new relic

Alerts Onboarding

An introduction to New Relic alerts

Adam Marshall - Senior Technical Success Manager
adammarshall@newrelic.com

February - 2026

Safe Harbor

This presentation and the information herein (including any information that may be incorporated by reference) is provided for informational purposes only and should not be construed as an offer, commitment, promise or obligation on behalf of New Relic, Inc. ("New Relic") to sell securities or deliver any product, material, code, functionality, or other feature. Any information provided hereby is proprietary to New Relic and may not be replicated or disclosed without New Relic's express written permission.

Such information may contain forward-looking statements within the meaning of federal securities laws. Any statement that is not a historical fact or refers to expectations, projections, future plans, objectives, estimates, goals, or other characterizations of future events is a forward-looking statement. These forward-looking statements can often be identified as such because the context of the statement will include words such as "believes," "anticipates," "expects" or words of similar import.

Actual results may differ materially from those expressed in these forward-looking statements, which speak only as of the date hereof, and are subject to change at any time without notice. Existing and prospective investors, customers and other third parties transacting business with New Relic are cautioned not to place undue reliance on this forward-looking information. The achievement or success of the matters covered by such forward-looking statements are based on New Relic's current assumptions, expectations, and beliefs and are subject to substantial risks, uncertainties, assumptions, and changes in circumstances that may cause the actual results, performance, or achievements to differ materially from those expressed or implied in any forward-looking statement. Further information on factors that could affect such forward-looking statements is included in the filings New Relic makes with the SEC from time to time. Copies of these documents may be obtained by visiting New Relic's Investor Relations website at ir.newrelic.com or the SEC's website at www.sec.gov.

New Relic assumes no obligation and does not intend to update these forward-looking statements, except as required by law. New Relic makes no warranties, expressed or implied, in this presentation or otherwise, with respect to the information provided.

Agenda

01	What is New Relic Alerts	5 mins
02	Key concepts and terminology	5 mins
03	Platform demo	30 mins
04	Q&A	5 mins
05	Setting goals and next steps	5 mins

new relic

New Relic All-in-one Observability Platform

new relic

01 What is New Relic Alerts

new relic

VS

new relic

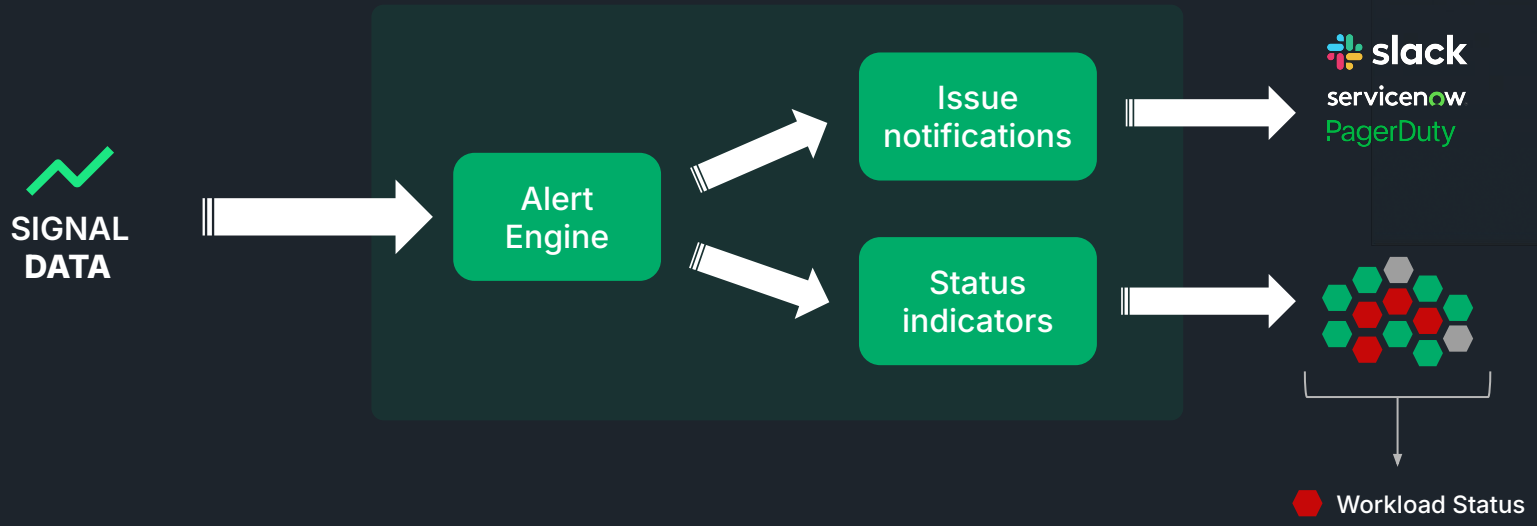
New Relic Alerts is a **pro-active** mechanism for automating the **detection and notification** of **changes in your systems'** data.

It encompasses a suite of tools that **continually analyses data signals** against user defined set of thresholds, **generating issues** and **notifying end users** of problems as they occur.

