

Incident Response at Slack

Colm Doyle
Developer Relations Lead, EMEA

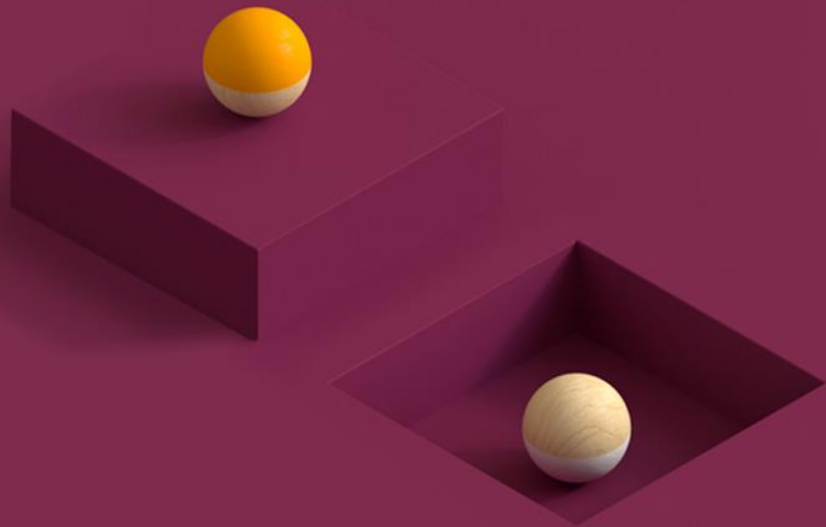


When everything is on fire - how not to panic

Colm Doyle
Developer Relations Lead, EMEA



The one minute history of Slack



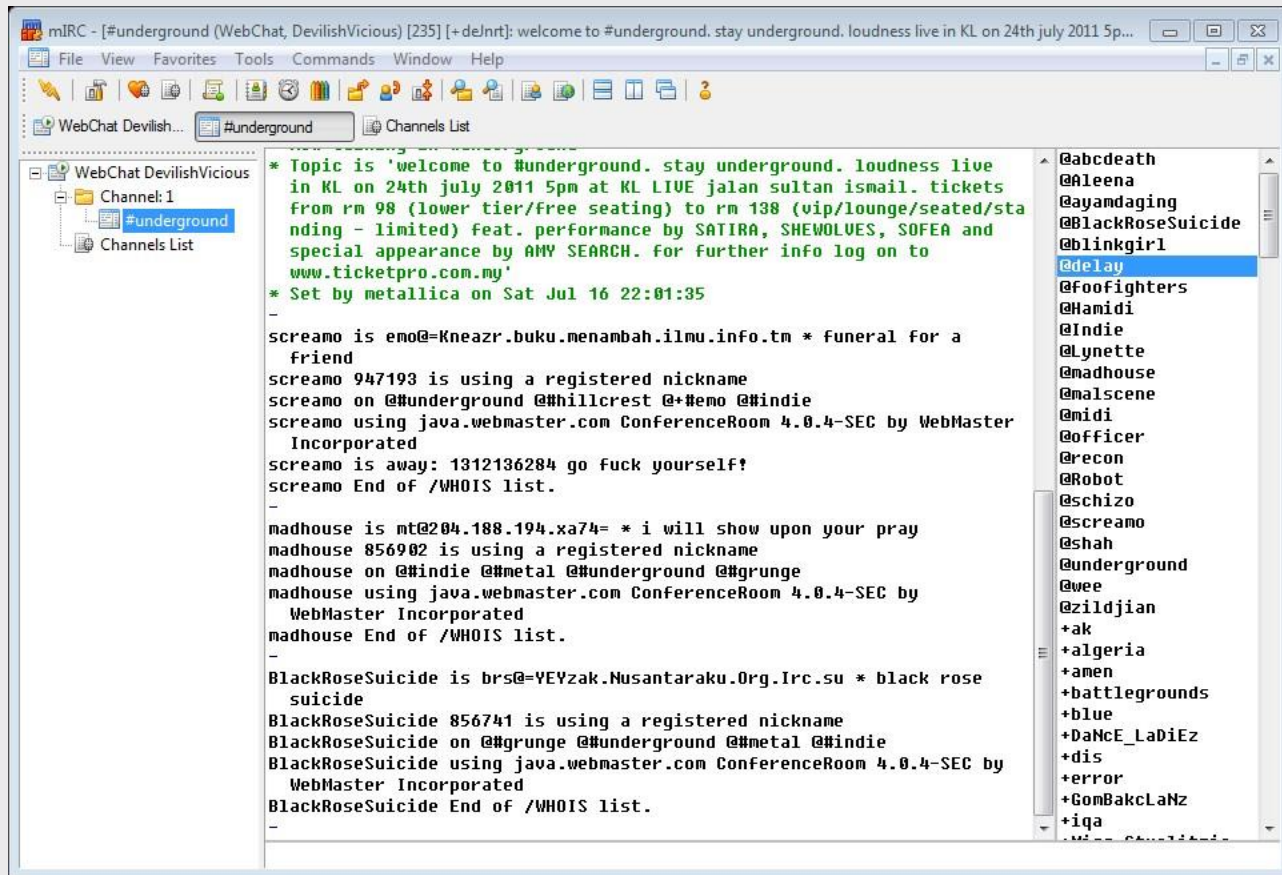


169
Quadrants



Inventory

Furniture



alirayl_test1

★

#general

Search

+

3 members

YOUR CHANNELS

#general

#random

+4 more...

DIRECT MESSAGES

slackbot

More...

