

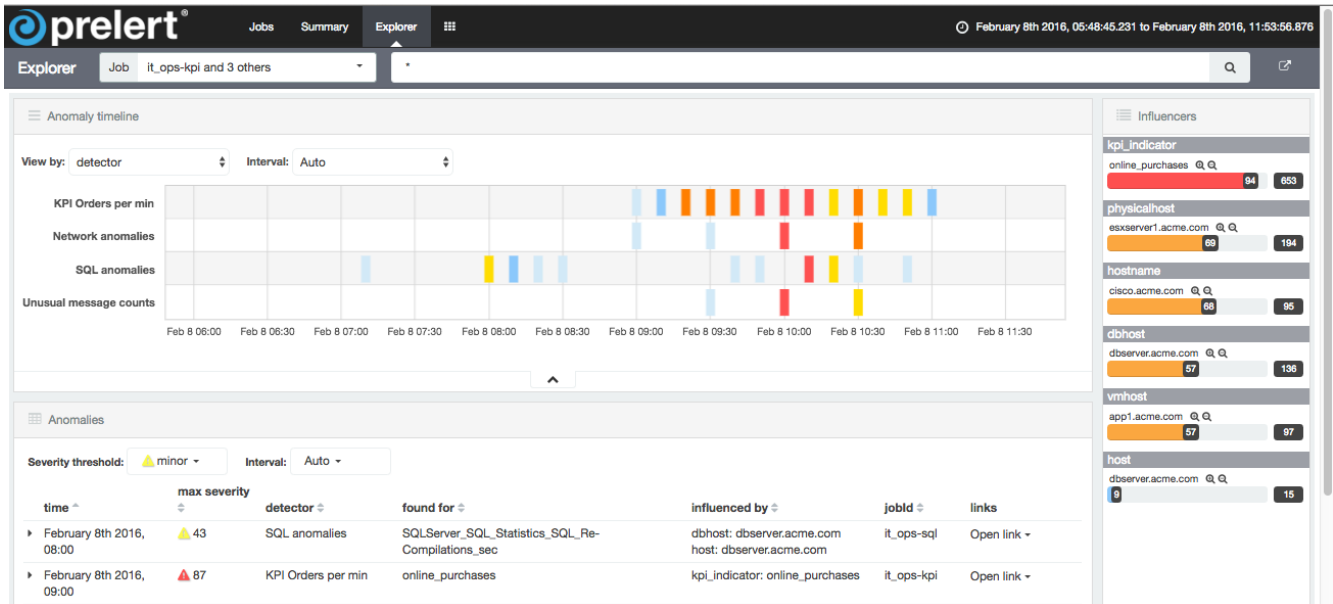
# Behavioral Analytics

## for the Elastic Stack

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

Executing as a Kibana app, Prelert Behavioral Analytics for the Elastic Stack is tightly integrated. Data is pulled from Elasticsearch for analysis, and anomaly results are displayed in Kibana dashboards. Behavioral Analytics for the Elastic Stack is also compatible with other Elastic Products such as Shield and Watcher. It's easy to download and deploy in minutes—no data import or export required.

Prelert Behavioral Analytics for the Elastic Stack helps you automate the analysis of massive Elasticsearch data sets using machine learning technology. Since the automated analysis operates in an online mode, it flags real 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rules and thresholds that return false positives if set too strictly, miss activity if set too loosely, and become outdated over time.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.



"Anomaly timeline" dashboard showing anomaly search job "swimlanes" that help analysts understand relationships between anomalous behaviors. Here anomalies in the application metrics trigger other anomalies in KPIs, network behavior, and database performance.

Prelert Behavioral Analytics for the Elastic Stack software analyzes IT-related log data residing in Elasticsearch, finds anomalies within the data, links them together and lets your data tell the story behind operational issues. Behavioral Analytics for the Elastic Stack extends the power of the Elastic Stack with automated machine learning-based analytics capabilities that can be applied to any type of IT operations-related data in Elasticsearch. These capabilities include an innovative statistical influencer tracking capability that helps 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).

Behavioral Analytics for the Elastic Stack can automate the analysis of many different types of 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 Elasticsearch. 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 KPI's that can indicate past, current, or future problems.

## Behavioral Analytics for the Elastic Stack

### 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 Behavioral Analytics for the Elastic Stack 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

Preelert 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

Preelert 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 Elasticsearch, Prelert analyzes your data, generating accurate models that evolve as fast as your data does, identifying outlying user behavior and alerting you about what is most important in your environment.

## Behavioral Analytics for the Elastic Stack

System Requirements:

[info.prelert.com/system-requirements/elastic](http://info.prelert.com/system-requirements/elastic)

**DOWNLOAD FREE TRIAL**

[www.prelert.com](http://www.prelert.com)

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.