Documentation on alerting concepts

new relic

10,000ft view



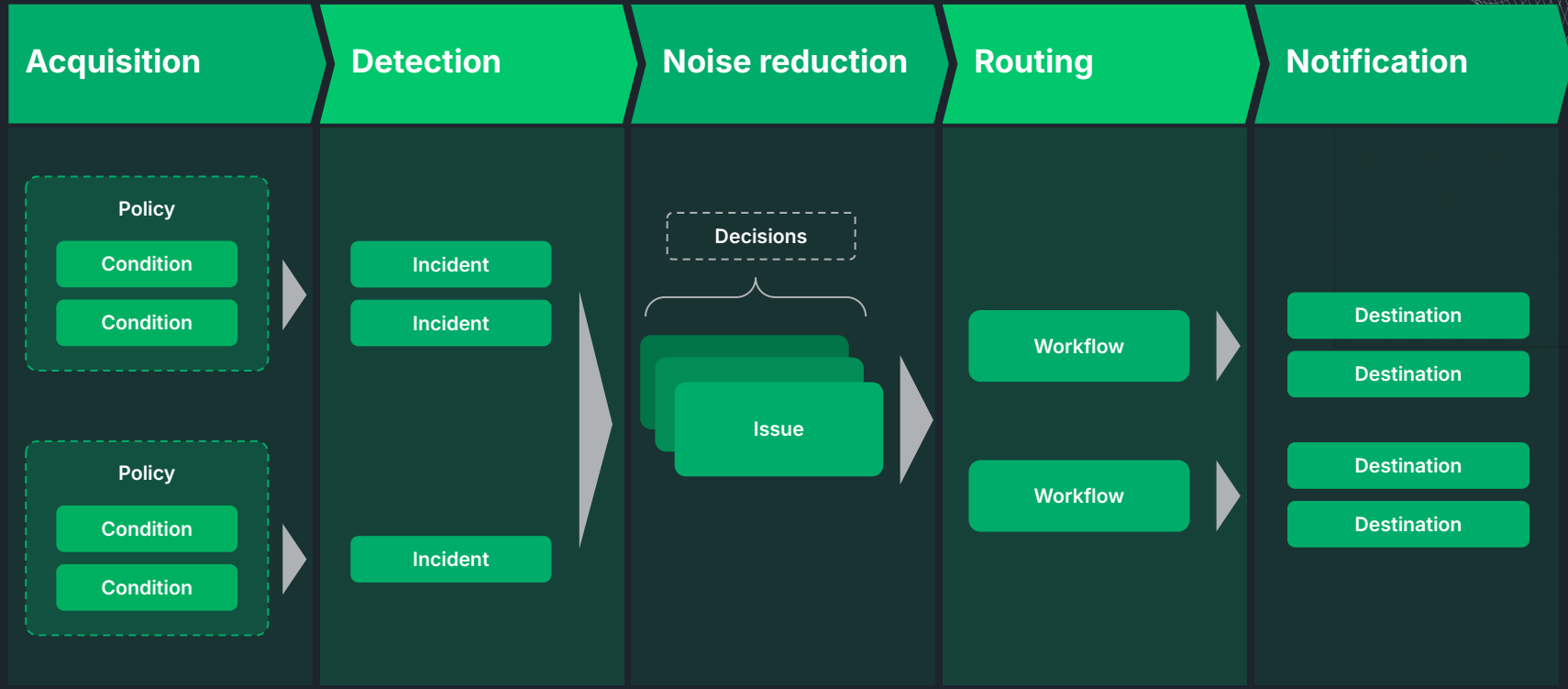
new relic

02 Key concepts and terminology

The building blocks of alerts

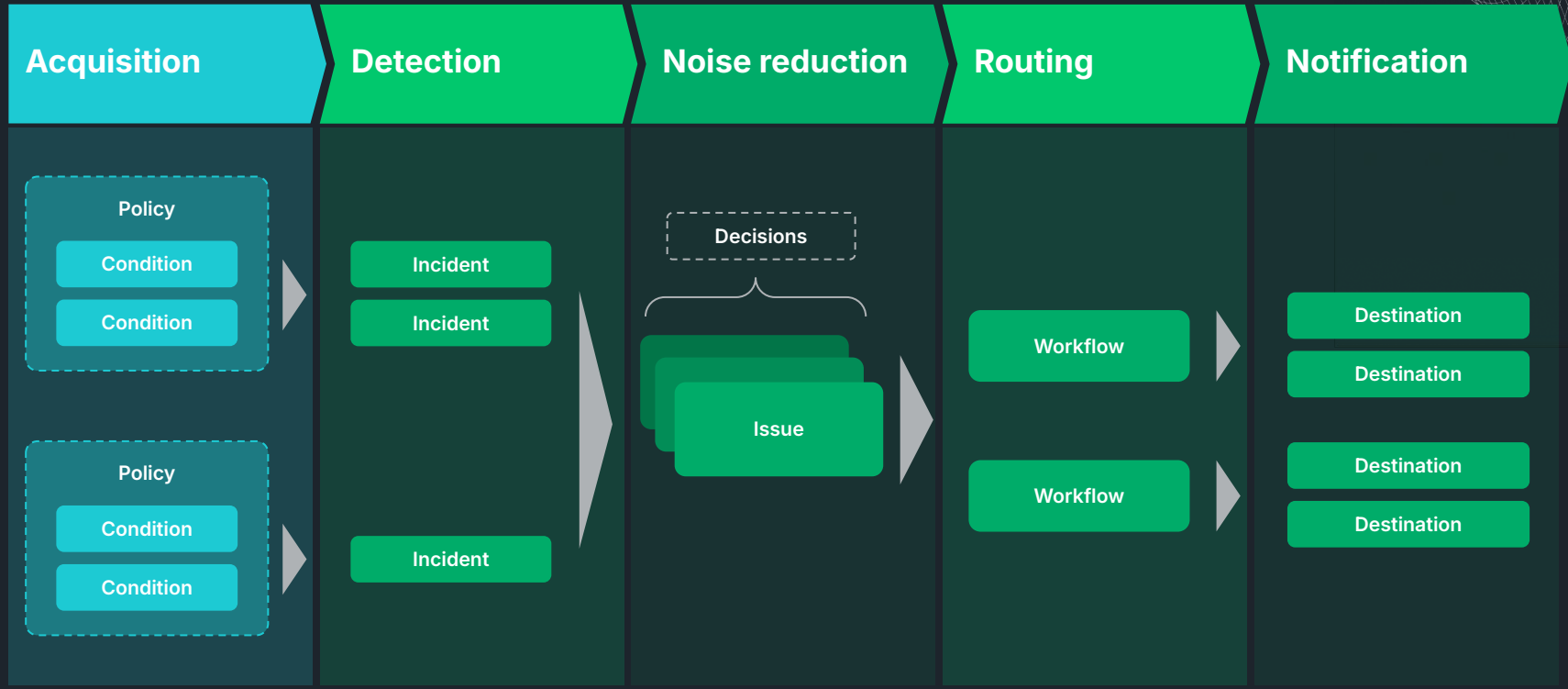
