How AI Revolutionized Traditional SIEM Technology

Security Information And Event Management or SIEM provides data analysis, event correlation, aggregation, reporting, and log management to help your security teams keep track of what's going on in your IT environment. While being an important cybersecurity services tool, SIEM has barely progressed beyond the ability to give a better, more searchable rule-based log engine over the years. A study states that 88% of companies have problems with their SIEM platforms, and 99% want more SIEM automation.

This is where AI came into play. AI's adaptability permits it to be used in a variety of ways, and by integrating AI with SIEM systems, the efficiency of data analysis, vulnerability management, and threat management software can be increased exponentially. Artificial Intelligence for IT Operations or AIOps is a term coined by Gartner in 2016. SIEM solutions are rapidly incorporating AI and Machine Learning-based technologies with predictive analytics. SIEM gains deep learning capabilities and a plethora of integrated tools as a result of this integration, allowing for more informed outcomes.

The advantages of an integrated SIEM are as follows:

Preventing Stealth Attacks

A typical SIEM correlates events from several sources acquired over a short period of time. AIOps systems collect event data over a long period of time (years) and store it in a database and then apply analytics to it. AIOps can use this data to change the infrastructure baseline and warning levels over time, as well as perform some remedial steps automatically. Using big data allows SIEM to detect even the slowest or stealthy network actions that it would normally overlook as a one-off.

Noise Elimination

A typical SIEM generates a large amount of monitoring data/logs, however, the data in SIEM reports is difficult to comprehend and contains too much noise. An AI-integrated SIEM solution efficiently manages big data and easily automates redundant tedious activities.

Detecting Threats

AI and machine learning technology can include threat intelligence feeds in addition to conventional log data. If your SIEM has continuous access to one or more threat intelligence feeds, machine learning technologies can utilize the context it provided. And as it learns more, it begins to recognize dangerous behavior warnings beyond the data it was given at the outset. It increases the SIEM's decision-making, especially in terms of accuracy, and it provides cybersecurity solutions from dangers it has never seen before.

Pattern Prediction

Machine learning algorithms enhance SIEM systems, allowing them to predict and anticipate future data based on existing patterns. Consider some data patterns exposed during a security breach. Machine learning skills allow systems to internalize patterns and then utilize them to detect suspicious activity that could indicate a subsequent attack.

Read More: How AI Revolutionized Traditional SIEM Technology

Sattrix®

How AI Revolutionized Traditional SIEM Technology?

info@sattrix.com

+1 (325) 515-4107