

How is Predictive Analytics Transforming ITOps | Technology

SLOUGH, UK, UNITED KINGDOM, May 6, 2021 /EINPresswire.com/ -- In today's dynamic and highly componentized IT landscape, predictive analytics offers the much-needed ability to proactively predict future outages and automate fixes before they bring down the entire infrastructure.

Owing to the rapid digitization of business operations, IT teams need to constantly monitor and analyze large volumes of data, resulting in extended delays in identifying and solving issues. On top of that, a single IT issue can trigger thousands of alerts, logs, and events, and with the ITOps team working in disconnected silos, it becomes extremely difficult to diagnose the root cause and solve issues.



Predictive analytics, powered by big data, artificial intelligence (AI), and machine learning, overcomes these obstacles to improve application performance, network uptime, and IT infrastructure resiliency by predicting and mitigating outages, and reducing maintenance and operations expenditure in the process.

Gartner predicts that the number of large enterprises that use artificial intelligence in IT operations to combine big data and machine learning functionality to enhance or optimize IT operations and automate processes and tasks to grow by 40% by 2023.

Let's understand how predictive analytics is transforming ITOps.

Predictive Analytics: An Evolution In IT

Today's IT operations monitoring and management systems leverage predictive analytics for collecting and integrating data, normalizing it, and analyzing it in real-time.

Machine learning algorithms analyze past incident data to predict and resolve potential incidents in the future.

Here are some ways in which predictive analytics is transforming IT operations.

1. Dynamic Thresholding And Anomaly Detection

An anomaly detection algorithm uses unsupervised machine learning to get familiar with the IT environment, recognize expected behavior, and set dynamic thresholds against vital performance metrics.

Consequently, event patterns are analyzed in real-time and compared against expected behavior, and the IT team is alerted when a series of events showcase anomalous activity.

Moreover, fuelled by artificial intelligence, the system also accounts for false alert suppression and seasonality, i.e. alerts are sent only when a critical application displays abnormal behavior during an unexpected time period. For example, a 90% system utilization is normal during peak business hours, but indicates an issue when the same metric is hit on a Sunday morning.

Anomalous group of events are helpful in –

Alerting the team regarding an unplanned activity, for example a cyber attack

Making IT operations more agile by improving planning for significant events, for example, Amazon increasing capacity to ensure infrastructure and applications perform well during the 'Big Billion Sale'.

2. Predictive Maintenance Of Application Health In Real-Time

Performing application health monitoring in real-time allows ITOps teams to respond to a degradation in application health before operations come to a standstill.

Available data generated by the application, including configuration data, network logs, application logs, performance logs, and error logs, is compiled. Multivariate machine learning techniques analyze this data, across different dimensions, to learn the application's normal behavior.

As new data enters the application, the model identifies unusual patterns and sends it to the IT personnel to follow up before a business-critical outage takes place.

3. Predict Network Downtime Using Sequential Pattern Analysis And Time-Series Event Correlation

A survey by an AIOps Exchange states, "45% of businesses are using AIOps for better root cause

analysis and to help predict potential problems.”

Thousands of events across applications and infrastructure are correlated in a time series and analyzed by an ML-powered algorithm to identify patterns.

These patterns proactively alert the team regarding any potential outages and network downtime, reduce the quantum of alerts and pinpoint the root cause, and understand the future impact of similar patterns being repeated.

4. Predict And Prevent Common Capacity Issues

Machine learning algorithms analyze historical utilization trends of infrastructure resources, including CPU, memory, etc. to predict capacity exhaustion.

Predictive analytics ensures more bandwidth can be added via automation or manual intervention, so no resource becomes non-operational due to capacity issues.

Moreover, organizations may purchase additional capacity and reserve instances in advance, to cope with the additional demand, leading to large cost savings.

5. Ensuring Cybersecurity By Detecting Fraud

The use of predictive analytics in detecting fraud has gained prominence in ensuring cybersecurity. ML-enabled tools analyze typical fraudulent activity, recognize patterns, and find anomalies.

Continuous monitoring of IT systems leads to early detection of any potential fraudulent activity.

vinay

acuvate

+44 1895 542351

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/540409711>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.