MC MONTE CARLO

Monte Carlo Mastery: Creating an Alert Strategy that Guarantees Action

Meet your hosts

Jennifer Hubert

Solutions Architect

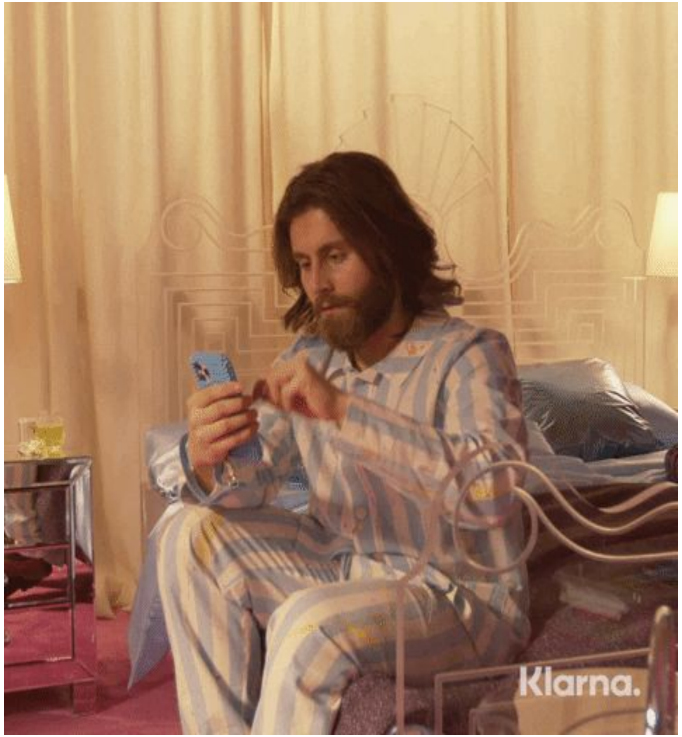
Steve Stenberg

Customer Success Manager

Agenda

- What is Alert Fatigue?
- Causes of Alert Fatigue
- Best Practices
- Takeaways

What is alert fatigue?



alert fatigue 😩 is an instance where an overwhelming number of alerts causes an individual to become desensitized to them. Alert fatigue can lead to a person **ignoring or failing to respond** to a number of safety alerts.