~ FIN ~

Recent Activity

Today

1 person joined the team:

alirayl_test1

More...

Monday April 8th, 2013

3:08 PM

alirayl

i like to talk

3:08 PM

to myself

3:08 PM

like i do

3:08 PM

hey

3:09 PM

we remove extra spaces between words

3:09 PM

i wonder if we want to do that

Tuesday April 9th, 2013

+ File + Post

Activity

Files

Posts

Team

all on DEV

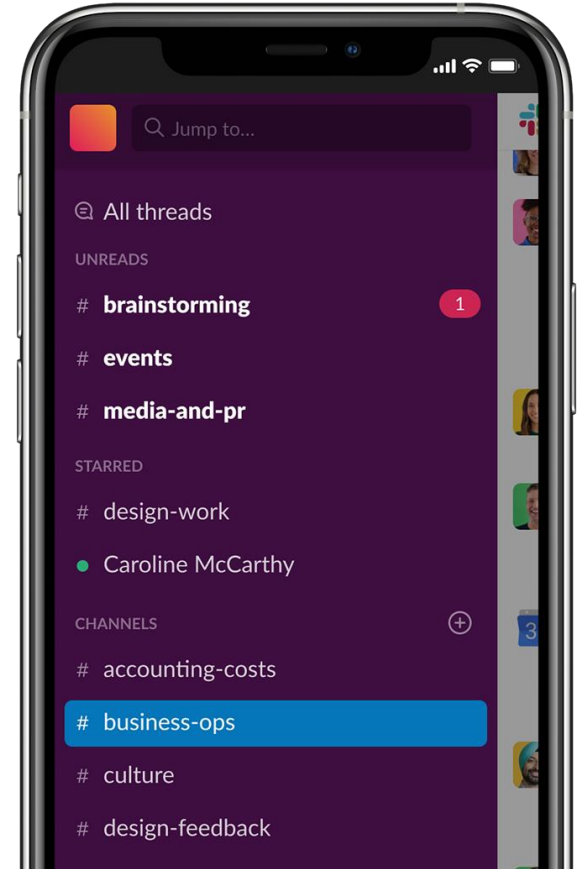
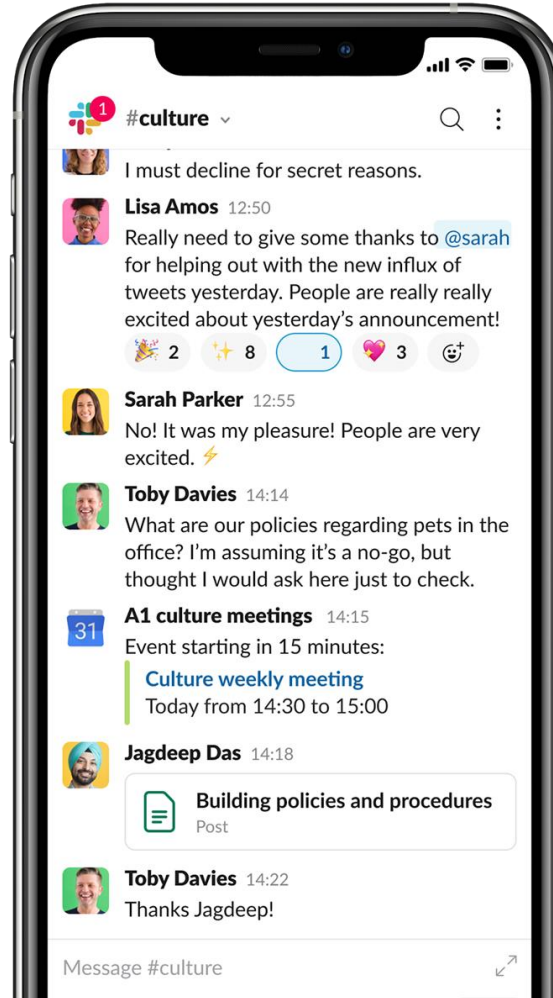
SLACK HISTORY

