BW SECURITY WORLD

Seqrite Unveils Key Cybersecurity Initiatives at 19th Annual AISS

The report highlights 369 million malware detections from an installation base of 8.44 million devices in India, underscoring the nation's cybersecurity challenges

Seqrite, the enterprise division of Quick Heal Technologies Limited, introduced major cybersecurity advancements at the 19th nasscom-DSCI Annual Information Security Summit (AISS) 2025. The announcements reflect Seqrite's focus on strengthening India's digital infrastructure to combat an ever-evolving cyber threat landscape.

At the core of its presentation was the launch of the *India Cyber Threat Report 2025*, a comprehensive study conducted in collaboration with the Data Security Council of India (DSCI). The report offers a detailed analysis of the cyber threat environment in India, shedding light on the rising scale of attacks and vulnerabilities.

The report highlights 369 million malware detections from an installation base of 8.44 million devices in India, underscoring the nation's cybersecurity challenges. Signature-based methods accounted for 85.44 per cent of detections, while behaviour-based methods contributed 14.56 per cent, emphasising the growing need for adaptive security techniques.

Malware detections were broken down into subcategories, with Trojans leading at 43.38 per cent, followed by Infectors at 34.23 per cent. Android-based threats were another significant concern, with malware comprising 42 per cent of detections, followed by Potentially Unwanted Programs (PUPs) at 32 per cent, and adware at 26 per cent. Telangana, Tamil Nadu, and Delhi emerged as the most affected regions, while the BFSI, healthcare, and hospitality sectors were identified as the most targeted industries.

Seqrite also introduced its advanced *Seqrite Malware Analysis Platform (SMAP)*, designed to provide detailed insights into suspicious files and URLs that evade traditional detection methods. SMAP uses isolated virtual environments to perform static and dynamic analyses safely, supported by advanced sandboxing technology and real-time behavioural analysis. It integrates seamlessly with existing security infrastructures such as SIEM, SOAR, and EDR/XDR platforms, offering a comprehensive threat response system.

Another highlight was the launch of *Seqrite Threat Intel*, a real-time cyber defence hub powered by Seqrite Labs, India's largest malware analysis centre. The platform aggregates threat intelligence from diverse sources, including open-source intelligence (OSINT) and Computer Emergency Response Teams (CERTs). It leverages Seqrite's extensive endpoint network to provide real-time insights and contextualise threats based on specific industries.

Commenting on the announcements, Vishal Salvi, CEO of Quick Heal Technologies Limited, said, "The unveiling of the *India Cyber Threat Report 2025* alongside Seqrite Malware Analysis Platform and Seqrite Threat Intel solution represents our comprehensive approach to addressing the evolving cybersecurity challenges faced by Indian businesses. These solutions are not just about responding to threats but anticipating them. I sincerely thank DSCI and our dedicated experts for advancing excellence in cybersecurity and ensuring our clients stay ahead in this digital arms race."

Vinayak Godse, CEO of DSCI, added, "The *India Cyber Threat Report 2025* provides a detailed view of India's cyber threat landscape, offering insights across states, cities, infrastructures, and industry segments. The growing demand for behaviour-based malware detection reflects the sophistication of attacks and the evolution of defence strategies. This report is a strategic tool for organisations to navigate the dynamic threat environment. We are delighted to collaborate with the Quick Heal team on this initiative."

These announcements come at a critical time as threats like AI-driven attacks, cloud vulnerabilities, and advanced ransomware campaigns become more prominent. Seqrite's integrated approach, combining threat intelligence, advanced malware analysis, and proactive defence mechanisms, aims to equip Indian businesses and government entities with robust tools to address both current and future cybersecurity challenges.