new relic

The Alert Pipeline



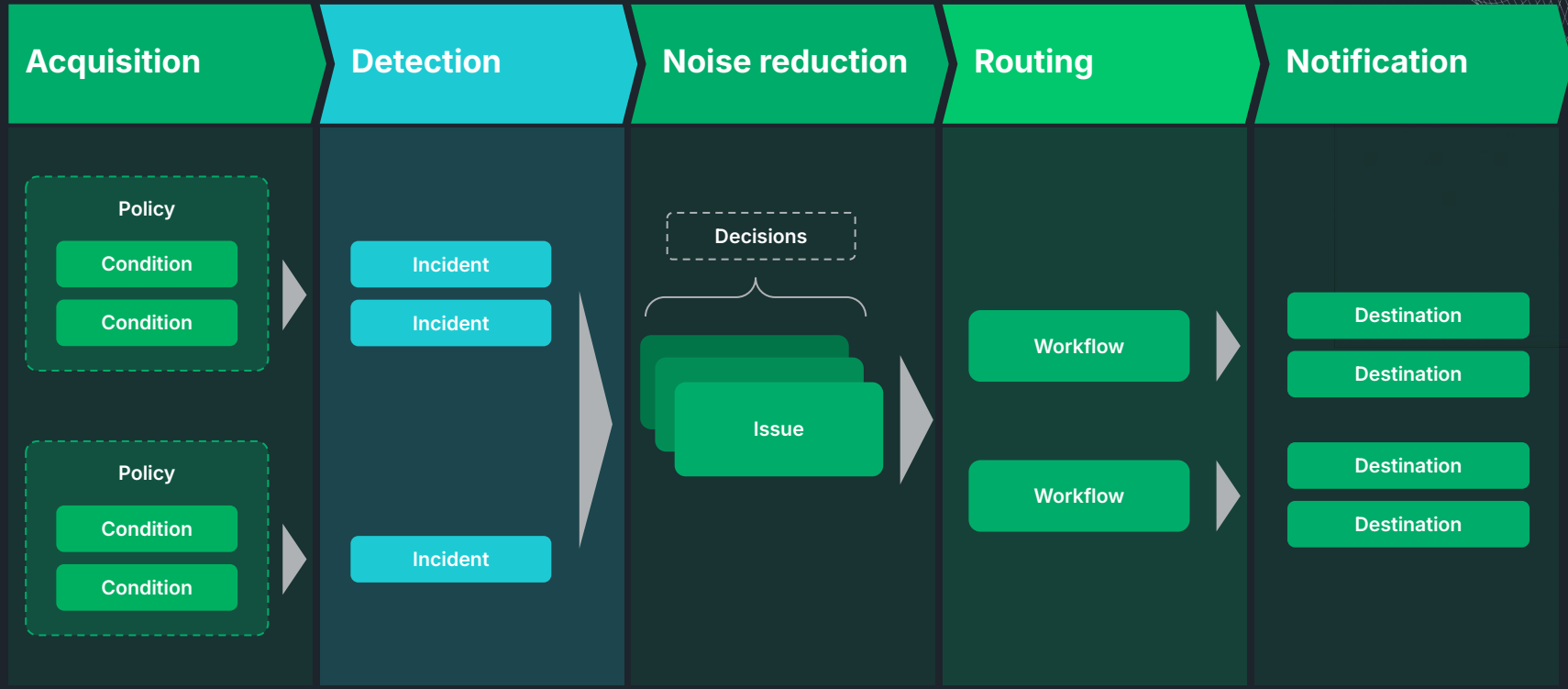
new relic

The Alert Pipeline



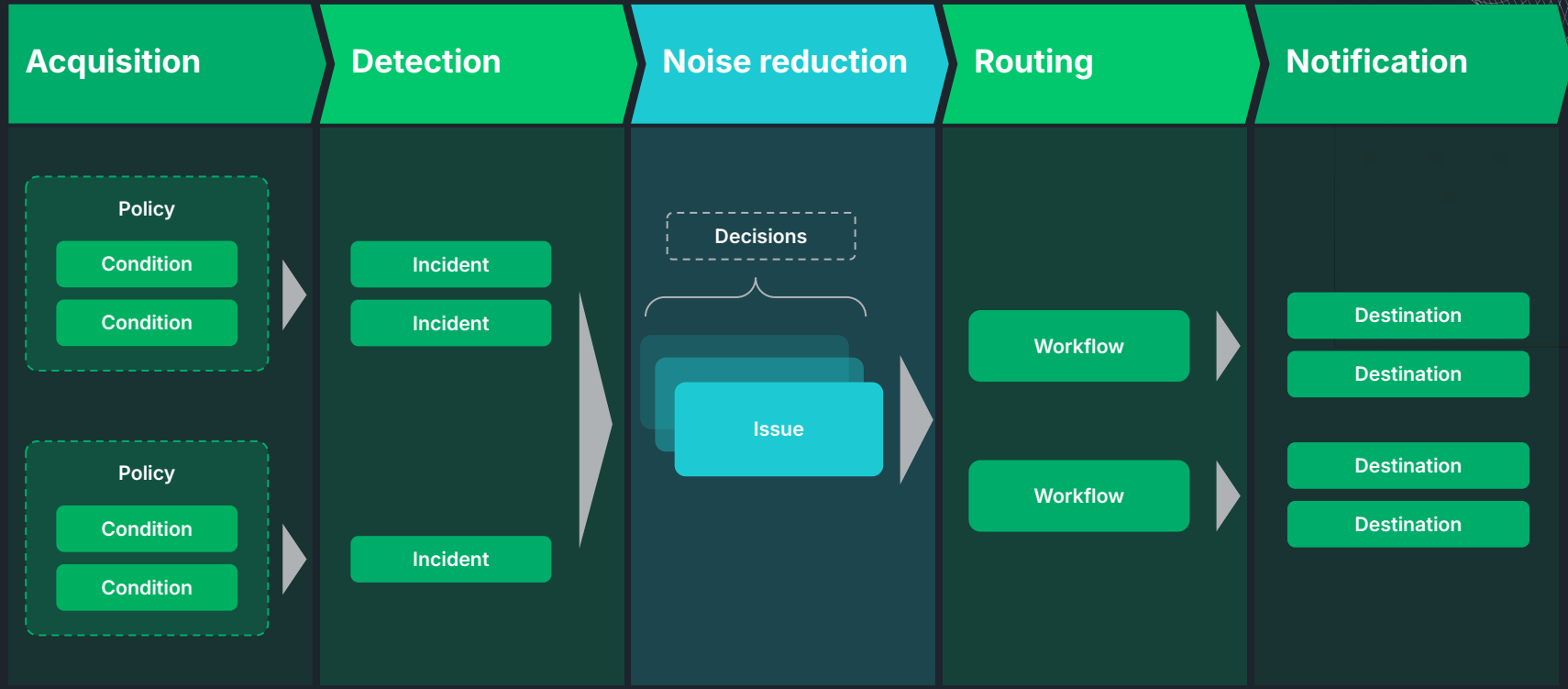
new relic

The Alert Pipeline



