing world-class cybersecurity innovation from India while addressing both domestic and global security challenges. Our positioning as a "Made-in-India" solution is reinforced through indigenous AI development, where SIA represents cutting-edge generative AI capabilities developed entirely within India by our engineering teams. This is our way of showing the world that Indian cybersecurity companies can create solutions that compete with global leaders while maintaining complete technological sovereignty.

Built on insights from Seqrite Labs, India's largest malware analysis facility, SIA incorporates region-specific threat patterns and attack vectors. This local intelligence enhances the platform's effectiveness for Indian enterprises while providing valuable insights for global customers facing similar threat actors. SIA integrates seamlessly with our full-stack cybersecurity architecture, including endpoint protection, XDR, ZTNA, and MDR services. This end-to-end capability, developed entirely in India, stands as a testament to our ability to deliver enterprise-grade solutions without dependencies on foreign technologies. The "Made-in-India" advantage becomes particularly relevant as organisations worldwide seek to reduce dependencies on solutions from geopolitically

sensitive regions, making Seqrite an attractive alternative for sovereign cybersecurity needs.

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?
The future of cybersecurity lies in the intelligent convergence of AI capabilities with deep threat understanding, and Seqrite is positioned to lead this transformation through several strategic initiatives. We're advancing beyond reactive security toward predictive analytics that can anticipate emerging attack vectors. Our AI systems will increasingly identify threat patterns before they fully manifest, enabling proactive defence rather than incident response.

Building on SIA's foundation, we envision security platforms that can autonomously detect, analyse, and respond to threats with minimal human intervention. This evolution will be crucial as cyberattacks become more sophisticated and faster-moving. Our GoDeep.AI technology will continue evolving to become more self-aware and adaptive, learning from global threat intelligence while maintaining the ability to identify novel attack methods. This includes defending against AI-powered attacks where adversaries use machine learning to evade traditional detection.

Our AI systems will facilitate better threat intelligence sharing between organisations and sectors, creating a collective defence ecosystem powered by machine learning insights. The key to staying ahead lies in maintaining our commitment to innovation while ensuring that AI enhancements remain accessible, reliable, and aligned with India's strategic cybersecurity objectives. As cyber threats increasingly leverage AI, our defence systems must evolve not just to match but to surpass the sophistication of adversarial AI capabilities.