Seqrite CEO Vishal Salvi on AI-Led Cybersecurity and India's Digital Future

In an interview with TimesTech, Vishal Salvi, CEO of Quick Heal Technologies, discusses the evolving cyber threat landscape in India and how Seqrite is leveraging AI, machine learning, and behavior-based detection to stay ahead. From countering zero-day attacks to enabling compliance with the DPDP Act, he outlines Seqrite's vision of making cybersecurity smarter, scalable, and accessible across enterprises and MSMEs alike.

TimesTech: India has witnessed 369.01 million cyber threat detections, with trojans accounting for 43.38% of all attacks. What key factors are driving this surge in cyber threats, and how have attack patterns evolved in recent years?

Vishal: The cybersecurity landscape in India today is defined by two factors – opportunity and vulnerability. Our digital economy is booming, and is projected to contribute 20% to GDP by 2026. However, at the same time, this growth has outpaced our collective security maturity. Cybercriminals are observing this and capitalizing on it.

To make matters worse, the democratization of hacking tools has lowered barriers to entry. Geopolitical tensions are also increasingly playing out in cyberspace. State-sponsored groups like Lazarus and APT41 now target Indian infrastructure with surgical precision, blending ransomware with espionage. Furthermore, IoT expansion has created new vulnerabilities. Our researchers at Seqrite Labs, India's largest malware analysis facility, recorded a 59% spike in IoT attacks this year alone, which is a concerning figure.

TimesTech: With cyberattacks becoming more targeted and sophisticated, how should enterprises rethink their cybersecurity strategies beyond traditional defenses?

Vishal: AI-powered cyber threats like the BlackMamba keylogger represent a paradigm shift in the security landscape, using AI for evasion and payload generation to create polymorphic malware that adapts to defenses in real time. To combat these threats, organizations must move beyond signature-based detection, which represents 85% of current detections but cannot keep pace with evolving attack patterns.

To counter this, organizations must prioritize behavior-based detection that identifies malicious activity based on patterns rather than static signatures. Our data shows a 974.6% surge in behavior-based detections since 2021, highlighting its growing necessity. AI-driven predictive analytics further strengthen security by detecting emerging risks before they escalate.

The human element remains critical, with awareness training evolving to counter AI-generated social engineering attacks. At Seqrite, our XDR solutions leverage machine learning (ML) models to detect and neutralize AI-driven cyber threats effectively. Beyond this, we are developing unsupervised ML models that learn autonomously from vast datasets of malicious activity, enabling real-time anomaly detection.

Looking ahead, we are advancing "AI for AI"—experimental AI models designed to detect and neutralize AI-generated attacks, ensuring proactive defense against the next generation of cyber threats.

TimesTech: Seqrite's Malware Analysis Platform (SMAP) and Threat Intel (STI) aim to provide proactive threat detection and response. How do these solutions enhance an organization's security posture, especially against zero-day threats?

Vishal: Seqrite Malware Analysis Platform (SMAP) employs advanced multi-stage processing to detect and neutralize unknown threats with precision. It begins with static analysis, where file structures are examined without execution to detect suspicious patterns, followed by dynamic analysis in isolated sandboxes, allowing files to be safely executed to observe real-time behavior. The system accurately classifies malware types, such as viruses, ransomware, and trojans, while analyzing their intended purpose, persistence, command-and-control (C2) communication, and destructive actions like data theft or system disruption. By identifying zero-day threats that evade traditional signature-based detection, SMAP enables proactive defenses against emerging cyber risks. Its strength lies in correlating findings across multiple detection engines and leveraging advanced machine learning capabilities, continuously improving through insights from an 8.44-million-strong installation base.

Seqrite Threat Intelligence (STI) delivers context-rich, actionable insights tailored to India's threat landscape, something global feeds often overlook. Unlike generic threat intelligence, STI provides industry-specific analysis, helping organizations prioritize defenses against the most relevant threats. Our investigation into Operation Celestial Force uncovered targeted attacks on Indian government entities using sector-specific lures. With intelligence on over 150 hacktivist groups targeting Indian organizations, STI offers early warnings and geopolitical cyber risk insights to stay ahead of emerging threats.

