CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

IN THIS EDITION:

CELEBRATING 5 YEARS OF EXCELLENCE

JANUARY 2018

MORE INSIDE!

WHY AI IS EXACTLY WHAT THE CYBERSECURITY INDUSTRY NEEDS

By Giridhara Raam, Product Analyst, ManageEngine

More than half a year after WannaCry, the trend of evolving cyberattacks doesn't seem to have slowed down. Large organizations like the National Health Service (NHS), Maersk, Equifax and Uber have all fallen victim to cyberattacks this year. Instead of creating new malware, attackers have started to upgrade existing variants by configuring them with the right threat evasion parameters. As 2018 approaches, it's clear that companies need to adopt a high-level cyber security mechanism to keep their data safe and secure.

While some organizations are still wondering how to brace their networks with the right threat detection and breach prevention technology, many CIOs and CISOs have already begun to incorporate artificial intelligence (AI) into their organization's cybersecurity plan.

What Is AI?

Artificial intelligence is a machine or program that's created to perform a task by simulating human cognition. Generally, AI is provided with datasets and sensory parameters that make it capable of analyzing its environment and taking the best-suited action for a predefined situation. Most AI today is known as weak AI, designed to perform a specific task or a narrow domain of tasks.

How Can AI Make a Difference?

These days, malware is developed to be adaptive (meaning it contains minor AI attributes). This type of malicious software can analyze an organization's environment, monitor their network's vulnerability level and wait for a gateway to open so it can breach their network. If a malware variant is both autonomous and adaptive, the chance of a breach is overwhelmingly high, regardless of platform or device.

Depending on how efficient an organization is, it can take them minutes, days or even weeks to detect a malware breach in their network. AI can help technicians detect threats the moment they emerge.

When we consider SQL injections, humans simply don't have enough time to look at every SQL injection and confirm whether those attempts were successful or not. As organizations accumulate data, the responsibility to secure their networks can become an immense burden if the advantages of AI aren't utilized. There is no organization in the world that can efficiently detect each and every SQL injection without the help of AI.

According to a recent report by Spiceworks, 30 percent of organizations have already applied AI to their IT department, while 25 percent are in line to adopt AI next year.

How Is Machine Learning Different from AI?

AI is ideal for identifying, analyzing and understanding a situation as well as taking action based on predefined algorithms. Machine learning is an application of AI, with the goal to program computers so they can act on their own. From face recognition to smarter web search suggestions, there are many modern applications of machine learning that are already using data analysis to improve user experience.

Artificial neural networks (ANNs) are one of the most popular technologies associated with machine learning. An ANN is essentially a computer mechanism where systems learn progressively and improve task performance by analyzing and understanding examples, all without any decisions preprogrammed at the back end.

Modern cybersecurity solutions can employ an ANN to help admins analyze any new emerging threats and handle the situation with the right mitigation procedures. Machine learning doesn't just help IT teams identify threats via a smarter alerting system; machine learning can also prevent future breaches by continuously monitoring networks for established threat patterns.

For instance, take a look at the case of two ransomware variants, WannaCry and Petya. Exploiting the infamous EternalBlue vulnerability, WannaCry hit organizations in May of this year. Just a month later, Petya used the same exploit to infect even more organizations, including global shipping company Maersk. AI-enabled systems could have studied WannaCry's impact and automatically patched machines that were prone to EternalBlue, avoiding the second wave of ransomware attacks from Petya.

Is AI Ready to Be Deployed?

Despite major breakthroughs like Elon Musk's self-driving cars or Saudi Arabia's new robot Sophia, strong AI has yet to be developed and is still undergoing research and analysis. Some firms have already started employing machine learning to secure their IT departments, but the loopholes associated with AI have not been explored yet. Until organizations that are curious about AI have a clear set of prerequisites and multiple test cases (including both successful and failed cases), their best bet is to stay safe by keeping all vulnerabilities and loopholes periodically patched with the current tools at hand.

Many CIOs have already decided to embrace threat detection and breach prevention solutions for security information and event management (SIEM), endpoint security, identity and access management, and enterprise mobility management (EMM) to keep their organizations secure.

Pairing AI with SIEM, Endpoint Security and EMM

Certain machine learning techniques will soon be tightly incorporated with SIEM, endpoint security and EMM. Leveraging AI for enterprise security will hopefully follow in the next 10 to 15 years, but the downside of slow adoption is that organizations will be playing catch-up with cybercriminals who are already employing AI to infiltrate networks.

Given the current technological trends, machine intelligence will continue to develop and strong AI will eventually become a reality. In the future, we'll see whether industry predictions come true and it becomes common place for organizations to employ AI in their cybersecurity framework. By combining an organization's IT department with an advanced cybersecurity framework, AI is just what organizations need to prevent increasingly complex cyberattacks.

About the Author

Giridhara Raam is a product analyst at ManageEngine, a division of Zoho Corp. He works with the endpoint management team, marketing the Desktop Central solution and free Windows admin tools. Meanwhile, he also immerses himself in cybersecurity research from an endpoint management context. His love of IT is rivaled only by his passion for FC Barcelona and football in general. For more information on ManageEngine, the real-time IT management company, please visit www.manageengine.com; follow the company blog at blogs.manageengine.com/ and on LinkedIn at https://www.linkedin.com/company/manageengine-/, Facebook at http://www.facebook.com/ManageEngine and Twitter @ManageEngine.