Lack of skilled professionals, not cost, the principal barrier to adoption of AI among Asia-Pacific businesses: LogRhythm channel partners

SINGAPORE, 22 November 2023 – At its recent Asia-Pacific Tech University event in Bangkok, Thailand, LogRhythm gathered the insights of its channel partners around their approach and perceptions of AI, including opportunities and fresh risks for businesses arising from AI's capacity to enhance business operations.

The survey found that the main challenge to AI adoption is the lack of skilled AI professionals within organisations. Specifically, 35% of respondents pinpointed the absence of skilled AI professionals as the top obstacle, followed by integration with existing systems (23%). Interestingly, cost was not a major barrier to adoption, with only 15% sharing that their AI adoption efforts are hindered by cost-related issues.

"Despite the advantages AI offers in terms of automation, human expertise remains paramount in bridging the gap between the capabilities of an AI solution, and an organisation’s unique requirements," said Joanne Wong, Vice President, International Markets, LogRhythm.

Nevertheless, the survey revealed that the momentum for adopting AI tools and technology is building. Over a third of LogRhythm’s channel partners shared that their clients are now using AI tools, and notably, around two-thirds employ AI in their operations, signalling that operational efficiency is the primary impetus for these AI deployments.

AI a Double-Edged Sword in Cybersecurity

For all the optimism around the promise of AI in driving operational efficiency, concerns remain around the security threats that the AI boom has enabled. In fact, a significant 62% of respondents believe that AI results in a moderate expansion of the current threat surface.

Data privacy concerns have been a major hurdle for enterprises seeking to adopt AI, particularly when it comes to the use of publicly-available large language models (LLMs). 47% of channel partners express grave concerns about AI tools causing data leaks. Additionally, 18% are particularly anxious about potential leaks of proprietary business data.

Businesses have been proactively addressing these looming threats, however. The survey indicates that they have been mitigating risks by undertaking risk assessments and laying down internal AI usage policies and guidelines, with both actions at 28%.

Singapore’s National Cyber Threat Analysis Centre recently reported that cybercriminals have increasingly turned to generative AI platforms for crafting potent ransomware, and are manipulating AI tools for their nefarious activities. This concerning trend underscores the dangers of AI tools becoming fresh vectors for data breaches.

"It is reassuring to see businesses take measures like risk assessments and provision of internal guidelines. While the potential of AI to transform operational efficiencies and drive bottomline is immense, it is just as important that businesses take a measured approach to the adoption of AI," Wong noted.

"This includes managing the associated security and privacy risks associated with its implementation, acknowledging that the threat landscape has significantly increased with the availability of nefarious AI, and investing in the right tools and resources that can monitor and action on potential threats at speed and scale" added Wong.

About LogRhythm

LogRhythm aids security teams in stopping breaches by converting scattered data and signals into reliable insights. Whether connecting the dots across varied log and threat intelligence sources or employing advanced machine learning to detect anomalies in network activity and user behaviour, LogRhythm precisely identifies cyber threats, enabling professionals to act swiftly and effectively. With flexible deployment options both in the cloud and on-premises, seamless integrations, and advisory services, LogRhythm ensures rapid value realisation and adaptability to an ever-changing threat scenario. In collaboration with LogRhythm, clients can confidently monitor, detect, investigate, and counteract cyber threats. Discover more at logrhythm.com.