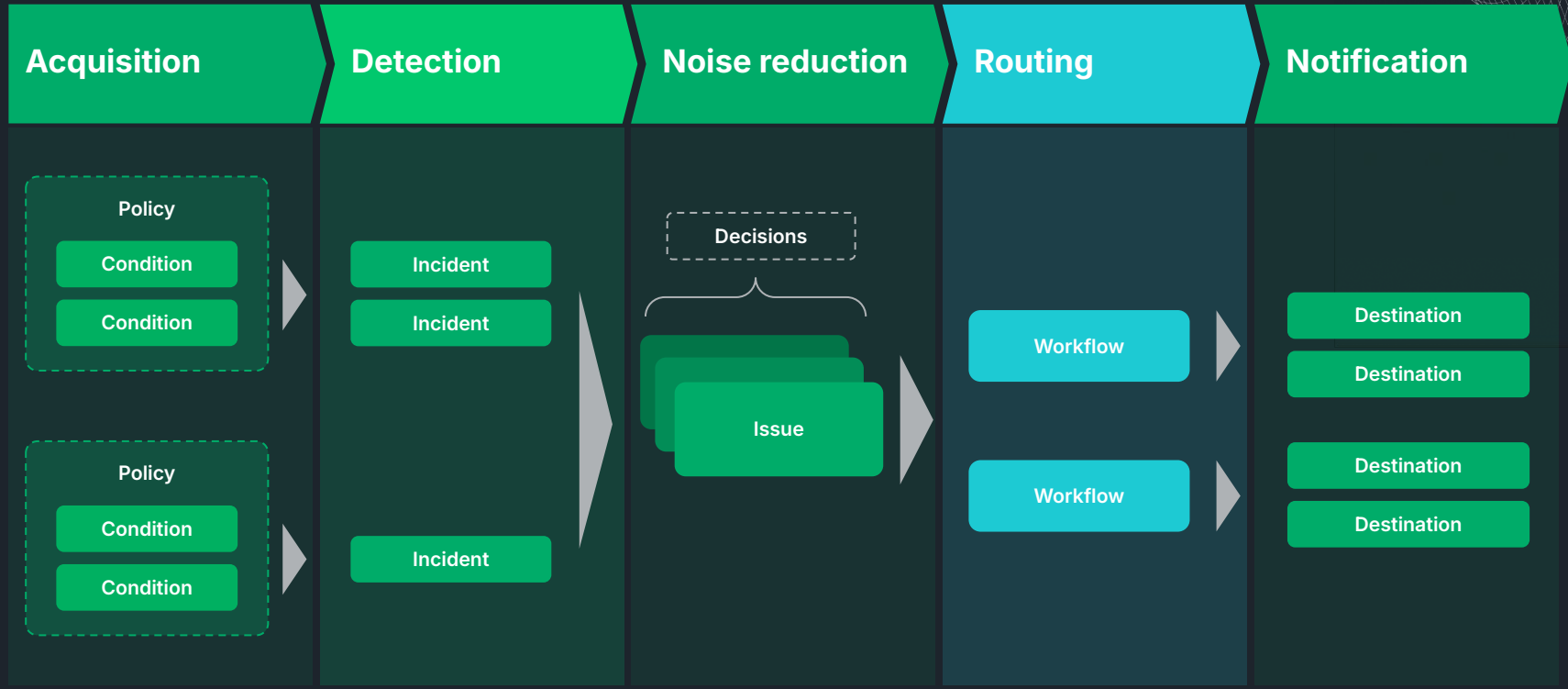
new relic

The Alert Pipeline



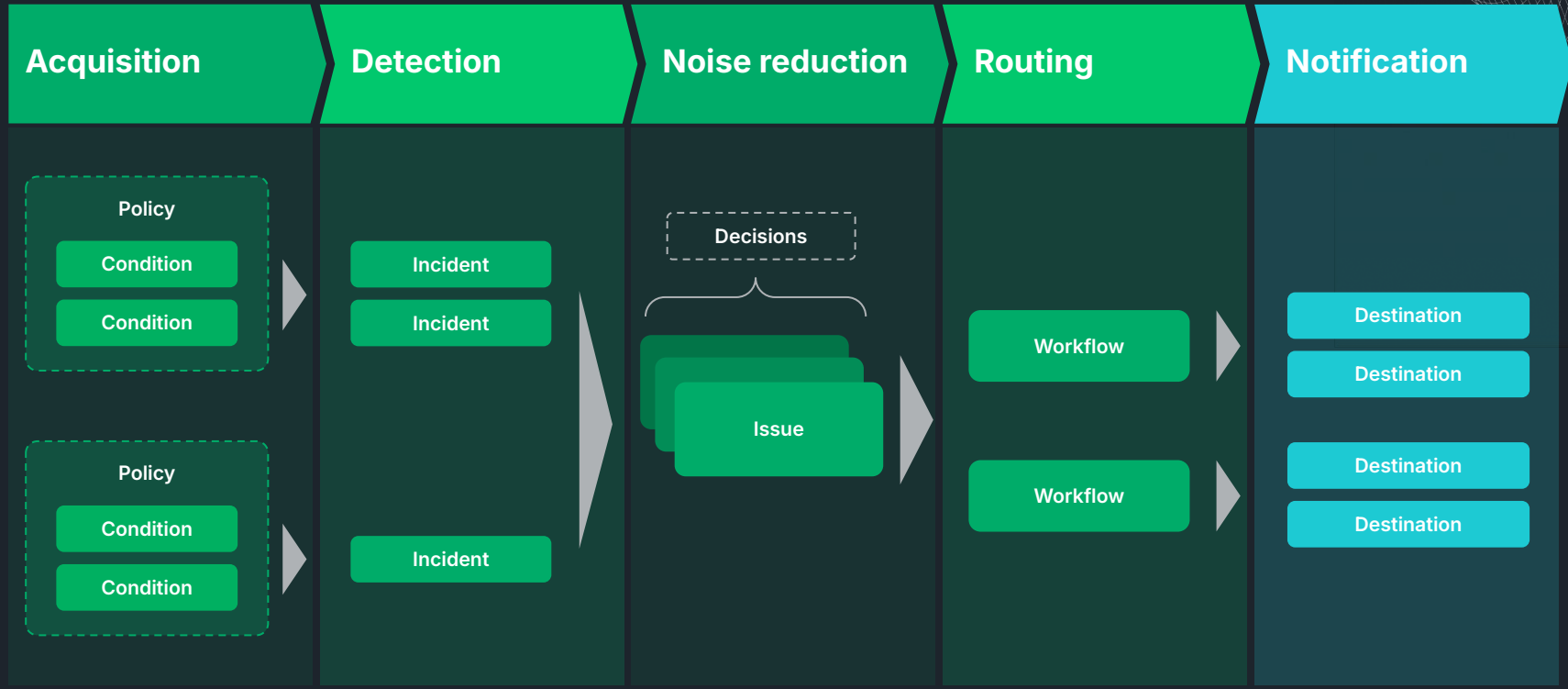
new relic

The Alert Pipeline



new relic

The Alert Pipeline



new relic

What is a “Signal”?

