Anomaly Detective® App

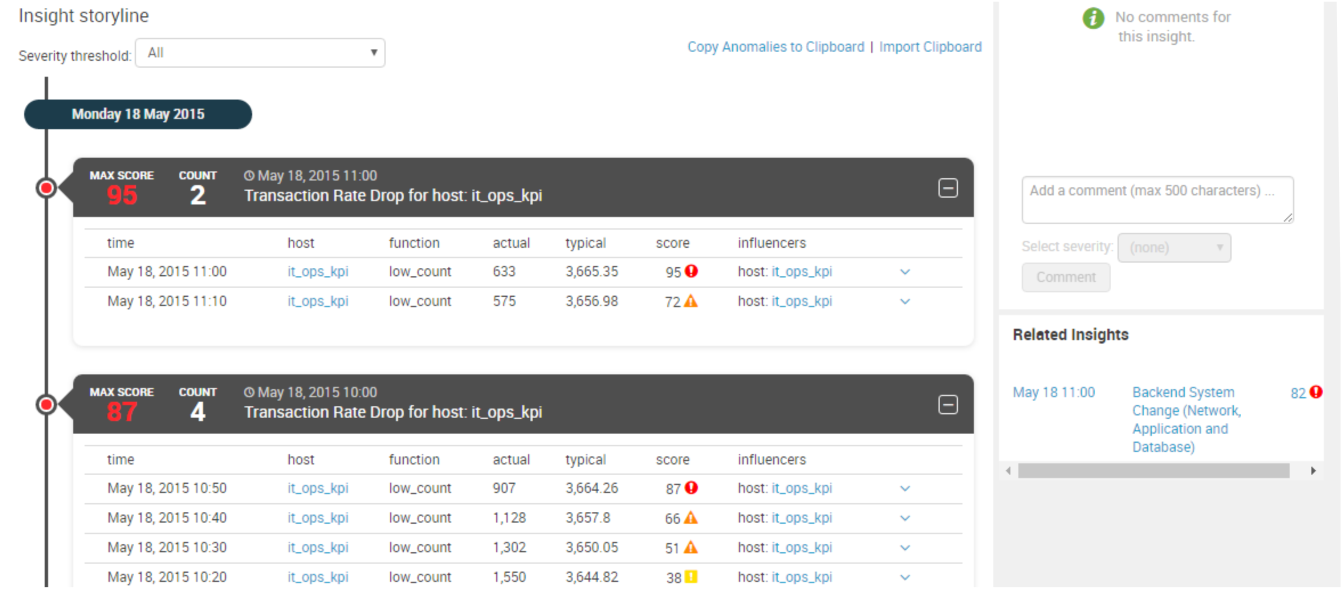
for Splunk®

Prelert Behavioral Analytics: Let Your IT Operations Data Tell the Story

Prelert's Anomaly Detective App for Splunk analyzes log data, finds anomalies, links them together and lets your data tell the story behind operational anomalies. The Anomaly Detective app extends the power of Splunk's platform with behavioral analytics capabilities that can be applied to any data source. These capabilities include an innovative new feature called the Insight Storyline that helps teams visualize events and connect them to root causes faster and more easily.

Prelert's Anomaly Detective app for Splunk helps you automate the analysis of massive data sets using machine learning technology. Since the automated analysis operates in an online mode, it flags problems in near-real-time, eliminating the need for traditional data monitoring rules and thresholds that return false positives if set too strictly, miss activity if set too loosely, and become outdated over time. Prelert analytics include statistical influencer tracking, which provides critical contextual data for each detected anomaly so entities that are associated with anomalous activity can be identified quickly for further investigation and remediation.

Tightly integrated with Splunk, the Anomaly Detective app is easy to download and deploy in minutes—no data import or export required. Anomaly Detective also supports Splunk Cloud™, Hunk® and the Enterprise Security application.



Insight storyline

Severity threshold: All

Copy Anomalies to Clipboard | Import Clipboard

Monday 18 May 2015

MAX SCORE 95 COUNT 2 May 18, 2015 11:00
Transaction Rate Drop for host: it_ops_kpi

time	host	function	actual	typical	score	influencers
May 18, 2015 11:00	it_ops_kpi	low_count	633	3,665.35	95 !	host: it_ops_kpi
May 18, 2015 11:10	it_ops_kpi	low_count	575	3,656.98	72 ⚠	host: it_ops_kpi

MAX SCORE 87 COUNT 4 May 18, 2015 10:00
Transaction Rate Drop for host: it_ops_kpi

time	host	function	actual	typical	score	influencers
May 18, 2015 10:50	it_ops_kpi	low_count	907	3,664.26	87 !	host: it_ops_kpi
May 18, 2015 10:40	it_ops_kpi	low_count	1,128	3,657.8	66 ⚠	host: it_ops_kpi
May 18, 2015 10:30	it_ops_kpi	low_count	1,302	3,650.05	51 ⚠	host: it_ops_kpi
May 18, 2015 10:20	it_ops_kpi	low_count	1,550	3,644.82	38 !	host: it_ops_kpi

No comments for this insight.

