Elasticsearch x-pack machine learning

Statistical ModelMathematical description of data over time4 Keys of Anomaly DetectionFeature selection

Loading Existing Data

Period Detection

Empirical Sorting ON Feature selectionCreating detection rules off of your data pointsPeriod DetectionChoosing what frequency of time is meaningful to the data.

Empirical scoringDefining which automatically detected anomalies are important. Bucket SpansParameter range that divides data into batches for processing (usually time)Analysis functionFunction that is applied to the bucket span, count, sum, metric etc. Machine Learning JobRunning of the analysis function(s) over the determined bucket spansDetectorMultiple analysis functions with a shared bucket span. Event/Data FeedPushes data into a job.

May be a query.

Can be range based or live.

Can be run on pre-aggregated data. InfluencerAttribute that has an influence on the data, something that has contributed to the anomalyAnomaly ScoreCombination of individual item scoring and bucket scoringIndividual item scoringHow anomalous an event is to a baseline.

Based on past behaviorBucket scoringComparing an anomaly to other readings in the bucket.

Aggregate score across all detectors for the job

Only one score per bucket. Partition fieldsFields with a low enough cardinality to run a machine learning job over each distinct value.

Advanced job parameter that duplicates the job over values of the field and performs analysis in parallel. Individual Anomaly DetectionComparison of a behavior to it's own historical behaviorPopulation Anomaly DetectionComparison of a behavior to the behavior of other members of a population. Over FieldsAdvanced job parameter used to perform population anomaly detection. By fieldsAdvanced job parameter used to perform individual anomaly detection. Jobs are performed in serial, then categorized BY field. By field anomaly scoreUses total anomaly ratio for all by field valuesPartition field anomaly scoreUses individual anomaly ratio for all partition field values