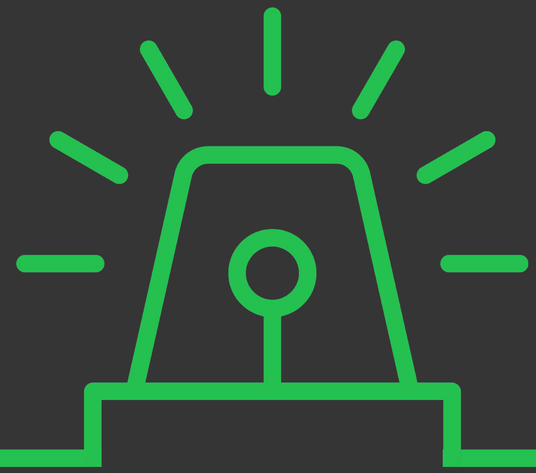
BLAMELESS POSTMORTEMS
HOW TO ACTUALLY DO THEM

Lilia Gutnik
Product Manager & Serious Grown-Up, PagerDuty

Matty Stratton
DevOps Advocate & Thought Validator, PagerDuty



pagerduty

@superlilia
@mattstratton

What will we cover

- What is a Postmortem?
- Blameless Culture
- How to Write a Postmortem
- Postmortem Meetings
- Putting it into Practice

@superlilia
@mattstratton

What **is** a postmortem?

@superlilia
@mattstratton

What went wrong, and how do we **learn** from it?

@superlilia
@mattstratton

Organizations may refer to the postmortem process in slightly different ways

After-Action Review

Post-Incident Review

Learning Review

Incident Review

Incident Report

Root Cause Analysis (or RCA)

@superlilia
@mattstratton

Why do postmortems?

@superlilia
@mattstratton

KEY TAKEAWAY

The postmortem process drives focus, instills a culture of learning, and identifies opportunities for improvement that otherwise would be lost.

@superlilia
@mattstratton

When to do a postmortem

@superlilia
@mattstratton

Do a postmortem after every major incident

@superlilia
@mattstratton

Postmortems are done shortly after the incident is resolved, while the context is still fresh for all responders.

@superlilia
@mattstratton

Who is responsible for the postmortem?

@superlilia
@mattstratton

Designate a single owner

@superlilia
@mattstratton

Ownership Criteria

- Took a leadership role during the incident
- Performed a task that led to stabilizing the service
- Was the primary on-call responder for the most heavily affected service
- Manually triggered the incident to initiate incident response

@superlilia
@mattstratton

Dedicated investigators

@superlilia
@mattstratton

Postmortems are not a punishment

@superlilia
@mattstratton

Blameless

@superlilia
@mattstratton

KEY TAKEAWAY

The impulse to blame and punish has the unintended effect of disincentivizing the knowledge sharing required to prevent future failure

@superlilia
@mattstratton

KEY TAKEAWAY

The goal of the postmortem is to understand what systemic factors led to the incident and identify actions that can prevent this kind of failure from recurring

@superlilia
@mattstratton

Why blamelessness is **hard**

@superlilia
@mattstratton

J. Paul Reed

Principal Consultant, Release Engineering Approaches

Humans are hardwired through millions of years of evolutionary neurobiology and thousands of years of social conditioning to use the technique of blaming as a way to give voice to painful and uncomfortable feelings, in order to effectively disperse them from our psyches

@superlilia
@mattstratton

By being aware of our biases, we will be able to identify when they occur and work to move past them

@superlilia
@mattstratton

Fundamental attribution error

@superlilia
@mattstratton

Confirmation bias

@superlilia
@mattstratton

Hindsight bias

@superlilia
@mattstratton

Negativity bias

@superlilia
@mattstratton

Bias	Definition	Countermeasure
Fundamental attribution error	What people do reflects their character rather than their circumstances.	Discuss ‘what’ questions instead of ‘who’. Focus on the system, the infrastructure, and the situation - not the people involved.
Confirmation bias	Favoring information that reinforces existing positions.	Appoint someone to play devil’s advocate to take contrarian viewpoints during investigations.
Hindsight bias	Seeing the incident as inevitable despite there having been little or no objective basis for predicting it because we know the outcome.	Explain events in terms of foresight instead. Start your timeline analysis at a point before the incident, and work your way forward instead of backward from resolution.
Negativity bias	Things of a more negative nature have a greater effect on one’s mental state than neutral or even positive things.	Reframe incidents as learning opportunities, and remember to describe what was handled well in incident response.