Add a comment (max 500 characters) ...

Select severity: (none)

Comment

Related Insights

May 18 11:00	Backend System Change (Network, Application and Database)	82 !

"Insight Storyline" dashboard showing anomaly linkage that help analysts understand relationships between anomalous behaviors. Here anomalies in the backend database metrics triggered anomalies in transaction performance KPIs.

Prelert Behavioral Analytics extends the power of Splunk with automated "machine learning" that can be applied to any type of IT operations-related data including application logs, database logs, virtual infrastructure logs, Windows event logs - essentially any time-series log data that can be stored in Splunk. These capabilities include innovative statistical influencer tracking and insight storyline capabilities that help operations analysts visualize multiple anomalous events, connect them to root causes faster and more easily, and improve key operational metrics such as MTTR (mean time to recovery) and better understand business KPIs (key performance indicators). Users simply choose the desired set of use cases to deploy. With easy-to-use parameterized configuration of anomaly search jobs, users can augment Prelert-supplied use cases by creating their own use cases leveraging their own subject-matter expertise. Anomaly Search jobs detect changes, disruptions, outages, slowdowns, and other anomalous behaviors in log data and other business-related KPIs without training.

Anomaly Detective App for Splunk

Prelert Behavioral Analytics Offers

Early Detection of Operational Issues

Prelert uses machine learning to analyze log data in near real-time, detecting anomalies associated with operational issues such as software bugs, user misconfigurations, H/W problems, virtual infrastructure resources, network performance issues, and more. This allows IT operations teams to identify incidents earlier, without the manual effort and human error traditionally involved, and ultimately ensuring a positive end-user experience.

Reduced False Positives

Prelert's behavioral analytics capabilities save you time by helping you quickly identify and contain real problems. By analyzing your log data, finding anomalies in various log sources and linking them together, Prelert Anomaly Detective App for Splunk provides deeper context to help minimize the false positives that waste your time.

Speedy Detailed Root Cause Analysis

Using "online machine learning," Prelert algorithms continuously refine the model of what data behaviors are normal for your environment. With Prelert, operations teams can now get the real story behind issue-related activity, while involving fewer people in incident response and remediation.

Why IT Operations Teams Choose Prelert

Unsupervised Machine Learning

Proprietary unsupervised machine learning algorithms baseline normal behavior without the need for training data sets. Even better, organizations don't need a team of data scientists to use Prelert effectively.

More Accurate Anomaly Detection

Sophisticated machine learning algorithms provide you with accurate information (read: fewer false positives) so you can quickly detect, investigate and respond to operational issues. No more manual effort writing rules or human error parsing alerts.

Organization-Specific Insights

Prelert lets your data tell the story. Linked by common statistical influencers, related anomalies provide insight by telling you what you need to know now and what requires further investigation.

Speedy Data Analysis

Prelert is designed to analyze massive, high-cardinality data sets in moments, showing you what you need to know and making it easy to uncover what is worthy of your attention.

Near Real-Time Alerts

Just moments from the time your log data is indexed in Splunk, Prelert analyzes your data, generating accurate models that evolve as fast as your data does, identifying outlying anomalous behavior and alerting you about what is most important in your environment.

Anomaly Detective App for Splunk

System Requirements:
info.prelert.com/system-requirements

DOWNLOAD FREE TRIAL

www.prelert.com/downloads

Or call us to learn more: (888) PRELERT or +1 (508) 319-5322

About Prelert

Prelert is the leading provider of behavioral analytics for IT security, IT operations, and business operations teams. The company's solution analyzes an organization's log data, finds anomalies, links them together and lets the data tell the story behind advanced security threats, IT performance problems, and business disruptions. Leveraging machine learning anomaly detection and other behavioral analytics capabilities, the solution automates the analysis of massive data sets, eliminating manual effort and human error. Hundreds of progressive IT organizations rely on Prelert to detect advanced threat activity, reduce false positive alerts and enable faster root cause analysis. Prelert lets your data tell the story.