Slack now

Persistent chat

Integrations

User experience



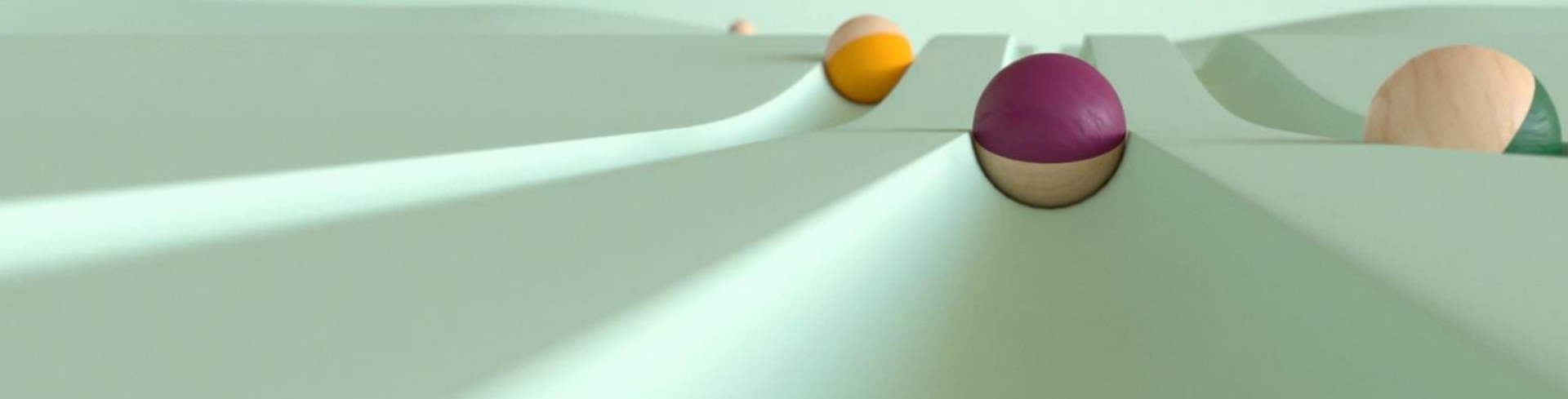
Slack now

10m DAU

1b messages/week

2000+ integrations

Why does incident response matter?