@superlilia
@mattstratton

How to avoid blame

@superlilia
@mattstratton

KEY TAKEAWAY

Ask "*what*" and "*how*" questions rather than "*who*" or "*why*"

@superlilia
@mattstratton

Consider multiple and diverse perspectives

@superlilia
@mattstratton

Ask yourself why a reasonable, rational, and decent person may have taken a particular action

@superlilia
@mattstratton

Abstract to an inspecific responder

@superlilia
@mattstratton

Contrast what you did not intend with what you **do** intend

@superlilia
@mattstratton

How to introduce postmortems

@superlilia
@mattstratton

Sell the business value of blamelessness

@superlilia
@mattstratton

Acknowledge that practicing blamelessness is difficult for everyone

@superlilia
@mattstratton

Get buy-in from individual contributors too

@superlilia
@mattstratton

Psychological safety

@superlilia
@mattstratton

Amy Edmondson

Professor, Harvard Business School

[Psychological safety is] a sense of confidence that the team will not embarrass, reject, or punish someone for speaking up.

@superlilia
@mattstratton

Conversational turn-taking

@superlilia
@mattstratton

High social sensitivity or empathy

@superlilia
@mattstratton

Start small

@superlilia
@mattstratton

Information sharing

@superlilia
@mattstratton

Being transparent about system failure reinforces a culture of blamelessness

@superlilia
@mattstratton

Create a community of experienced postmortem writers to review postmortem drafts and spread good practices

@superlilia
@mattstratton

Schedule postmortem meetings on a shared calendar

@superlilia
@mattstratton

Email completed postmortems to all teams involved in incident response

@superlilia
@mattstratton

Accountability

@superlilia
@mattstratton

Set a policy for postmortem action items

@superlilia
@mattstratton

Clarify ownership of postmortem action items

@superlilia
@mattstratton

Engage the leaders that prioritize work

@superlilia
@mattstratton

Open tickets for postmortem action items in your work management ticketing system

@superlilia
@mattstratton

Actually doing it

@superlilia
@mattstratton

The Steps

1. Create a new postmortem for the incident.
2. Schedule a postmortem meeting within the required timeframe for all required and optional attendees on the "Incident Postmortem Meetings" shared calendar.
3. Populate the incident timeline with important changes in status/impact and key actions taken by responders.
    - For each item in the timeline, include a metric or some third-party page where the data came from.
4. Analyze the incident.
    - Identify contributing factors
    - Consider technology and process.
5. Open any follow-up action tickets.
6. Write the external messaging.
7. Ask for review.
8. Attend the postmortem meeting.
9. Share the postmortem.

@superlilia
@mattstratton

Owner responsibilities

- **Scheduling the postmortem meeting** on the shared calendar and inviting the relevant people (this should be scheduled within 3 business days for a Sev-1 and 5 business days for a Sev-2).
- **Investigating the incident**, pulling in whomever you need from other teams to assist in the investigation.
- **Ensuring the page is updated** with all of the necessary content. Use your organization's template for what should be included.
- **Creating follow-up tickets**. (You are only responsible for creating the tickets, not following them up to resolution).
- **Reviewing the postmortem content with appropriate parties** before the meeting. Running through the topics at the postmortem meeting (the Incident Commander will "run" the meeting and keep the discussion on track, but you will likely be doing most of the talking).
- **Communicating the results** of the postmortem internally.

@superlilia
@mattstratton

Administration

@superlilia
@mattstratton

Who should attend?

- Service owners involved or impacted in the incident.
- Key engineer(s)/responders involved in the incident.
- Engineering manager for impacted systems.
- Product manager for impacted systems.
- Customer liaison (only for Sev-1 incidents).
- Incident commander and/or a facilitator
- Incident commander deputy, shadow, scribe (if present).

