Prelert's IT Operational Analytics for Splunk

Prelert
945 Concord St.
Framingham, MA 01701
www.prelert.com
1-800-773-5378

Most IT organizations are rich with operational data – collected from networks, servers, applications, storage, databases and more. However, a lot of this data sits unused because there's simply too much of it to analyze. Just as difficult as finding the needle in the haystack, finding IT problems remains as a challenge for IT staffs.

Prelert recently announced a solution that helps IT staffs find the IT operations "needles in the haystack", which it calls Anomaly Detective for Splunk environments. By applying Big Data analytics to IT operations data, Anomaly Detective first learns what is normal behavior so it can identify abnormal behavior when and where it happens.

Anomaly Detective for Splunk environments

Prelert's app for Splunk environments leverages the wealth of IT data that Splunk collects from various data sources. Prelert applies advanced analytics to the data to determine "normal behavior" patterns so it can identify behavioral changes that may point to operational and security issues. The key to Prelert's approach is using machine intelligence to sift and filter through mounds of IT data to identify abnormal behavior or anomalies, so it can predict potential operational problems. Then IT staffs can focus on investigating and resolving the predicted problems before they escalate into bigger issues.

Anomaly Detective automatically learns normal behavior patterns in Splunk data searches and identifies the anomalies. It then automatically isolates data related to the change in behavior, so IT experts can investigate. Self-learning minimizes the need to configure and set up analytics rules, which makes it quicker to implement and easier to use. Anomaly Detective is designed to not replace but instead to complement human IT expertise.

The software is easily downloadable, and installed as a native Splunk app. Annual subscription prices scale with the volume of data indexed per day, with free usage under 500 MB of data.

The Final Word

The IT Operational analytics that Prelert delivers in Anomaly Detective could significantly change IT's ability to circumvent potential problems before they impact IT operations. Just as a doctor looks for abnormal symptoms and signs to find and diagnose a patient's illnesses, Anomaly Detective aids in finding the anomalies that IT professionals can use to find and diagnose IT's ills.

Voluminous IT data that sits idle in log files, data files and in other places can be analyzed comprehensively and collectively by Anomaly Detective, which is impossible for humans to do.

There are many “gold nuggets” potentially hidden in the mounds of IT data that Anomaly Detective can identify for further human investigation.

Potential users must be aware that a Splunk subscription is also required to use this application. It is a complementary app for Splunk users.

The new industry trend of applying analytics to IT operational data holds much promise in changing the effectiveness and cost efficiencies in IT. Additional insight provided by analytics has the potential to help IT figure out the cause and resolution for IT problems more quickly, as well as providing solutions for problems that were previously unexplainable because IT staffs just didn’t have enough information. IT Operational analytics is a welcomed trend for IT operations, and Prelert’s Anomaly Detective for Splunk environments is definitely worth a look.

Publication Date: February 4, 2013

About Ptak, Noel & Associates LLC

We help IT organizations become "solution initiators" in using IT management technology to business problems. We do that by translating vendor strategy & deliverables into a business context that is communicable and actionable by the IT manager, and by helping our clients understand how other IT organizations are effectively implementing solutions with their business counterparts. Our customers recognize the meaningful breadth and objectively of our research in IT management technology and process.
www.ptaknoel.com

About the Author

Audrey Rasmussen leverages her experience of over 30 years in the information technology industry, to help her clients as they navigate through the accelerating changes in the information technology industry. Over the years, she has developed expertise and experiences in various contexts (expertise in systems and application management, working with very small companies to very large corporations, industry specializations, business focus, and technical focus, as well as vendor and consulting experience), which combine into unique insights into the information technology industry.

arasmussen@ptaknoel.com