Incidents happen to ***everyone***

Incident response at Slack

The cost of incidents

\$100M

Amazon loss per hour on prime day

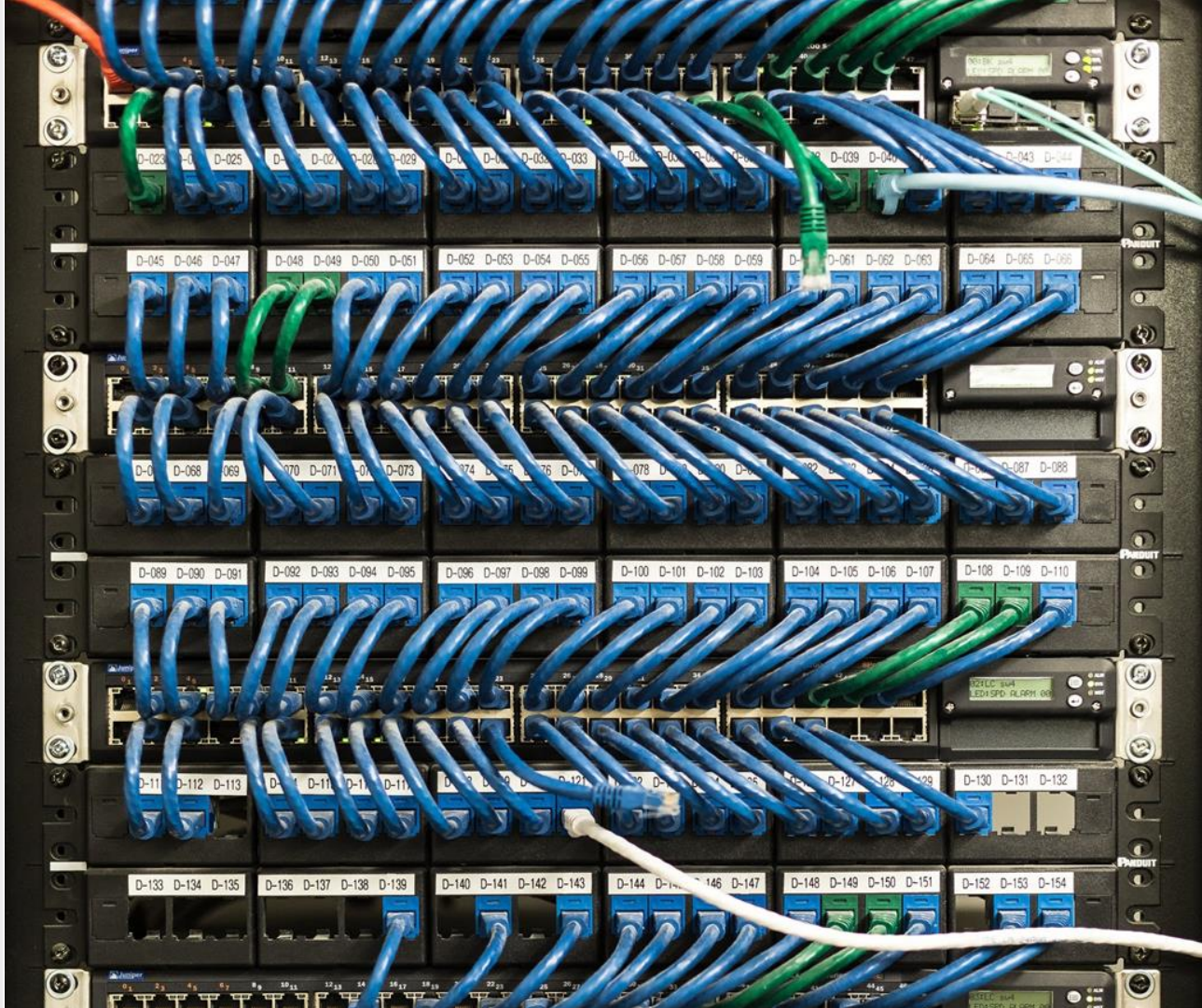
\$6.3M

Facebook losses per hour

\$150M

Delta Airlines cost for five hours of downtime

An organised approach to addressing and managing an incident



WHY INCIDENT RESPONSE

Allows your team to focus on resolving the incident, not the drama of it *being* an incident



