MACHINE LEARNING

Future is here and better!

"With an avalanche of data, Machine learning is a game-changer."

As large as any enterprise network gets, it is feasible to get prone to thousands of risks in their security/network systems and we need next-generation cyber-security to act in place. Attackers have been developing more sophisticated ways to invade systems and the fact that the number of attack perpetrators will always be bigger than the number of people trying to protect against them. The goal here is to get better intelligence and better analytics. Fortunately, machine learning can aid in solving the most common tasks including regression, prediction, and classification based on the data that is given by us.

METMOX

Delivering values innovatively

What is Machine Learning?

The ability to learn without explicitly programmed is Machine learning, simply put, it is a branch of artificial intelligence, it converts data into decisions. Machine learning algorithms use mathematical techniques across huge datasets, to build models of behaviors which can be used as a basis for making future predictions based on new input data. If your system learns constantly, makes decisions based on data or examples rather than algorithms, and changes its behavior, it's Machine Learning.

Why machine learning for Cyber Security

With evolving security strategies, malicious actors are using machine learning to automate their attacks, such as making breaches difficult to detect. Attackers use machine learning to automate the selection of victims and to find vulnerabilities in defense systems.

- In order to be ahead of the hackers, cybersecurity systems need to deploy machine learning algorithms which are powerful and complex.
- Machine learning pre-emptively stamps out cyber threats and bolsters security infrastructure through pattern detection, real-time cybercrime mapping, and thorough penetration testing.
- With its ability to sort through millions of files and identify potentially hazardous ones, machine learning is increasingly being used to uncover threats and automatically suppress them before they can wreak havoc.
- In addition to early threat identification, machine learning is used to scan for network vulnerabilities and automate responses.

The rules for identifying machine learning applications in your cybersecurity business:

1. Address tightly defined well-scoped problems
2. Be time-sensitive, high value, and high volume
3. Integrate easily with existing workflows, tools, and architecture
4. Have available data to support modelling
5. Have a reduced cost of false negatives/positives
6. Allow for frictionless performance evaluation

Machine Learning Use Cases:

1. **Hunt for malicious activity:** In the case of endpoint security and SIEM, machine learning uses its data learning abilities to identify, analyze, and respond to malicious activity. Unlike traditional techniques, which depend on signatures to detect malicious behavior, machine learning uses other traits to detect malware with fewer false positives.
2. **Mobile endpoints:** Machine Learning plays a major role in analyzing threats against mobile endpoints, while protecting the growing number of bring-your-own and choose-your-own mobile devices.
1. **Close zero-day vulnerabilities**: Zero-day threats put everyone – from organizations to individuals – at risk of losing sensitive data via an unknown exploit. Machine learning can help track down these threats and stop them before they severely impact operations.
2. **Automate security tasks**: The greatest potential of Machine Learning is automating high-volume and repetitive tasks that have complex rules and large amounts of data.

Machine Learning helps cybersecurity analysts minimize global cyber-attacks. Big data can be used in several algorithms to improve the current state of cybersecurity with ML.

In conjunction with other technologies, machine learning algorithms can pick up the information collected and QUICKLY SCALE the analysis process. The main benefit of machine learning is that the algorithms will learn and predict based on experience and results. It means a task which takes 1 day yesterday, tomorrow it will take 20 hours, the next day it will take 12 hours and so on. AI by "learning and predicting" effectively scale the effort to a level human cannot do, especially when dealing with automated tasks.

We're not being attacked by human beings anymore. Computers are attacking us; software is attacking us. The only way forward is using artificial intelligence.

www.metmox.com

CERTIFIED ISO 27001 CERTIFIED

Email: info@metmox.com