- **Any data** being sent to New Relic
- Result of an **NRQL query** against incoming data
- If you can **query it you can alert** on it!

Some examples

Class	Signal
Host Metrics	Resources, scaling, restarts
APM Golden Metrics	Latency, throughput, errors
Synthetic journeys	Success rate, duration
Log Data	Error messages, business data
Business metrics	Customers, satisfaction, $$$

What three key signals (data) would you set alerts upon?

new relic

Signals to alert on

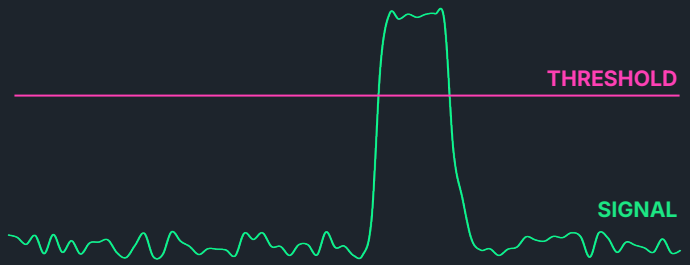
Some examples

- Host metrics - resources, scaling, restarts
- APM Golden metrics - latency, throughput, errors
- Mobile - crash rate by version, users affected by exception
- Key transactions
- Synthetic journeys - success rate, duration
- Log data - error messages, business data
- Business metrics - customers, satisfaction, $$$

- .... Your ideas here...

Conditions

Signal acquisition and evaluation



Signal query

Defined by NRQL query including optional WHERE and FACET clauses.

Guided wizard available to help build.

**Additional non-NRQL conditions soon to be deprecated*

Threshold

Value, which if breached by signal for a defined time period, will trigger an incident to be opened.

A threshold can be set for both **warning** and **critical**

Some examples

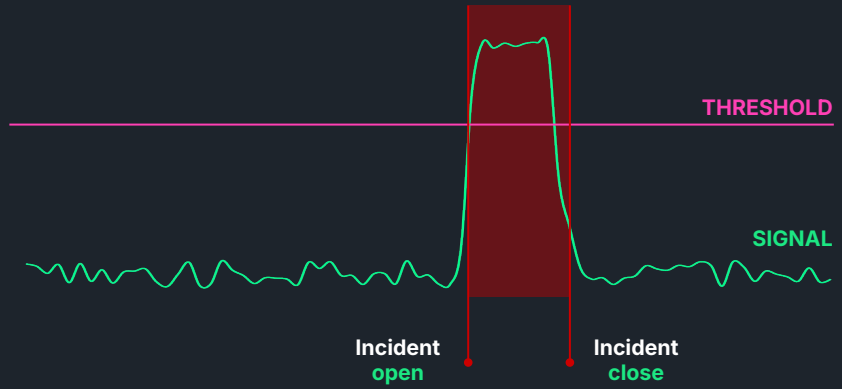
Signal	Threshold
% Error rate	% error **> 5%**
Average basket value	median(value) **< $20**
Login attempts per user	uniqueCount(user) **> 10**

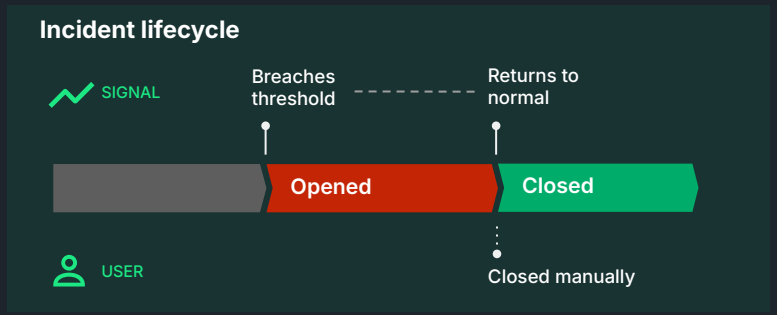
Documentation on alert conditions

new relic

Incidents

Signal breach detection



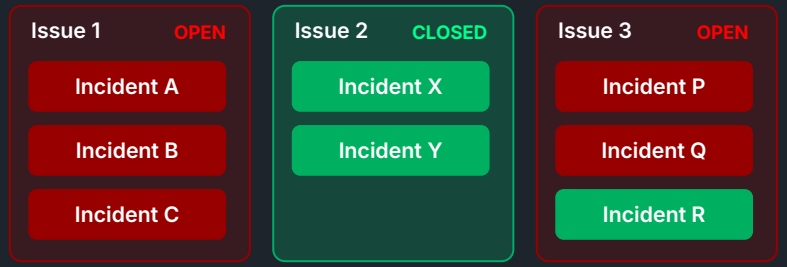


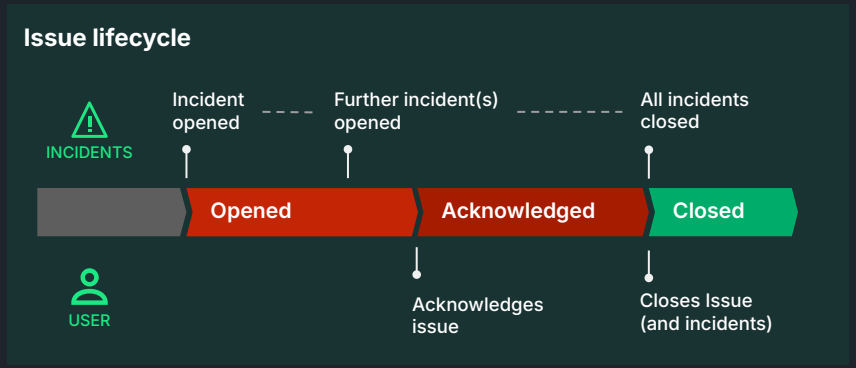
- Incidents **open** when a **signal breaches the threshold** defined in a condition.
- Incidents **close automatically** when the signal is no longer in breach.
- There will be some **latency** between signal breaching and incident opening based on condition settings.
- Incident will open for **each signal facet**
- Incidents can be **manually closed** by user

new relic

Issues

Incident management and noise reduction





"Incidents are the symptoms of a larger problem (the issue)"

Issues **group incidents together**, reducing noise and driving notification workflows.