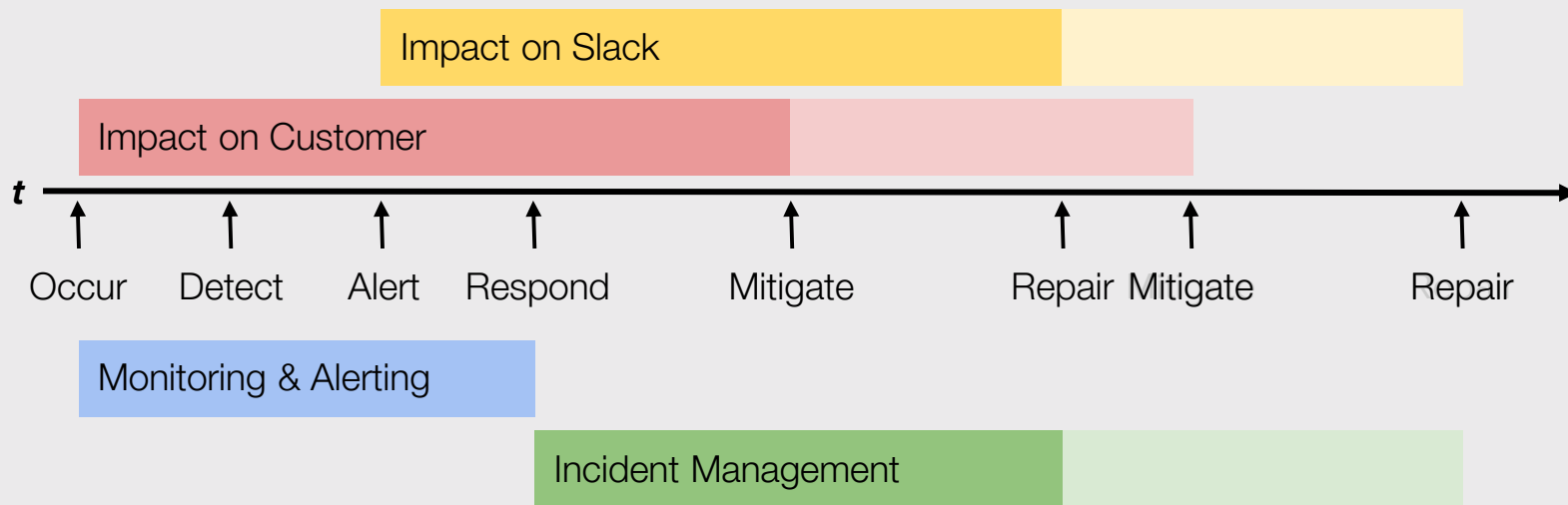
Incident response at Slack

How Slack does it

A photograph of a fire station with two red fire trucks parked inside. The text is overlaid on the image.

Based on the **Incident
Command System**,
originally designed for
California wildfire response

Incident Management Timeline



Severity Levels

S1

Critical

Critical system issue that warrants our most extreme response.

S2

High

Critical system issue actively impacting many customers' ability to use the product.

