Seqrite Issues Urgent Cybersecurity Warning Following the Disclosure of Anthropic's Claude Mythos AI Model

Seqrite, the enterprise security arm of Quick Heal Technologies Limited, today issued a critical advisory to enterprises and financial institutions in response to the public revelation of Anthropic's "Claude Mythos" AI model. This advanced AI can autonomously discover and weaponise zero-day vulnerabilities in critical software infrastructure, signalling a permanent and concerning shift in the global cybersecurity threat model.

Anthropic's recent disclosures and the launch of the defensive "Project Glasswing" initiative highlight an alarming reality: the window between a vulnerability being discovered and exploited has collapsed from months to mere hours. With industry experts predicting that unregulated, open-weight AI models could reach comparable capabilities within six months, Seqrite warns that malicious actors will soon possess unprecedented power to launch automated cyberattacks at machine speed and scale.

Addressing the urgent need for a significant shift in enterprise cyber defence and echoing concerns raised by regulators, **Dr. Sanjay Katkar, Joint Managing Director of Quick Heal Technologies Limited**, stated: *"The Reserve Bank of India's assessment of risks around advanced AI models such as Anthropic's Claude Mythos reflects a critical inflection point in cybersecurity. These systems are not just analytical tools; they have demonstrated the capability to identify and potentially exploit software vulnerabilities at a speed and scale that far exceeds traditional threat actors. Recent global developments indicate that such models can uncover thousands of weaknesses across core systems, raising concerns about accelerated and automated exploitation, particularly in complex sectors like banking.*

From a cybersecurity perspective, this fundamentally shifts the threat model. As highlighted in the India Cyber Threat Report 2026, India is already witnessing 265.52 million detections across over 8 million endpoints, with threats increasingly driven by automation, AI-assisted phishing, and identity compromise. When combined with advanced AI capabilities, this creates a scenario where vulnerabilities can be discovered, weaponised, and deployed in near real time.

Organisations must respond by moving beyond reactive security to predictive and intelligence-led defense. This includes adopting continuous vulnerability assessment, AI-driven threat correlation, and zero-trust identity frameworks. Equally critical is strengthening secure coding practices and reducing patch latency, as AI models can exploit even short windows of exposure. From a resilience standpoint, financial institutions must treat AI as both a tool and a threat surface. Investments in behavioural monitoring, real-time anomaly detection, and external threat intelligence will be key. In an AI-driven threat landscape, the ability to anticipate and neutralise risks before exploitation will define the next frontier of cyber resilience."

The emergence of AI models capable of bypassing advanced security controls, such as autonomously chaining vulnerabilities to break out of browser sandboxes or discovering 27-year-old flaws in core internet plumbing, means that legacy security postures are no longer viable.

Seqrite strongly advises all enterprise Governance, Risk, and Compliance (GRC) and security teams to take immediate action:

- **Review Patch SLAs**: Standard operational timelines are obsolete. Critical internet-facing patches must be deployed within 72 hours.
- **Re-evaluate Vendor Risk**: Third-party risk assessments must now include AI-augmented vulnerability exposure, as foundational open-source dependencies are increasingly on the front lines.
- **Update Incident Response**: Playbooks designed for human threat actors must be revised to account for AI finding and exploiting zero-days at an unprecedented scale.

As the global threat surface expands, Seqrite remains committed to empowering enterprises with DPDP Act-compliant security solutions, predictive threat intelligence, behavioural monitoring, and strong zero-trust frameworks to anticipate and neutralise these advanced risks before they can be executed.