- Issues are **opened when incidents open**
- Issues can **contain multiple incidents**
  based on policy preference or correlation decisions
- Issues **close automatically** when all contained incidents have closed or if inactive for defined period
- Issues can be **manually closed**, which close all contained incidents.

Documentation about issues

new relic

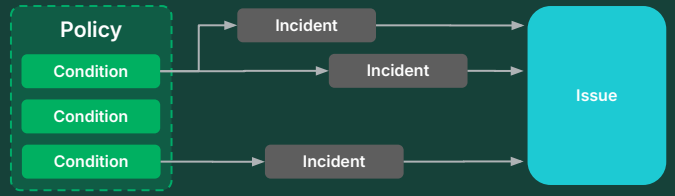
Policies

Predetermined incident grouping

FEWER ISSUES

MORE ISSUES

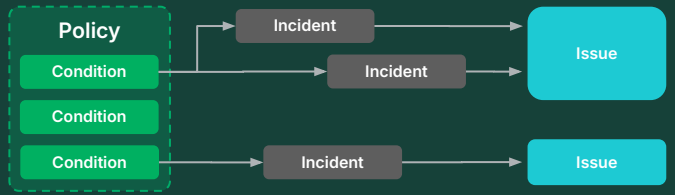
1 Per Policy



Only one issue will be open at a time for the **entire policy**.

- Requires immediate action and closing the issues to be effective

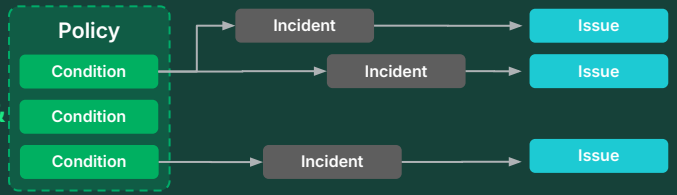
2 Per Condition



One issue will be open at a time for **each condition** in your policy.

- Useful for policies containing conditions that focus on entities that perform the same job

3 Per Condition & Signal



An issue will be created for **every incident** of **each condition** in your policy.

- Useful if you need to be notified of every violation or if you have an external system where you want to send alert notifications

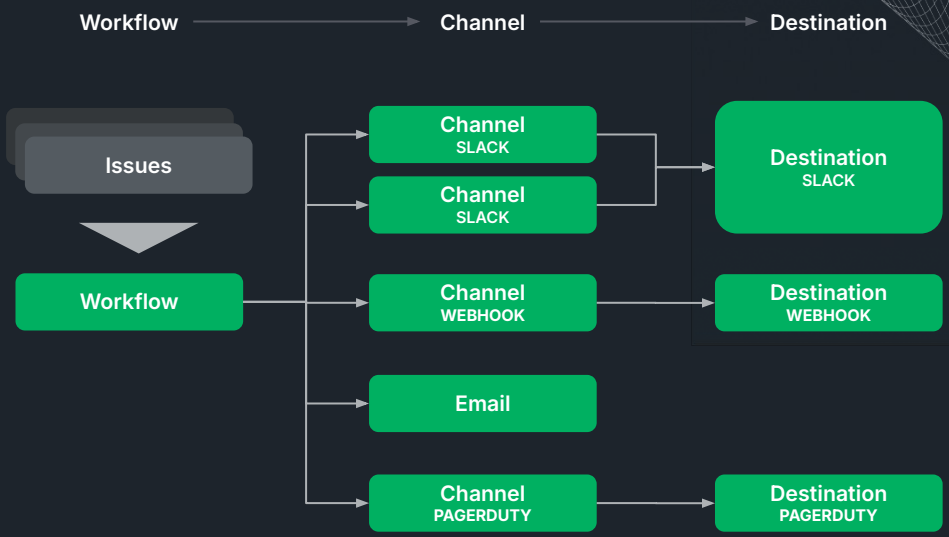
Documentation on alert policies / issue preference

new relic

Workflows

Notification triage and routing

- Control **when** you want to receive notifications about issues
- **Notify correct teams** based on issue context
- Channels offer comprehensive **payload templating** options
- **Enrich notifications** with additional New Relic data



Channels allow **multiple different message payloads** to be sent to **multiple destinations**

Documentation on setting up workflows

new relic

Destinations

Notification dispatch

Destination inform **people** or **third party services** about issues state change.

Supported destinations:

- Email & mobile push
- Native: Jira*, ServiceNow*, PagerDuty*, Slack
- Webhook: e.g. OpsGenie, MS Teams, etc..
- AWS EventBridge

Destinations **setup once per account** and can be used by multiple workflows.

*two way integrations

Documentation on notification destinations

03 Platform demo

new relic

Alert Design Concept: Tiered Alerts

Tier 1 - Immediate Response

For business / user impacting issues.

Good for:

- Always-actionable alerts
- Alert conditions with severe thresholds (e.g. 25% drop in traffic)
- Golden signal alerts on critical services tuned to not flap - using multiple conditions or longer evaluation windows.

Tier 2 - Same Business Day

For emerging issues or modest degradations.

Good for:

- SLO Error budget alerts.
- Predictive alerts with 1 day+ timeline.

Use tagging or naming conventions make expected response timelines clear.

Tier 3 - Informational Only

Created by an engineer or an SRE for informational, aspirational, or learning purposes only.

Filter from other tier alerts via tagging or naming conventions.

