WORK IN PROGRESS
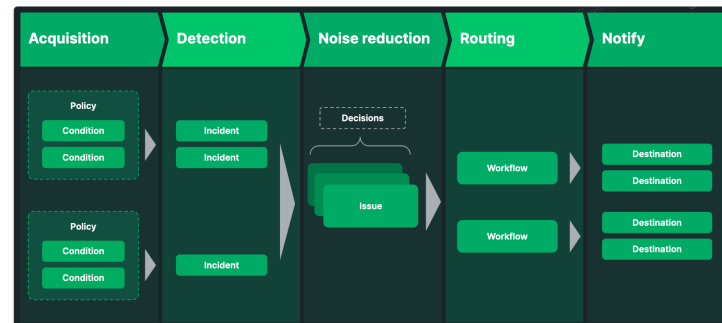
Alerting Pipeline

Acquisition	Detection	Noise reduction	Routing	Notify

Policy
- Condition
- Condition

Incident
Incident

Decisions

Issue

Workflow

Destination
Destination

Policy
- Condition
- Condition

Incident

Workflow

Destination
Destination

NrSignal
NrAIncident

```
Policy:
    Preference: incident for every issue
    Correlation

Decisions:
    All default decisions are enabled

Condition:
      SELECT      Function    |    Event Type    |         Condition
NRQL: SELECT      count(*)    |    from  Log     |   where message like 'this is a test log message'

Event Aggregation:
    Window:  1 minutes
    Streaming method:  timer

Threshold:
    above | below | equal | ...
    { Value }
    at least once in | for at least
    is < Evaluation Duration > minutes
```

ACQUISITION

Define Events

Stage: Filter Events

Stage: Aggregate Events

FROM
Looks at every event
Defined on nrql FROM

From Log

Telemetry Data

WHERE
Filters events based on nrql condition

Where message like 'this is a test log message'

true
false

event is discarded

filtered events

config: window duration

Example: 2 minutes
- Exactly when an aggregation window is submitted to the evaluation stage is determined by the streaming method
- If there are no events in an aggregation window, nothing happens - if gap filling strategy is None.

Gap Filling becomes active if an aggregation window is empty.

Gap filling strategy
Fill data gaps with

Streaming Method
Streaming method

Timer: time driven
Timer
1 minutes

- As soon as an event arrives, a timer is started.
- If an event arrives while a timer is active, then the timer will be reset and start again
- Only after a timer reached zero will the aggregation window be submitted to the next stage: evaluation.

For best results, make sure:
- The timer is equal to or longer than your window aggregation.

If the timer is less than your window aggregation and your data flow is inconsistent, then events may be evaluated before all of the events for the current aggregation window arrived.

Flow: event driven
Delay
2 minutes

Flow is event driven - as soon as an event for a subsequent aggregation window arrives Will the current window be moved to evaluation. Optionally, a delay can be specified.

SELECT
Function

count(*)

NrSignal

Signal Loss

Consider the signal lost after

NrSignal

Optional: Delayed Evaluation

Evaluation delay
Use evaluation delay

Allows initial values of a signal to be ignored.

This is intended for signals expected to begin in a violating pattern, requiring time to stabilize before generating trustworthy alerts.

Define Threshold (Evaluation)

Static
Set static thresholds
Set thresholds for a query that return to a static value.

Open incidents
Severity level: Critical

When a query returns a value   ABOVE   at least once in   MINUTES

Compare Signal Value against Threshold

Dynamic - Anomaly
Set anomaly thresholds
Set flexible thresholds that adjust across your expectations.

Threshold direction: Upper and lower

Open incidents
Severity level: Critical

When a query returns a value outside the threshold

standard deviations

More incidents   Fewer incidents

DETECTION

Incident

NrAIncident

NOISE REDUCTION

Correlation
Decisions

Issues