datacentrix

Reducing cyber risk with next-gen technology

The attack surface within the cybersecurity landscape is ever expanding and gaining in complexity, meaning that today, the securing and tracking of sensitive data is of the utmost importance – perhaps more than ever before.

“In fact,” explains Gideon Viljoen, Datacentrix Presales Specialist: ICT Security, “with the introduction of legislation such as the Protection of Personal Information Act (POPIA), organisations can be penalised for not taking every conceivable measures to ensure that data is protected and secured.

“Add to this the fact that businesses are moving from an on-premise environment to the cloud, allowing users access to data sets and information to be used for daily activities, and it's clear that it is becoming increasingly challenging to control and protect information.”

All these challenges are further exacerbated by the current global shortage of cybersecurity skills, which is a serious growing concern, Viljoen explains.

“Maintaining control and an audit trail of cybersecurity activities can be daunting and expensive if you are investing in human resources to manage and maintain this on your behalf. And it's not just the skilling up of cybersecurity staff that is a challenge – retaining knowledgeable staff is another problem area, as experts in this field are frequently poached by the highest bidder.

> The use of AI and ML technologies and techniques can assist the human resources with the 'heavy lifting' of sifting through the data, analysing it much faster, making a decision based on collected artefacts, and only requiring human interaction for the verification of the presented artefacts.

Reducing cyber risk with AI & ML:

- Combat alert fatigue
- Improve the quality of alerts
- Decrease false positives
- Automate repetitive tasks

AI and ML are helping under-resourced cybersecurity teams stay ahead according to Mimecast's 7th Annual State of Email Security Report:

50%

more accurate threat detection

49%

improved ability to block threats

48%

faster remediation post attack

“Furthermore, with the sheer amount of data flowing through our organisations on a daily basis, with millions, if not sometimes billions, of alerts and notifications pinging through, 'alert fatigue' has become a real challenge.

Unfortunately, this can equate to significant threats sometimes being missed due to the 'noise' of it all, as it becomes more difficult to identify actionable threats from false positives.”

This being said, Mimecast's 7th Annual State of Email Security Report offers some optimism amongst all of these worries, stating that artificial intelligence (AI) and machine learning (ML) are helping under-resourced cybersecurity teams stay ahead of the curve.

The report states that 92 percent of companies are either using or plan to use AI and ML to bolster their cybersecurity. Forty-nine percent of those surveyed are already using some combination of these technologies (compared to 46 percent last year and just 38 percent the year before). It also says that, amongst the companies already using AI/ML, more accurate threat detection (50 percent), an improved ability to block threats (49 percent), and faster remediation when an attack has occurred (48 percent) are viewed as the three biggest benefits.

In addition, most SOES participants (81 percent) agree that AI systems that are able to provide real-time, contextual warnings to email and collaboration tool users would be a huge boon. Twelve percent went so far as to say that the benefits of such a system would revolutionise the ways in which cybersecurity is practiced.

Says Viljoen: “The use of AI and ML technologies and techniques can assist the human resources with the 'heavy lifting' of sifting through the data, analysing it much faster, making a decision based on collected artefacts, and only requiring human interaction for the verification of the presented artefacts.

“AI and ML toolsets are becoming extremely useful for our everyday lives and businesses alike, helping to combat alert fatigue, decrease false positives, automate repetitive tasks and improve the quality of alerts to the human for verification.

“These valuable tools play an important supporting role, assisting cybersecurity professionals to do more with less and allowing them to deliver peace of mind in an ever-changing world,” he concludes.

For more information, please contact Elzette du Preez on edupreez@datacentrix.co.za