Performance Degradation Detection

Using Service Levels and Alerts

Good	Report	Review	Urgent	Most Urgent
Period over period Service Levels shows you what runs well.	Period over period Service Levels shows you where to improve.	Operational Service levels and error budget alerting shows you what requires an engineer to review within 1 business day.	Alerts with time windows up to an hour let you see if a modest decline in performance resolves itself before you act.	Alerts with short time windows allow you to act immediately if performance drops significantly.
		Tier 2 - Same Business Day	Tier 1 - Immediate Response 	Tier 1 - Immediate Response 

new relic

Service Levels vs Alerts

	Service Levels	Alerts
View of performance	Over time	Real time
Reduces MTTD by	Revealing problematic areas and gradual performance deterioration	Notifying engineering teams of a current issue
Thresholds	Closely aligned with expectations	Far enough from normal to require immediate review
Reviewed	Daily, Weekly, or per sprint	Immediately after trigger
Tune	Periodically, such as quarterly	After an incident, as needed
Used for executive reporting	Yes	No

Service Level Signals vs Alert Signals

	Service Levels	Alerts
Boundary applications	Yes	Yes
Web and mobile applications	Yes	Yes
Synthetics	Yes	Yes
Shared services & Platform	Yes	Yes
Low level compute metrics	**No**	Yes

05 Next steps

new relic

Resources

New Relic University course:

- New Relic University courses: NRU Alerts
- Also be sure to view the Hands-on tutorials

Blog posts:

- Best practices for fixing your alerts
- Alert! Best practices for alert quality

Setup guides:

- How to configure workflow email destinations
- Setup a JIRA workflow destination
- Send notifications to Slack using workflow destinations
- How to configure workflow Pagerduty destinations
- How to to configure ServiceNow workflow destinations

Documentation links:

- Alert conditions
- Issues and incident management
- Alert policies
- Issue incident grouping preference
- Workflows in New Relic
- Notification destination integrations

Videos:

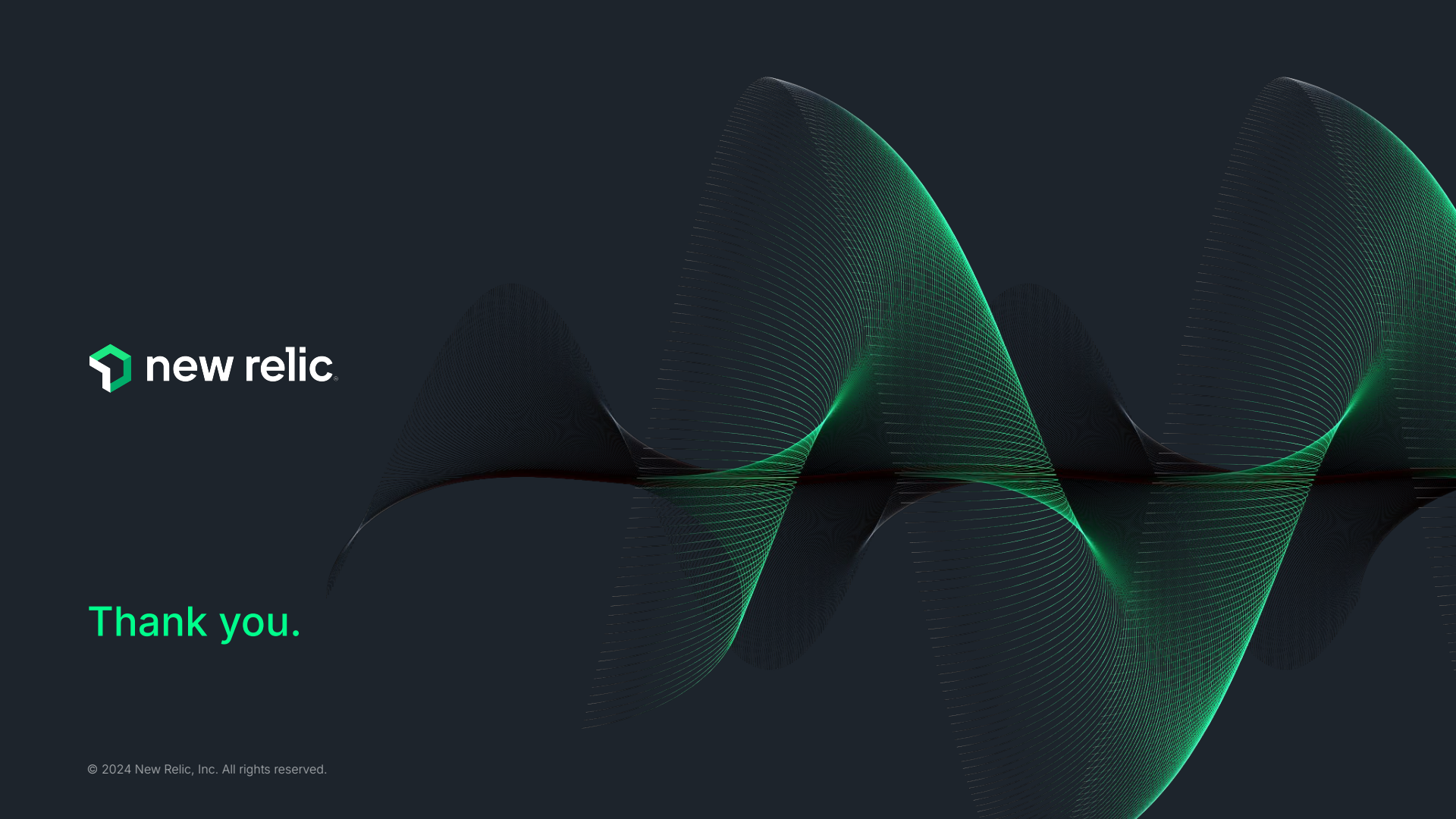
- The New Alert Condition Creation Form
- Never miss an alert with New Relic's mobile app
- Setting Muting Rules for Workflows
- How to set up webhook destinations for workflows
- Set up Sliding Window Aggregation in your Alert Conditions
- Alert aggregation methods explained

New Relic Docs
docs.newrelic.com

Explorer's Hub
forum.newrelic.com

Developer's Site
developer.newrelic.com

new relic



Thank you.

Additional slides

Information regarding related capabilities.
You may choose to include them in your presentation too.

new relic

Alert quality management

Improving and optimizing the quality of your alerting

- Strategies to focus on **reducing the number of nuisance incidents** so that you focus only on alerts with **true business impact**
- Ensure that **fewer, more valuable**, incidents are created
- Includes **strategies, best practice** and **tooling** for measuring and analysing **alert quality**

Documentation on alert quality management

new relic

NRQL condition tuning

Improving signal acquisition

Many more features for refining how signal data is processed and evaluated.