@superlilia
@mattstratton

Create a timeline

@superlilia
@mattstratton

Timeline tips

- Stick to the facts.
- Include changes to incident status and impact.
- Include key decisions and actions taken by responders.
- Illustrate each point with a metric.

@superlilia
@mattstratton

Document the impact

@superlilia
@mattstratton

Analyze the incident

@superlilia
@mattstratton

KEY TAKEAWAY

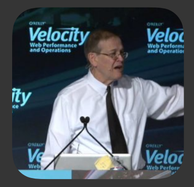
There is no single root cause of major failure in complex systems, but a combination of contributing factors that together lead to failure

@superlilia
@mattstratton

KEY TAKEAWAY

An individual's action should never be considered a root cause.

@superlilia
@mattstratton



Dr. Richard Cook

Department of Integrated Systems Engineering at the Ohio State University

All practitioner actions are actually gambles, that is, acts that take place in the face of uncertain outcomes.

@superlilia
@mattstratton

Check data

@superlilia
@mattstratton

Helpful questions

- Is it an isolated incident or part of a trend?
- Was this a specific bug, a failure in a class of problem we anticipated, or did it uncover a class of issue we did not architecturally anticipate?
- Was there work the team chose not to do in the past that contributed to this incident?
- Research if there were any similar or related incidents in the past. Does this incident demonstrate a larger trend in your system?
- Will this class of issue get worse/more likely as you continue to grow and scale the use of the service?

@superlilia
@mattstratton

Follow-up actions

@superlilia
@mattstratton

Action items

- Actionable
- Specific
- Bounded

@superlilia
@mattstratton

Poorly Worded	Better
Investigate monitoring for this scenario.	**Actionable**: Add alerting for all cases where this service returns >1% errors.
Fix the issue that caused the outage.	**Specific**: Handle invalid postal code in user address form input safely.
Make sure engineer checks that database schema can be parsed before updating.	**Bounded**: Add automated presubmit check for schema changes.

@superlilia
@mattstratton

Don’t create too many tickets

@superlilia
@mattstratton

The person who creates the ticket is not responsible for completing it

@superlilia
@mattstratton

Write external messaging

@superlilia
@mattstratton

External messaging components

- **Summary**: Two to three sentences that summarize the duration of the incident and the observable customer impact.
- **What Happened**: Summary of contributing factors. Summary of customer-facing impact during the incident. Summary of mitigation efforts during the incident.
- **What Are We Doing About This**: Summary of action items.

@superlilia
@mattstratton

Postmortem Review

pagerduty

@superlilia
@mattstratton

Do

- Make sure the timeline is an accurate representation of events.
- Define any technical lingo/acronyms you use that newcomers may not understand.
- Separate what happened from how to fix it.
- Write follow-up tasks that are actionable, specific, and bounded in scope.
- Discuss how the incident fits into our understanding of the health and resiliency of the services affected.

@superlilia
@mattstratton

Don’t

- Don't use the word "outage" unless it really was an outage.
- Don’t change details or events to make things "look better.”
- Don’t name and shame someone.
- Avoid the concept of "human error."
- Don’t just point out what went wrong.

@superlilia
@mattstratton

The postmortem meeting

@superlilia
@mattstratton

Send the postmortem document in advance

@superlilia
@mattstratton

KEY TAKEAWAY

The most important outcome of the postmortem meeting is buy-in for the action plan

@superlilia
@mattstratton

Participants

Incident Commander

Incident Commander
Shadow, Scribe, Deputy

Service Owners

Engineering Managers

Product Managers

Customer Liaison

@superlilia
@mattstratton

Facilitation

@superlilia
@mattstratton

Facilitator's Role

- Encourage people to speak up, and make sure that everyone is heard.
- Clarify insights and challenge the team with questions.
- Help the team to see different angles and different options.
- Keep everyone on time and on track. Cut off tangents and stop people from dominating the entire meeting.

@superlilia
@mattstratton

More on facilitation

- The facilitator does not make decisions.
- The facilitator does not take sides.
- Try to speak as little as possible.
- Be a shadow that guides discussions, not a presenter who takes over the meeting.