S3

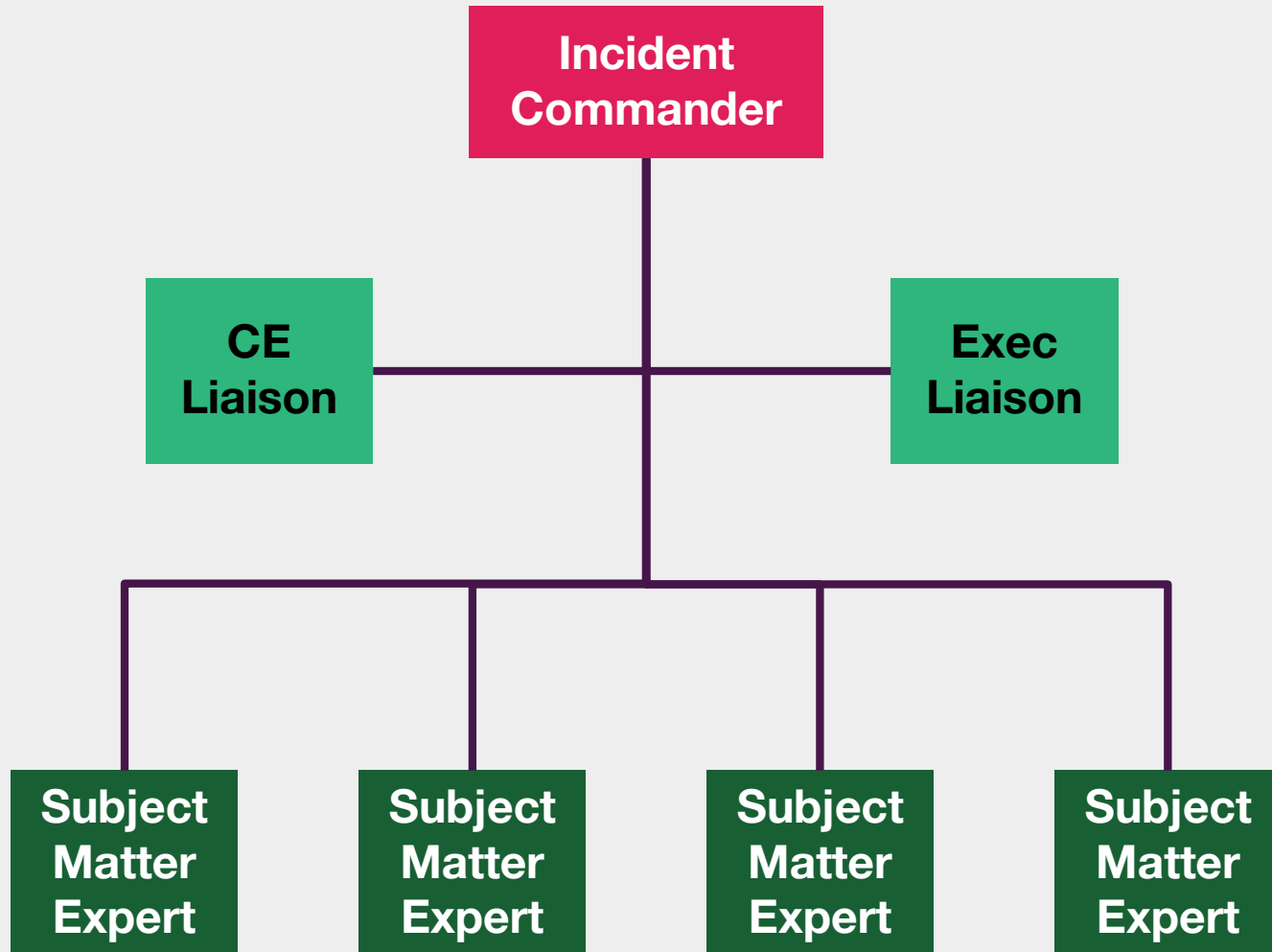
Medium

Stability or minor customer-impacting issues that require prompt attention from service owners during normal business hours.

S4

Low

Minor issues requiring action, but not affecting customer ability to use the product.

