How Cloud-Based AI is Combatting Modern Day Cyber Threats

Dubai - Dec 16, 2017: Organisations face a growing number of increasingly complex and ever-evolving threats – and the most dangerous threats are often the hardest to discover. Take the insider threat or stolen credentials, for example. We've seen many high-profile attacks stem from the unauthorised use of legitimate user credentials, which can be extremely difficult to expose. Organisations are under growing pressure to detect and mitigate threats like these as soon as they have been compromised – and this pressure will be amplified when the General Data Protection Regulation (GDPR) is enforced on 25th May 2018.

Security teams have a critically important job. They need to be able to protect company data, often without time and money on their side. Another common problem is finding enough cyber-security skilled employees, which means they end up doing more with fewer resources. They simply cannot afford to spend time on extensive manual threat-hunting exercises or deploying and managing multiple, disparate security products.

Out with the old, in with the new

The perimeter-based model of yesterday is insufficient for the mammoth task of protecting a company's assets. Instead, we are starting to see a shift towards automation and the application of cloud-based Artificial Intelligence (AI), which is fast becoming critical in the fight against modern cyber threats. In fact, a recent IDC report predicted that the AI software market would grow at a CAGR of over 39 percent by 2021, whilst separate research from the analyst firm stated that the future of AI requires the cloud as a foundation, with enterprise 'cloud first' strategies becoming more prevalent over the same period.

The cloud is, without doubt, transforming security by enabling easy and rapid customer adoption, saving time and money, and providing companies with access to a class of AI-enabled analytics that are not otherwise technically practical or affordable to deploy on-premise. Plug-and-play implementation lets security teams focus on their mission instead of spending valuable time implementing and maintaining a new tool.

What's more, when deployed in the cloud, AI can benefit from collective intelligence and a broader perspective to maximise intelligence. Imagine incorporating real-world insight into specific threats in real time. This will advance the ability of AI-powered analytics to detect even the stealthiest or previously unknown threats more quickly, and with greater accuracy than ever before.

Why cloud-based AI?

By combining a wide array of behavioural models to characterise shifts in how users interact with the IT environment, cloud-based AI technology is helping organisations pursue user-based

threats, including signatureless and hidden threats.

Applying cloud-based AI throughout the threat lifecycle will automate and enhance entire categories of work, as well as enable increasingly faster and more effective detection of real threats. Take analytics, for example. Hackers are constantly evolving their tactics and techniques to evade existing protective and defensive measures, targeting new and existing vulnerabilities and unleashing attack methods that have never been seen before. Cloud AI is beginning to play an important role in detecting these emerging threats. The technology is proactive and predictive, without the need for security and IT personnel to configure and tune systems, automatically learning what is normal and evolving to register even the most subtle changes in events and behaviour models that suggest a breach might be occurring.

Cloud-based AI essentially helps security analysts cut through the noise and detect serious threats earlier in their lifecycle so that they can immediately be neutralised. It provides rapid time-to-value through cloud delivery, and promises to eliminate or augment a considerable number of time-consuming manual threat detection and response exercises. This allows security teams to drive greater efficiency by focusing on the higher-value activities that require direct human touch.

ENDS

About LogRhythm:
LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented award-winning threat lifecycle management platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for five consecutive years, named a 'Champion' in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, received SC Labs 'Recommended' 5-Star rating for SIEM and UTM for 2016 and earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award.

LogRhythm is headquartered in Boulder, Colorado, with operations throughout North and South America, Europe and the Asia Pacific region.

For media enquiries, please contact:
Layth Dajani
Office: +971 (4) 447 2501
E-mail: layth@tcf-me.com

THECONTENT|FACTORY
http://www.tcf-me.com/