MC MONTE CARLO

The importance of alert ratios

# Alert Received	# Alerts I care about	Emotion
1	1	😍
2	1	😃
3	1	🙂
4	1	😟
5	1	😲
6	1	😭
7	1	😱
8	1	😩
9	1	😡

◀ **Mute**

The number of alerts I receive

vs

The number of alerts I care about

Types of alert fatigue

Types of Alert Fatigue

1. Scope is too wide

2. Custom monitors are noisy

3. Notifications aren’t segmented

Scope is too wide

Issue

You are receiving too many alerts generated from automatic / OOTB detectors

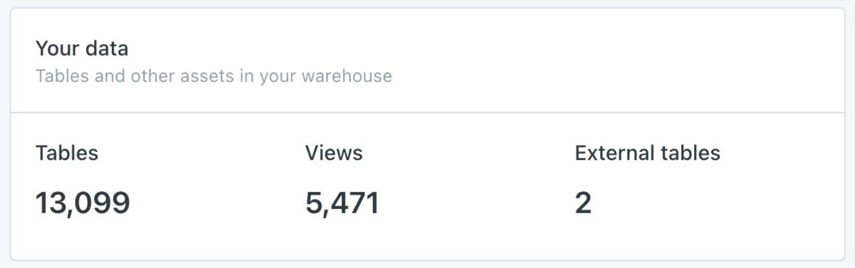
Solution

Scope down your tables to the most important use cases for the business

Resources

Insights reports - Use Key Assets & Cleanup Suggestions

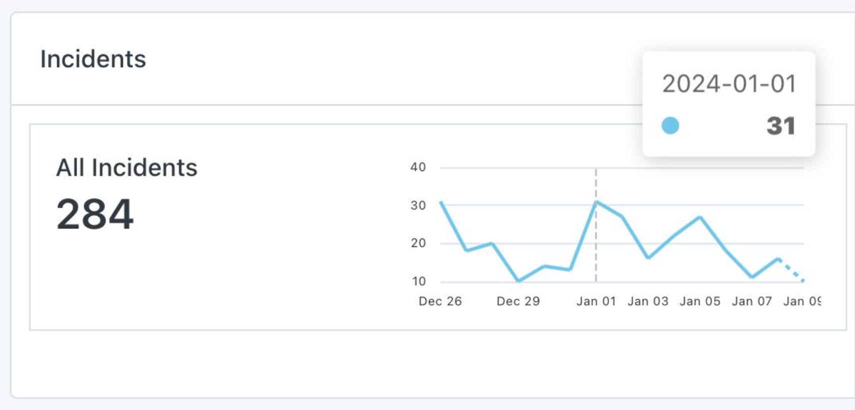
Muting tables



Your data

Tables and other assets in your warehouse

Tables	Views	External tables
13,099	5,471	2



Incidents

All Incidents

284

2024-01-01

● 31

Custom monitors are noisy

Issue

You are receiving too many alerts generated from custom monitors

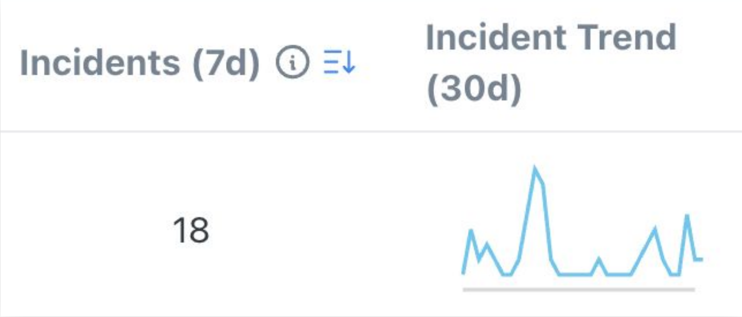
Solution

Update monitors to breach less frequently by editing the rule logic, changing breach thresholds or reducing notifications

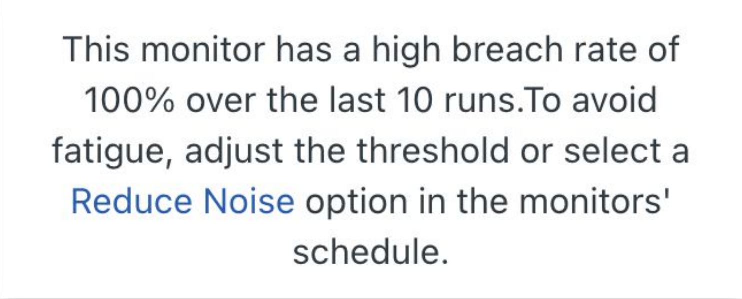
Resources

Insights reports - Use Notifications by Custom Monitor & Misconfigured Monitors

Misconfigured monitors daily digest



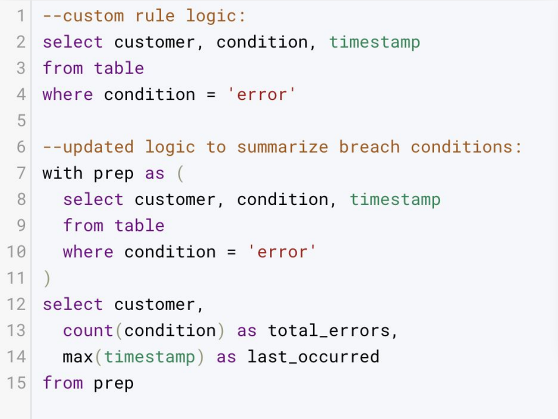
Incidents (7d) ⓘ	Incident Trend (30d)
18	



This monitor has a high breach rate of 100% over the last 10 runs.To avoid fatigue, adjust the threshold or select a Reduce Noise option in the monitors' schedule.

3 ways to reduce custom monitor noise

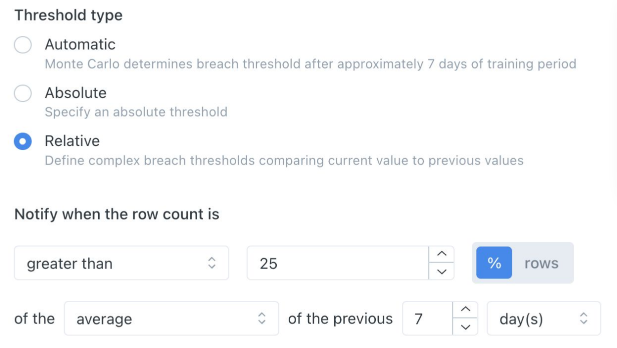
Update monitor logic



```
--custom rule logic:
select customer, condition, timestamp
from table
where condition = 'error'

--updated logic to summarize breach conditions:
with prep as (
  select customer, condition, timestamp
  from table
  where condition = 'error'
)
select customer,
  count(condition) as total_errors,
  max(timestamp) as last_occurred
from prep
```

Update thresholds



Threshold type

○ Automatic
Monte Carlo determines breach threshold after approximately 7 days of training period

○ Absolute
Specify an absolute threshold

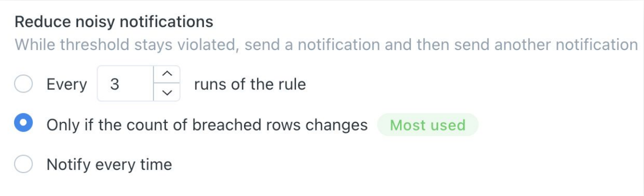
● Relative
Define complex breach thresholds comparing current value to previous values

Notify when the row count is

greater than | 25 | [✓ %] rows

of the average of the previous 7 day(s)

Update notification frequency



Reduce noisy notifications
While threshold stays violated, send a notification and then send another notification

