vmblog.com

Technology News and Information

November 29, 2021

By Arindam Ray Chaudhuri, COO at AgreeYa Solutions

How AI Can Help Your Business Stay a Step Ahead of Cyber attackers

Questions you should ask your cybersecurity vendor

AI offers speed and accuracy that organizations can leverage to ensure cybersecurity. AI-enabled cyber security solutions are capable of noticing and reacting to potential cybersecurity issues more quickly than a human or any manual process because of its capability to process large volumes of synchronized data.

Further, using AI for ensuring cyber security gives valuable time back to your human resources to focus on higher-value projects and strategic planning.

AI is smart to prioritize security action needs

AI-enabled solutions are capable of effectively identifying the probable risks and threats. Further, it prioritizes what needs to gets addressed and in what order.

AI-based cyber threat detection systems usually work by raising alerts when something seems to be wary. These AI-backed systems also give a score on how close the event is from a cyberattack point of view. AI is smart enough to prioritize events with higher scores. For instance, you can automate your systems/machines for events above a certain score. Automated action is then taken to stop the extremely serious and likely cyber threat or attack without any human intervention.

However, events with a lower score can be forwarded to human experts for further analysis. Events with low scores can be simply logged into the system without any action on them.

Questions you should ask your cybersecurity vendor

You should have a detailed conversation about your cybersecurity requirements with your vendor.

1. **Ask for the business goals AI-based cyber security solution help you achieve?**

When evaluating a cybersecurity solution, you should have absolute clarity about the business goals it will help you achieve. Having this clarity will help you evaluate the performance of your AI-based cyber security solution.

2. What specific problems will the solution help you solve ?

With respect to cyber security there are very specific challenges AI-solutions can help you resolve. When you evaluate a solution or a vendor, there should be clear understanding of the problems and challenges that the cybersecurity solution will help you overcome.

3. Ask them how they train their models?

Real data to train the learning model is always a better strategy instead of using fake data. Real data helps recognize explicit behaviors that can constitute malicious activity. This is because cybersecurity tools using real data will produce a much more effective cybersecurity protection vs the one using fake data.

4. Enquire about the learning period for the machine learning models?

Ask your service/solution provider about "learning" period for the machine learning models. Depending on the solution, type of algorithm and model being used, it could take anywhere from a few minutes to several days.

AI can be an effective constituent in a robust cyber-defensive strategy, but keep in mind that it shouldn't be considered a complete remedy. However, when used for a specific cybersecurity challenge, it's usually the best way to stay a step ahead of attackers.

Cybersecurity is not a single layer process

Cybersecurity must never be viewed as a single-layer process. The benefits of AI at any level helps with triage, preventive response, an understanding of the threat landscape and day-to-day events.

To keep a step ahead of bad cybersecurity actors, it is advised to conduct regular reviews of security systems, tools, and policies. Regular training helps with not only threat prevention but also the adoption of security as a mindset.

Add AI-based solution to your basic cyber security plan

AI-based cyber security solutions address cyber threats that involve complex, and time-intensive tasks, and high-velocity data.

AI-based cybersecurity solutions are most suitable to stay ahead of cyberthreat threats. However, before including AI-based solution to your cybersecurity plan, it is important to build a strong security foundation that links people, processes, and technologies together.

Introducing additional security in the form of AI-based cyber security solution on top of that basic security plan can help achieve an augmented effect.

Conclusion

AI has emerged as the must-have technology for enhancing the efforts of human information security teams. Since it is not possible for a human task force to safeguard their enterprises from cyber threats, AI-enabled solutions offer much-needed threat identification that can be timely acted upon by cybersecurity professionals to prevent any serious security, compliance and theft issues. AI empowers cybersecurity resources to form a powerful team of humans and AI that drive cybersecurity to new heights.

Last, but not least, an important step towards preventing cyberattacks is to educate your users to stay away from all kinds of suspicious activity. Cyber security is highly related to your organizational processes and user behaviors and thus administrative, education and awareness play a vital role in any well-designed cyber security strategy.

##

ABOUT THE AUTHOR

Arindam Ray Chaudhuri, COO at AgreeYa Solutions, has over 30 years of rich industry experience in the technology domain. He has greatly contributed to AgreeYa's software, *solutions and services portfolio, by integrating a global team, defining the technology and business vision of products and services, establishing large scale client engagement and leading time, cost and quality driven value via project governance and solution engineering.*

Published Monday, November 29, 2021 8:25 AM by David Marshall
Filed under: VMBlog Info, Contributed