# Anomaly detection

## Data

* Metrics
  + Time series, Time-stamped observations
  + Context
* Static Attributes
  + Units
    - Bytes
    - Requests
  + Data Type
    - Counter
    - Gauge
  + Granularity
  + Raw or Cooked
* Dynamic Attributes
  + Slowly Changing Dimensions (SCD’s)
    - Not Constant, but not always changing
    - Hosts in cluster
    - Number of replicated microservices, etc.
* Collections
  + Entities/Elements
    - Virtual or Physical
    - Dynamic attributes as time series represented as states as it moves through time
    - Example, a javamethodcall over time
  + Relationships
    - Containment, ie. Load Balanced Cluster
    - Sequencing, “Workflow”
  + Interactions
    - Business level work flow
    - Servers, to latency, to customer, to profit

## Types

* Point
  + A point anomaly is an observation that is unusual when compared with all the rest of available observations
* Contextual
  + A contextual anomaly is an observation that is unusual in a certain context but not in other contexts
* Collective
  + A collective anomaly occurs when a collection of related data instances is anomalous with respect to the entire data set.
  + Correlation of multivariate variables

|  |  |
| --- | --- |
| Anomaly type | Detection Data Requirement |
| Point | Uni-variate |
| Contextual | Uni-variate + contextual attributes |
| Collective | Multi-variate+ contextual attributes |

## Techniques

* Deterministic
  + Dashboards
    - Do not scale with growth of metrics
  + Static thresholds
    - Easy to set, but becomes manual
    - Sudden changes above or below thresholds cause false flags
    - Anomalies hidden in cumulative data
  + Transformations (Uni-variate)
    - Delta: raw[n] -> raw [n] – raw[n-1]
    - Rate: raw[n] -> raw [n]/time
    - Scale: raw[n] -> raw [n] \* constant
    - Min: raw[n] -> min(raw)
    - Max: raw[n] -> max(raw)
    - RHMAX: raw[n] -> raw [n]/ max(raw)
    - Summary: raw[n] -> (min,25pct,50pct,mean,75pct,max)
    - Allows for observations in other dimensions
* Statistical
  + Correlation Models
    - Probabilistically stable
    - 1 to -1 correlations between different values
    - As one metric moves the other metric moves the same way(1), or in the opposite (-1)
    - Pearson product moment coefficient of correlation for two metrics
  + Machine learning
    - Learning phase
      * Learning from test data
      * Consume test metrics and provide parameters
    - Detection phase
      * Consume Raw metrics and measure against Parameters
      * Detect anomaly
    - Adjustment
      * Consume raw metrics, measure against parameters
      * Detect anomalies and make corrections to detector