○ Every 3 runs of the rule

● Only if the count of breached rows changes Most used

○ Notify every time

MONTE CARLO

Notifications aren’t segmented

Issue

All notifications are funneling into one channel

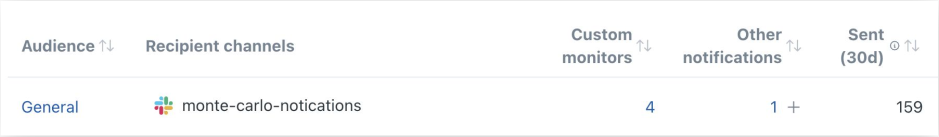
Solution

Split out notifications into high priority and lower priority channels

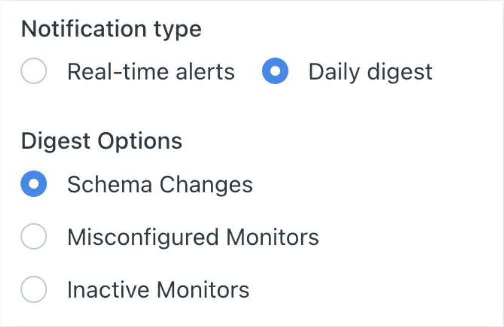
Resources

[Filter notifications by Key Assets or Importance Score]()

[Schema changes daily digest]()



Audience	Recipient channels	Custom monitors	Other notifications	Sent (30d)
General	monte-carlo-notications	4	1 +	159



Notification type

○ Real-time alerts ● Daily digest

Digest Options

● Schema Changes

○ Misconfigured Monitors

○ Inactive Monitors

Alert Strategy Best Practices

Key Components of Approach

Ownership

Who is responsible for responding?

Priority Levels

Which assets are most important?

SLAs

What time frame do you need a response in based on Priority?

Notification Levers

Muting

Mute Datasets and Tables that are less relevant

Domains

Use domains to build subsets of owned tables

Key Assets

Focus on the most important assets in the business

Importance Score

Filter notifications based on most important tables

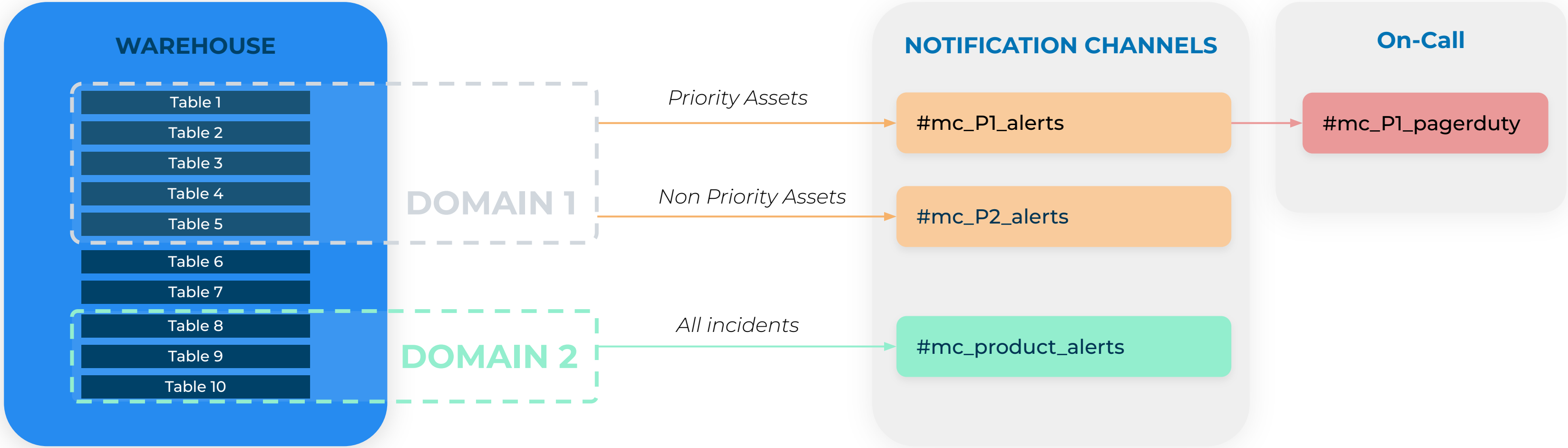
Notification Channels

Siphon notifications into different channels

Tagging

Leverage Tags to build notification channels or directly ping table owners in messages

Monitor Strategy



MC MONTE CARLO

Takeaways

1

3 Main Types of Alert Fatigue

Wide Scope, Noisy Custom Monitors, and Non-Segmented Notification

2

3 Key Components of Approach

Ownership, Priority Level, and SLA's

3

Alert Ratio

Number of alerts received vs number of alerts you care about. Aim for 4:1 ratio or lower!

4

6 Main Notification Levers

Muting, Domains, Key Assets, Importance Score, Tagging, and Notification Channel

Questions?

Thank you