Fine tuning

Configure aggregation windows, delay and streaming methods to reliably process your signal

Gap filling

Reduce false alerts caused by sporadic data by specifying gap filling strategy

Signal loss

What to do if a signal is no longer being received

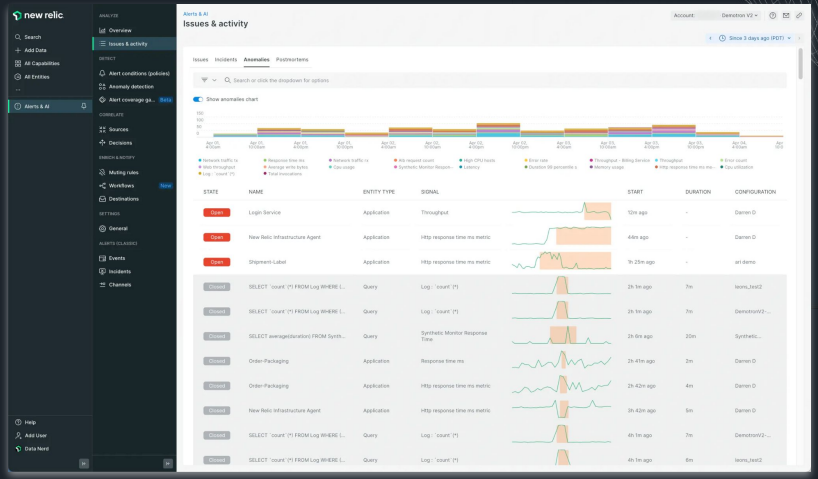
Documentation on NRQL condition tuning

new relic

Anomaly detection

Get alerted for unusual behaviour

- Applied intelligence automatically surfaces unusual behaviour of your golden signals
- Customise your own anomalous behaviour detection with NRQL conditions



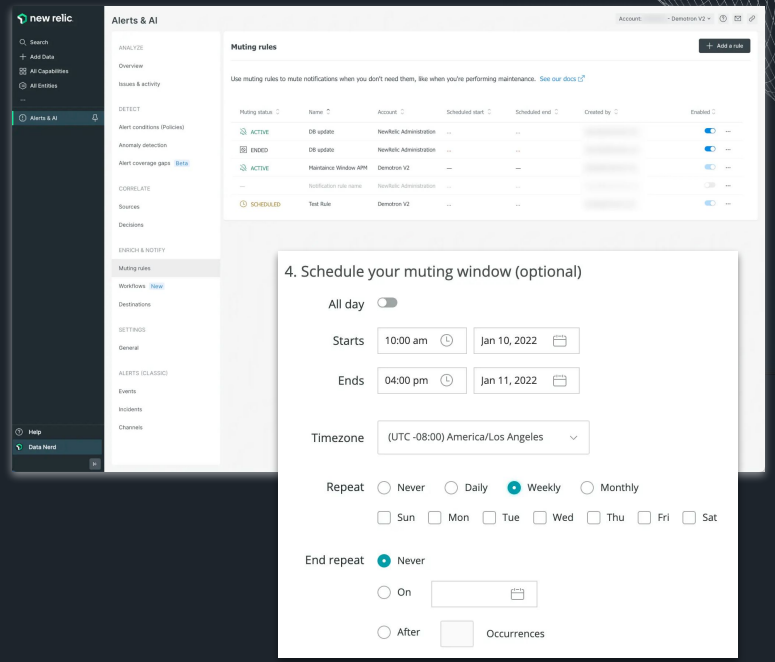
Documentation on anomaly detection

new relic

Muting rules

Temporarily mute notifications

- Mute **issue notifications**, for instance when **performing maintenance** or known **down periods**
- Issues are **still generated and queryable,** they just don't send notifications.
- **Filter incidents** by attribute, can target multiple workflows and destinations.
- Muting rules can be **scheduled and repeatable**



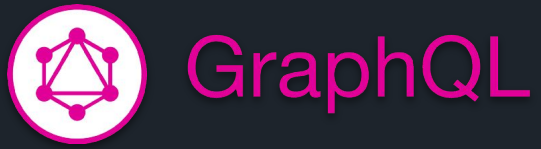
Documentation on muting rules

new relic

Observability as code

Manage your alerts with code

- Use graphQL (or Terraform) to **manage alerts programmatically**
- Allows for better **auditing** and **change control**
- Build workflows to **generate alerts automatically** from configuration



- Scale
- Stability
- Reusability
- Automation
- Compliance
- Security
- Innovation

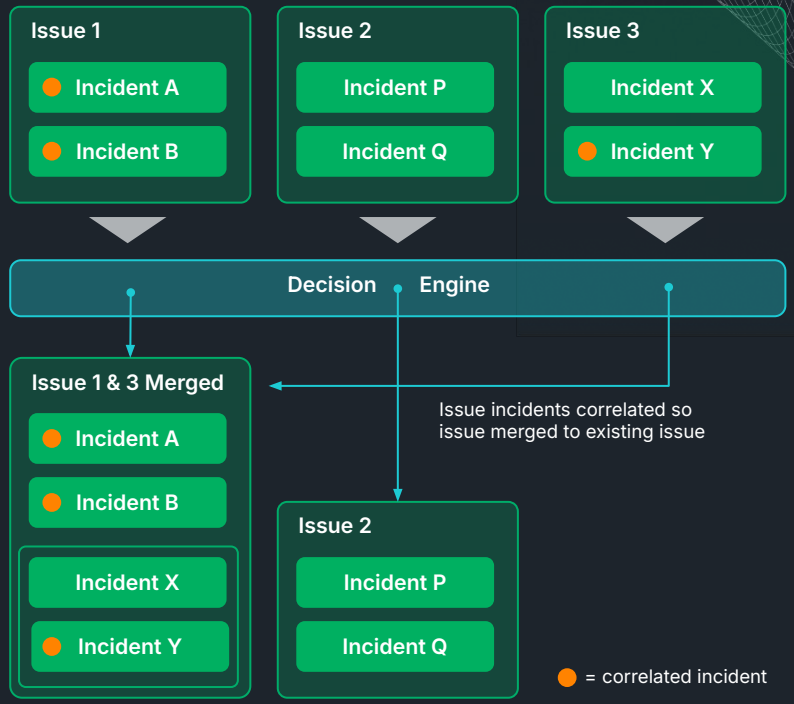
Documentation on Observability as Code

new relic

Decisions

Advanced noise reduction

- Decisions **reduce noise** by **merging issues** containing correlated incidents
- New issues are **merged to existing ones**
- **All incidents** within the issues are merged
- Decisions can be **customised** based on incident **attribute values, context and topology**



Documentation on issue correlation using decisions

new relic