What sets STI apart is its seamless integration across the Quick Heal security ecosystem, ensuring high-fidelity intelligence. With real-time visibility from 9 million+ endpoints, STI provides unparalleled insight into evolving cyber threats, enabling Indian organizations to strengthen their cybersecurity posture with immediate, actionable intelligence. STI supports STIX and TAXII formats, which shall be consumed through any Threat Intelligence Platforms or can directly be integrated to Security Platforms.

TimesTech: How is Seqrite leveraging AI and machine learning to strengthen threat detection, automate responses, and mitigate advanced cyber risks?

Vishal: As AI natives, all Seqrite solutions are powered by GoDeep.AI – a self-aware, malware-hunting technology that is capable of spotting patterns invisible to human analysts. It can detect anomalous DNS queries to newly registered domains, flagging reconnaissance activity before data exfiltration begins. This auto-remediation has been truly transformative. We are also leveraging ML for predictive defense, especially for analyzing dark web chatter, historical attacks, and system telemetry, and forecasting attack vectors.

In my opinion, using newer technologies such as AI and ML isn't about replacing humans but empowering them. We maintain rigorous human oversight in our operations. Every AI decision is reviewed by our Threat Ops team – a necessary check against adversarial AI attacks. The automation, however, has been truly transformative for our users. The quick and comprehensive overview of incidents, attack timelines, and recommended actions cuts down response planning from hours to minutes.

TimesTech: Compliance with evolving data protection regulations is a major challenge for enterprises. How does Seqrite help organizations stay compliant with the DPDP Act and global security standards?

Vishal: Compliance is the floor, not the ceiling. Our approach aligns security with regulations through four pillars. At Seqrite, we offer solutions to help organizations comply with the DPDP Act and other global data protection regulations. Automated data discovery is a key feature of Seqrite's Data Privacy solution, enabling businesses to discover, categorize, and manage sensitive information across endpoints, cloud environments, and legacy systems. These features are aligned with the DPDP Act's requirements for managing personal data effectively.

Our Data Loss Prevention (DLP) solutions also play a critical role in compliance by preventing leaks of confidential data. These solutions enforce security policies across physical devices and web applications, ensuring sensitive information remains protected within organizational boundaries. But where we truly differentiate is incident response. Our tools provide automated reporting workflows that detail impacted data subjects and root causes during breaches, helping organizations meet the DPDP Act's 72-hour reporting mandate.

TimesTech: As the CEO of Quick Heal Technologies, what is your long-term vision for Seqrite, and how do you see the future of enterprise cybersecurity evolving in India and globally?

Vishal: At Seqrite, our vision has been to make impactful contributions to India's digital transformation. We have designed platforms like SMAP and STI to provide proactive threat detection capabilities using advanced analytics and machine learning algorithms. Cyber immunity for all – launching affordable AI-powered protection for MSMEs – remains a key priority for us, because we firmly believe that comprehensive security against emerging threats shouldn't be a luxury. We also take immense pride in the global-local synergy that we have achieved – while expanding our footprint worldwide, we continue to deepen our roots in India.

The future demands cyber-physical convergence. As smart cities and IIoT expand, we are investing extensively in Operational Technology (OT) security solutions. Our work with NIST NCCoE on AI safety standards positions us to lead this transition. In India specifically, we expect three trends to dominate the cybersecurity landscape. Generative AI attacks will necessitate AI-augmented defenses, cyber resilience mandates will emerge, and there will be a greater focus on talent development in the cybersecurity domain. At Seqrite, we are already making solid progress with respect to all these future trends.

While the road ahead is challenging, we remain optimistic about the future of cybersecurity in India and across the globe. By making security simple, smart, and sustainable, Seqrite will empower businesses to innovate fearlessly. Because in our digital future, security isn't just about protection; it is about enabling progress.