For immediate release...for immediate release...for immediate release...for immediate release...

Machine Learning: The Next Step in Cyber Security

Detect and respond to user-based threats with artificial intelligence

Dubai - Apr 09, 2018: <p><em><a href="http://www.tcfnewswire.net/en/company/logrhythm/executive-biographies/mazen-a-dohaji-regional-director-mena-logrhythm">Mazen Dohaji</a>, Regional Director for Middle East, Turkey &amp; Africa, LogRhythm</em></p>

<p>Your organisation’s biggest asset could also be its biggest risk: its people.</p>

<p>In fact, according to a recent study of employees in the Middle East, Turkey and Africa, only 18% of respondents were fully aware of the IT security policies and rules in the organisations for which they work.</p>

<p>Most security products set up checkpoints at your network’s perimeter to prevent external threats from slipping in undetected. But few are designed to detect and respond to threats brewing within the bounds of your firewall. Compromised accounts, administrator abuse and misuse, negligent users and employees with malicious intent are just some of the insider threats that could jeopardise your brand, its reputation and its finances.</p>

<p>Because most organisations don’t monitor their internal network traffic, once inside, an attacker can conduct reconnaissance and collect data over time. The target information can then be packaged and moved out of the network all at once; by the time the alarm bells start going off it is too late, and the data is gone.</p>

<p>In such cases early detection is key. The first thing an organisation needs to catch insider threats is network visibility. Internal network traffic, access logs and policy violations need to be monitored closely for suspicious activity.</p>

<p>Your analysts need to know what a regular day looks like on your network. They need to know how much traffic to expect, who is expected to access sensitive information and what applications are used in the day-to-day business operations. Anything that falls outside of these norms should be investigated.</p>

<p>But considering the sheer volume of information and alerts security systems serve up, this could prove a needle-in-a-haystack scenario for analysts; how can they tell when something is happening within the environment that shouldn’t be?</p>

<p><strong><em>UEBA and cyber security</em></strong></p>

<p>The use of data analytics has now graduated to the forefront of securing IT infrastructure. Organisations are now deploying big data techniques to baseline the performance of an environment and detect anomalies that indicate attacks.</p>

<p><a href="http://www.tcfnewswire.net/en/company/logrhythm/interviews/general-data-protection-regulation-for-security-in-the-middle-east-and-africa">User Entity Behaviour Analytics</a> (UEBA) platforms first determine ‘normal’ activities specific to the organisation and its users. Then these UEBA tools quickly discern deviations from that norm that require further exploration. That is, they spotlight cases in which abnormal behaviour is underway.</p>

<p>UEBA tools can keep a track of where people usually log in from, what applications or file servers they use, what is their degree of access and other such information. These tools then gauge if a certain activity performed by a user is different from their daily tasks. If something doesn’t comply with the baseline, UEBA detects it and sends out alerts.</p>

<p>So far, UEBA has proved itself to be an indispensable asset in the world of cyber security. The UEBA market has doubled each year, with Gartner estimating its growth from USD 50 million in 2015 to USD 100 million in 2016, to USD 200 million by the end of last year.</p>

<p>&nbsp;</p>

<p><strong><em>How machine learning helps</em></strong></p>

<p>Artificial intelligence (AI) and machine learning (ML) models build baselines of normal behaviour for each user by looking at historical activity and comparisons within peer groups. Users at high risk are surfaced to analysts to enable them to quickly investigate the user’s behaviour in the context of their role and responsibility within the organisation.</p>

<p>Such solutions can quickly process huge unstructured and hybrid datasets, as well as reduce the time for investigating attacks and produce fewer false</p>

<p>positives. Machine learning algorithms can make security systems self-learning and augment human decision-making.</p>

<p>Incidentally, using a cloud-based ML tool can provide an organisation with significant additional benefits: it can reduce the cost of adoption compared with an on-premise deployment as it will require much less configuration before being put to work. Using a cloud-based delivery model also allows experience and knowledge gleaned in one place to be put to work in others.</p>

<p>These techniques not only throw up genuine alerts with a greater degree of accuracy, but most solutions have also automated the shutdown of malicious activity so that the problem is nipped in the bud in near real-time.</p>

<p>By working effectively together, AI and a skilled security team can be the most important tools in the war on cybercrime. UEBA frees up resources to concentrate on doing the things that humans need to do, such as working on the security strategy, applying patches, fixing vulnerabilities, responding to threats and more.</p>

### 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:
Frances Manabat
Office: +971 (4) 447 2501
E-mail: frances@tcf-me.com

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