@superlilia
@mattstratton

Who should facilitate?

@superlilia
@mattstratton

Facilitator competencies

- Reads non-verbal cues to assess how people are feeling in the room and sees who might have something to say.
- Paraphrases what is said to clarify for self and others.
- Asks open questions to stimulate deeper thinking.
- Comfortable interrupting when discussion gets off track or someone dominates the discussion.
- Redirects conversation to focus on goals.
- Drives discussion to decision making and action items.

@superlilia
@mattstratton

Facilitation tips

@superlilia
@mattstratton

Housekeeping

- Set ground rules at the beginning of the meeting.
- Establish a safeword for when the conversation gets off track.
- Share the agenda so the team is clear on what is on- and off-topic.
- Use a timer to timebox.
- Present the postmortem document from your laptop onto the TV so everyone can see.

@superlilia
@mattstratton

Avoid blame

@superlilia
@mattstratton

Keep on-topic

@superlilia
@mattstratton

One person dominating?

@superlilia
@mattstratton

Encourage contributions

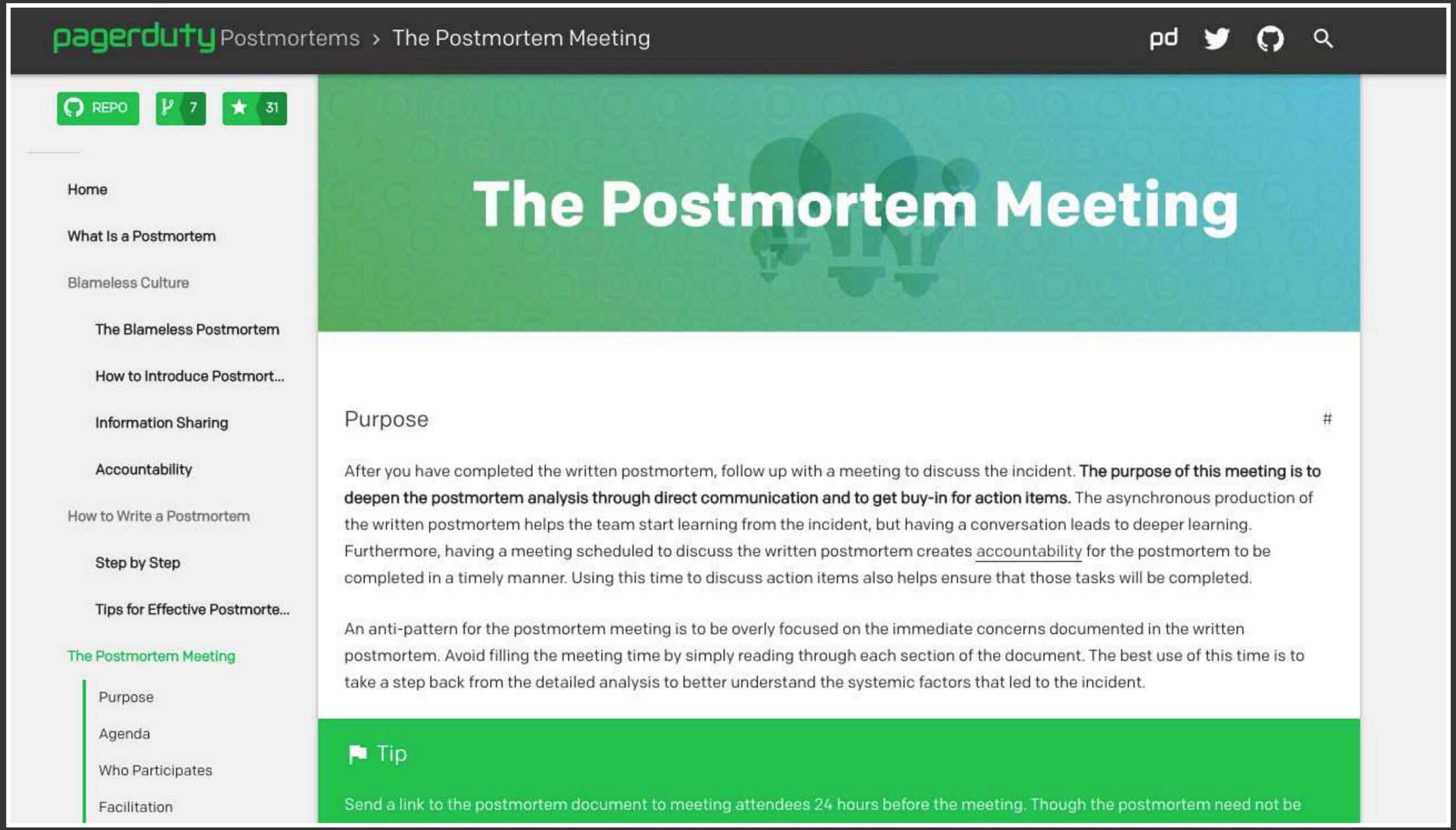
@superlilia
@mattstratton

Practice makes perfect

@superlilia
@mattstratton

https://postmortems.pagerduty.com

@superlilia
@mattstratton



@superlilia
@mattstratton

pduty.me/dodmsp

@superlilia
@mattstratton