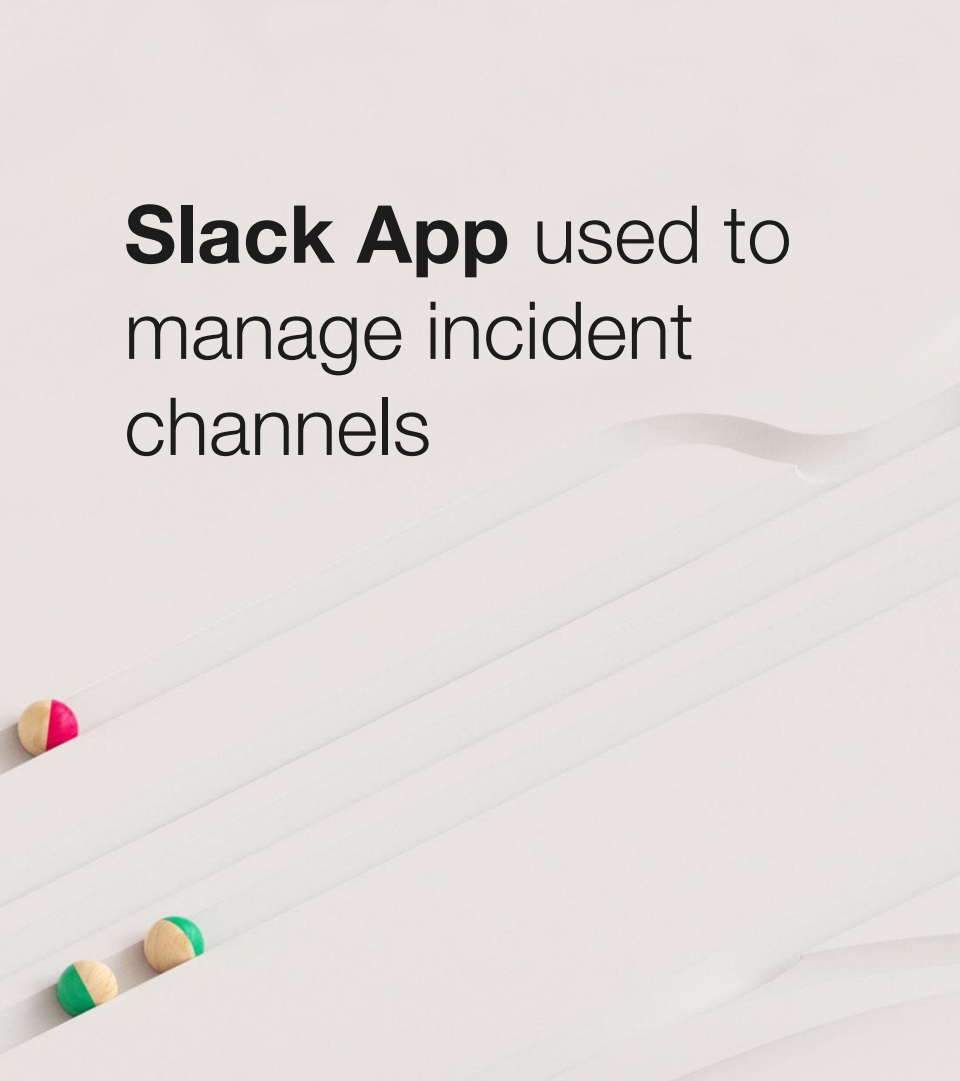


Separate channel for each incident

Naming Convention: #incd-YYMMDD-NNN-words

Ex: #incd-190328-459-frankfurt-down

- Makes easy to find channels via Quick Switcher (Cmd-K)
- Full history of incident is in channel
 - Helps new responders come up to speed quickly, without interrupting
 - Makes the postmortem easier



Slack App used to manage incident channels

/incident-pde create

- Creates JIRA ticket for tracking, and to get incident number (INCD project in JIRA)
- Creates new incident channel
- Invites **@incident-next-followers** user group
- Posts a message with quick-reference links
- Sets channel topic to reflect IC, Severity

/incident-pde convert

- All the same, but renames **current** channel rather than creating a new one

Other sub-commands to manage incident Severity Level, IC, status (active, paused, under control, all clear, etc.)



Standby channel kept ready for each incident

- **#incident-next**
- Captures “What are we seeing? Is this an incident?” preliminary discussions
- Renamed according to naming convention at start of incident, and new standby **#incident-next** channel created
 - Cron job creates **#incident-next** channel, if it doesn’t exist; runs every 5 minutes
 - **@incident-next-followers** user group invited to new channel
- First post is collection of quick-ref links



Additional channels for **complex responses**

- Ex: exec channel for policy discussion
- Ex: private channel for confidential data
- Messages shared between channels as needed to stay in sync
- Named using same naming convention as main channel

Long-lived channels for status updates

- **/incident-pde** bot reports newly-created/converted channels to **#incidents**
- Separate cronjob reports to **#every-incident** any new channel it discovers named **#incident-next** or **#incd-anything**
- Postmortems dates/docs shared to **#announce-postmortems** via reacji channeler

Other practices

Channel topic tells current state of incident:
Severity Level (Sev-1 through Sev-4),
status (active, on hold, under control, all clear),
IC, one-sentence description.

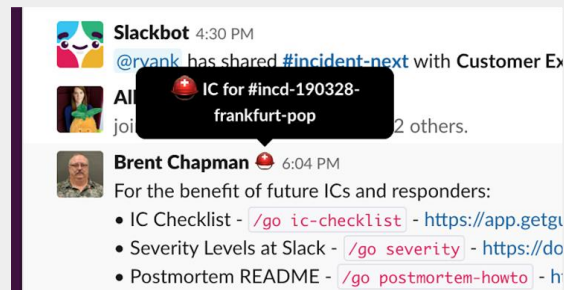
Ex: **S3** Sev-3 active 🚒 IC @brent |
Frankfurt pop outage

Pinned posts for periodic status/plans updates:
Responders joining incident channels know to
read those first, for a quick overview of incident

Threads for deep dives into particular topics

- Folks can ignore unless relevant to them
- Convention that decisions and key findings are shared back to main channel

Emojis to indicate various things, by convention



- 🙄 :eyes: to mean “I’m looking at this”
- ✅ :checkmark: to mean “This is done”
- 📧 :postbox: for postmortem follow-up
- ● Others to indicate agreement, doubt, etc.

