Why AI in Cyber Security is the "Need of the Hour"?

To summarize why AI in cyber security is the "Need of the Hour," Enterprises across the world are being harmed by the increased danger of cyberattacks. You must work with a cybersecurity company because, according to a University of Maryland study, a hacker attack occurs every 39 seconds.

Reference- https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Enterprises are losing millions of dollars because of the rise in cybersecurity breaches. According to a survey by the Capgemini Research Institute, 20% of firms experience losses of more than 50 million US dollars because of cybersecurity problems. It is important to note that the current digital technologies are contributing to an increase in cyberattacks.

Reference - Reinventing Cybersecurity with Artificial Intelligence, Capgemini Research Institute

It is important to note that, from the perspective of the article, AI plays a crucial role in both the current and upcoming generations. Right now, AI plays a crucial role in offloading work from human cybersecurity engineers and handling the depth and detail that humans are unable to handle quickly or accurately. some of the most urgent cybersecurity requirements that AI technologies and platforms may assist in addressing.

- Large-scale security data handling - AI software running on today's powerful processors can quickly easily filter through more data than humans could possibly process in a month and identify issues and anomalies right away.
- Finding threat needles in digital haystacks - AI can quickly analyze a wide range of circumstances and behaviors to find the threat needles that signify malicious activity.
- Accelerated detection and reaction times - By quickly cross-referencing various warnings and security data sources, AI can expedite the identification of real security issues.
- Keeping up with the AI arms race - Hackers have no qualms about launching more attacks, each one more deadly than the previous, employing the newest technologies. You must stay up in the armaments race between AIs.
- Providing breathing room for human cyber security teams - Humans thrive in implementing better security solutions and enhancing overall security posture by applying their creativity, knowledge, and judgment. However, they can return to their strengths with the assistance of AI.

What was convincing?

From the article, I'm convinced that hackers always develop new strategies to bypass security measures. Such crimes can occur day or night, at any moment. It is crucial to understand how to handle a cyber-attack and how to keep it secure, regardless of whether you are a decision-maker inside a company, an employee, or a person in such a circumstance.

The best course of action is to deploy AI technology to combat hackers and uphold businesses' cyber security. Artificial intelligence provides a degree of complexity to the battle against cyber security that has never been seen before. Given that the world is moving toward AI technology, why would we pass up this chance? So, it's high time that organizations started harnessing the power of AI in their operations!.

Benefits of AI in Cyber Security:

- AI Lowers the Cost of Detection and Response to Breaches
  Organizations engaged in cybersecurity may utilize AI to analyze threat patterns and repurpose them for new threat detection. Incident detection, investigation, and correction all go more quickly. Threats may be identified and fixed in less time, and the associated costs are likewise kept to a minimum.
- AI Quickens the Response Time to Breach
  Quicker action is essential if we want to protect your company against cyberattacks. About 12% less time is required overall to identify risks and breaches thanks to artificial intelligence. You may also apply fixes more quickly or fix a breach. Here, lowering time metrics is crucial.
- AI Increases the Effectiveness of Cyber Analysts
  Cyber analysts may now spend more time examining issues that AI cybersecurity algorithms have assisted in identifying. One of the biggest developments in cybersecurity for 2020 is the use of AI. One of the research institute Capgemini's conclusions was as follows: Three out of five CEOs think AI in cybersecurity improves the effectiveness and precision of cyber analysts.
- AI Brings up New Revenue Streams
  Businesses create bigger income streams as cyber analysts become more effective because of artificial intelligence and machine learning. For industrial control systems, GE's Digital Ghost technology, for instance, offers a protective layer with AI capabilities. The digital twins are used by this technology to learn more about the machine's operating principles. It determines whether cyberattacks are affecting the device.

what was not convincing?

According to the article, keeping up in the AI arms race is a bit unconvincing for me but it's true. A lot of machine learning relies on enormous data sets with ambiguous origins. When it comes to digital defenses, there is an issue. Machine learning is already being used by threat actors to support greater social engineering attempts. They can learn things about the passwords and improve their password hacking if they have access to huge data sets including countless numbers of passwords.

Additionally, more spear-phishing attacks—that is, specifically targeted, non-generic bogus emails—will be sent in the future as a result of machine learning algorithms.

"I would like to ask the author, how we can prevent AI cyberattacks?"

How does the text relate to your own experience?

I'm a newbie in AI & cybersecurity but the motivation behind selecting this course is that the Air India data breach highlights third-party risk. Before moving to the United States, a cyberattack happened on the most prestigious Indian government body—"Air India".

The impact of this attack is 4.5 million travelers' personal information globally. Passengers' personal information from Air India was exposed as a consequence of a cyberattack on systems at airline data service provider SITA. Between August 2011 and February 2021, when SITA notified the airline, the stolen data was gathered. The incident wasn't reported to passengers until March, and they had to wait

until May to get all the specifics. Singapore Airlines, Lufthansa, Malaysia Airlines, Cathay Pacific, and Singapore Airlines were all impacted by the cyberattack on SITA's passenger service system.

What questions do you have for the author(s)?

This article is a great resource for learning about the role of AI in cybersecurity. However, if the article included information on how to integrate AI into cybersecurity and the best strategies to deal with AI as an as an ally of the opposition, it would be more beneficial.

References -

I. https://venturebeat.com/ai/crippling-ai-cyberattacks-are-inevitable-4-ways-companies-can-prepare/
II. https://www.bloomberg.com/opinion/articles/2022-04-24/ai-poisoning-is-the-next-big-risk-in-cybersecurity#:~:text=The%20danger%20is%20data%20poisoning,by%202028%20to%20%2435%20billion.
III. https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html
IV. https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/
V. https://www.google.com/