Key Takeaways

- The postmortem process drives focus, instills a culture of learning, and identifies opportunities for improvement that otherwise would be lost.
- The goal of the postmortem is to understand what systemic factors led to the incident and identify actions that can prevent this kind of failure from recurring
- The most important outcome of the postmortem meeting is buy-in for the action plan
- Ask “what” and “how” questions rather than “who” or “why”
- There is no single root cause of major failure in complex systems, but a combination of contributing factors that together lead to failure
- An individual’s action should never be considered a root cause.
- The impulse to blame and punish has the unintended effect of disincentivizing the knowledge sharing required to prevent future failure

@superlilia
@mattstratton

Let’s practice!

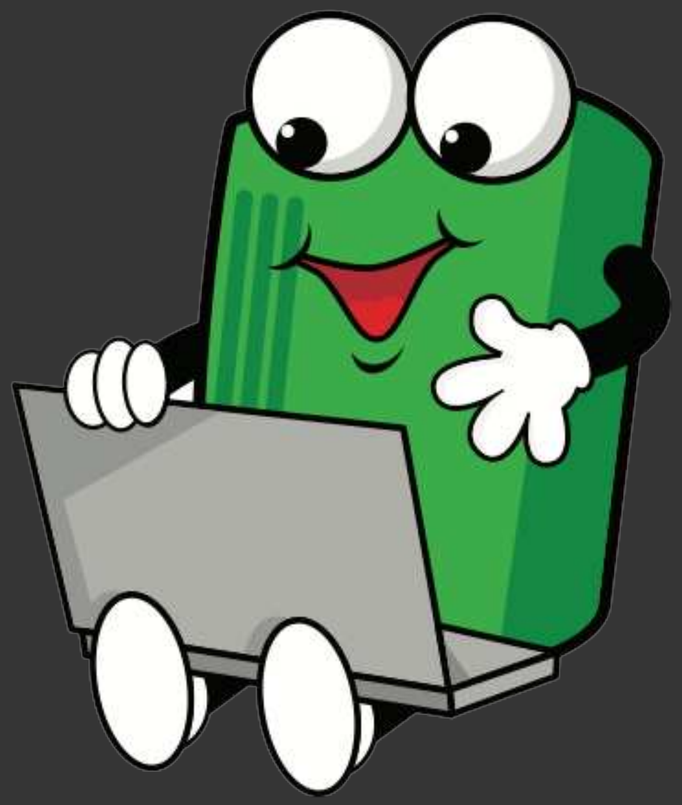
@superlilia
@mattstratton

Practice exercise

- Every group will get a bunch of LEGO and a picture of the outcome
- You will have a certain amount of time to try to work as a team to assemble your kit
- After the time runs out, you will work together to fill out a postmortem report on the activity
- You will then hold a postmortem meeting with the entire workshop

@superlilia
@mattstratton

Pagey says thank you



@superlilia
@mattstratton