HealthManagement
Promoting Management and Leadership

Agentic AI and the Future of Cybersecurity

The cybersecurity landscape is on the brink of a transformation unlike any before. The advent of agentic AI—artificial intelligence capable of reasoning, planning and acting autonomously—introduces both powerful defensive capabilities and heightened risks. As these AI-driven systems become widely accessible, they will redefine the cyber battlefield, empowering both security professionals and malicious actors alike. With ransomware attacks already evolving in complexity and new cyber threats emerging, organisations must reassess their security strategies to withstand the challenges of an AI-powered world. The ability of autonomous AI systems to operate with minimal human intervention means that security teams must prepare for a scenario where cyber defences and attacks are increasingly automated, intensifying the ongoing cybersecurity arms race.

The Rise of Agentic AI in Cybersecurity

Unlike traditional AI models that rely on user input, agentic AI operates independently, making it more akin to a human colleague than a simple tool. These intelligent systems can monitor networks, detect vulnerabilities and execute defensive protocols without direct human intervention. For cybersecurity teams struggling with personnel shortages, such automation promises enhanced threat detection and rapid response capabilities. AI-driven security systems can continuously analyse network activity, identify potential breaches and take preventive action before an attack materialises, reducing the burden on human analysts. However, the same autonomy can be leveraged by cybercriminals, who can deploy AI agents to conduct large-scale attacks with minimal effort.

Must Read: ***Strengthening Cybersecurity in Healthcare: HIMSS Insights***

The ability to navigate networks, exploit weaknesses and execute malware without direct human oversight could fundamentally shift the balance of power in cybersecurity. With cybercriminals gaining access to AI tools capable of automating attacks, the speed and scale of cyber threats are likely to increase significantly, forcing organisations to rethink their defensive strategies.

The Changing Ransomware Landscape

While AI-driven threats loom, ransomware remains a persistent and evolving challenge. The dismantling of major ransomware groups like LockBit and ALPHV in 2024 led to the emergence of smaller, unpredictable actors who now dominate the field. The decentralisation of ransomware operations has made attacks more frequent, with an increasing number of groups gaining access to sophisticated ransomware tools. This shift has led to a surge in cyberattacks, with ransom payments reaching unprecedented levels. The ease of entry into ransomware operations means that organisations now face a more fragmented and less predictable threat landscape, demanding more proactive security measures.

Businesses must recognise that the disappearance of large, organised ransomware groups has not lessened the risk; rather, it has resulted in a more chaotic and decentralised environment where smaller groups operate independently, making them harder to track and neutralise. As more criminals adopt ransomware tactics, the volume of attacks continues to rise, putting further strain on already overstretched security teams and requiring a more comprehensive approach to cyber resilience.

New Tactics Reshaping Cyber Attacks

Cybercriminals have refined their attack strategies to maximise efficiency and effectiveness. Ransomware groups now favour late-night intrusions, taking advantage of reduced IT staffing during early morning hours. Attack cycles have also accelerated, with breaches progressing from initial access to full system encryption in mere hours. Furthermore, attackers increasingly rely on legitimate software tools—commonly referred to as "living off the land" tactics—making it harder for security systems to differentiate between normal and malicious activity. The use of

commercial remote access software further complicates detection efforts, as these tools blend seamlessly into corporate environments. These evolving strategies highlight the need for organisations to move beyond traditional antivirus solutions and adopt behaviour-based detection methods to counteract emerging threats.

Defensive strategies must adapt to focus on identifying and stopping suspicious behaviour rather than merely blocking known malicious software. Additionally, businesses must ensure that their security measures account for vulnerabilities in widely used remote access tools, as attackers continue to exploit these avenues to gain initial entry. As cybercriminals refine their methods, organisations must prioritise continuous monitoring and proactive defence strategies to prevent small intrusions from escalating into full-scale attacks.

The convergence of AI-driven threats and evolving ransomware tactics presents an urgent need for adaptation. The organisations that embrace advanced security measures—such as 24/7 monitoring, AI-driven defensive strategies and behaviour-based threat detection—will be better equipped to counteract the growing sophistication of cyber threats. The ability to navigate this new digital battleground will ultimately determine which entities thrive in an era where agentic AI dictates the rules of engagement. Businesses must recognise that the cyber threat landscape is evolving rapidly, requiring a proactive rather than reactive approach to security. The organisations that successfully implement AI-driven defence mechanisms while staying ahead of emerging attack tactics will be in the best position to safeguard their networks and data. With cybercriminals increasingly relying on AI-driven automation, the future of cybersecurity will depend on which side harnesses these tools most effectively. In this evolving battle, vigilance, adaptability and innovation will be key to maintaining a secure digital environment.

Source: **Digital Health Insights**

Image Credit: **iStock**

Published on : Mon, 10 Mar 2025