MOVING FROM NOISE TO ALERTS WITH AI/ML MONITORING PRODUCTS: 10 KEY QUESTIONS

Some monitoring products provide a way to enter historical system data into their AI/ML monitoring products. Having this historical system data allows you to immediately train your AI/ML model. Once this data is analyzed some products are ready to go and can start identifying anomalies in your systems.

However, other AI/ML monitoring products do not have a way to import (ingest) historical data. These products must monitor your systems for weeks before they have enough data to detect anomalies. But, let's back up even more. Some products are just toolkits in that you have to select the individual metrics and figure out how to gather the metrics to get them into the monitoring tool. You may also have to adjust the sensitivity to the metrics you have chosen. Not all metrics are created equal some are much better indicators of problems than others. If you select the wrong metrics or the wrong sensitivity, your monitor may not provide any notifications or may provide many false positive notifications.

Metrics chosen often have complex relationships with other metrics that are useful when training your anomaly detection model. Multivariate (many related metrics) analysis requires an understanding of the relationship of the related metrics. Univariate (single metric) analysis only analyzes one metric at a time and is much more likely to cause false positive alerts. These relationships are why multivariate analysis is more valuable than univariate analysis. Related metrics tend to all move based upon their relationship when a problem occurs. Finding these relationships

yourself is often time-consuming and difficult. Multivariate analysis requires a large amount of situational data to develop a good model. Ideally, you want your product vendor to have already done this complex analysis and provide a model with multivariate analysis baked into the product.

Once you have done all of that, you think it would be monitoring nirvana but not so. Because you chose your specific metrics, you now must build your dashboards based on those metrics. Again, this is a case where it is much easier to work with a product where the vendor has already done the metric selection, the multivariate analysis, and designed a user interface to intelligently present this information. It is very time-consuming to build dashboards and charts and organize them in a way that is easy to navigate.

You also must test to verify if the model is detecting the expected anomalies and if it is sensitive enough to find the problem early enough to fix them before they cause an outage. So, when a product claims to have embedded intelligence, you should ask questions to determine if it really has the embedded intelligence you need or is it a science experiment that needs a lot of work and testing to get it configured correctly.

Before you decide to buy an AI/ML Product based upon a demo, keep the following questions in mind:

- Does it support import and processing of historical data for training so it is ready to monitor in days not weeks?
- Do you have to figure out which metrics you need to monitor out of hundreds of choices?
- Is the analysis done with multivariate analysis or is it a simplistic univariate analysis doing a simple weighted summary?
- Are the relationships between all of the metrics already known and defined in the model and ready to do the analysis?
- Do you need to start collecting new metric data you do not currently collect and feed it into the tool?
- Are the metric's sensitivities already known and adjusted for?
- Are the dashboards already complete and can you easily drill down into the more detailed data in charts when needed?
- Does the user interface provide an obvious starting point for doing diagnostics when an anomaly is detected?
- Does the user interface guide problem identification or does it just show a lot of numbers and graphs?
- Are the monitor intervals frequent enough to not miss early warnings of the potential outage?

It is important to ask these questions before buying an AI/ML monitoring product that requires more work and more expertise than your team can provide to get it configured. You can not overlook the amount of time it takes to provide useful alerts rather than more noise to evaluate the product's success.