This is just **one** approach

Automate the things



Incident management at Slack

Workflow Builder

Use Slack native functionality for simple incident response

Workflow overview



Actions menu

Starts when someone selects Report an Incident from the actions menu in #help-incidents

Edit



Collect form responses

Creates and sends a form with up to 10 questions

Edit

Help Desk Request

📄 Summary of your request

📄 Request category

📄 Urgency of your request

📄 Anything else we should know



Send a message

Sends a message to #team-incidents

Edit



Incident Manager WORKFLOW

! Incident Report

Urgency: Example text

👤 Incident Type:

Example text

👤 Submitted by:

@Example User

🗨️ Summary of Incident:

Example text

📄 Other Details:

Example text

Next Steps:


Please discuss in-thread & determine appropriate next step. The point person should **Claim for review** and follow up with @Example User directly.

Claim for review

Incident management at Slack

Workflow Builder

Use Slack native functionality for simple incident response

**Report an Incident**×

Incident Type

Security

Incident Summary

Stolen Laptop

Urgency of your request

Choose an option...

Choose an option...

< 48 hours

< 24 hours

< 1 hour

[? Learn more about Incident Manager](#)

Cancel

Submit

Incident management at Slack

Workflow Builder

Use Slack native functionality for simple incident response



Incident Manager APP 4:05 PM

INCIDENT REPORT - @Harry Boone

Incident Type:

Security

Incident Summary:

Stolen Laptop

Urgency of the request:

● < 24hours

Thank you for taking time to report this incident. The team in [#help-incident](#) will review and direct message you with next steps.

Incident management at Slack

Monzo

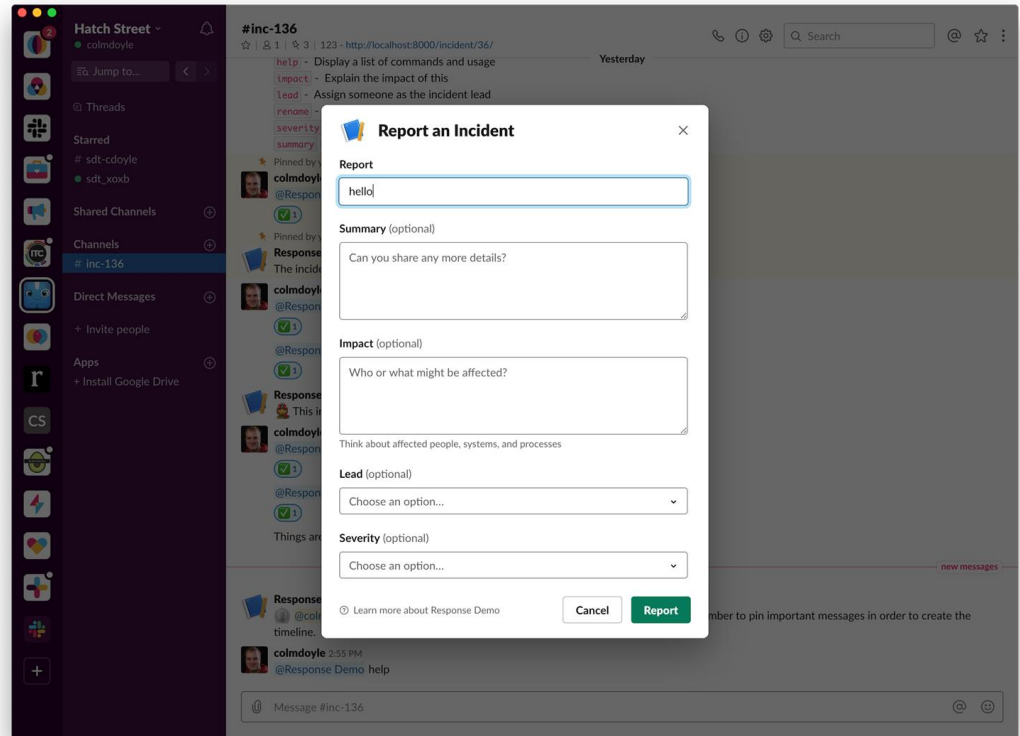
**Digital bank
founded in 2015**



Incident management at Slack

Response

Rich summary
messages, with a
common format



Incident management at Slack

Response

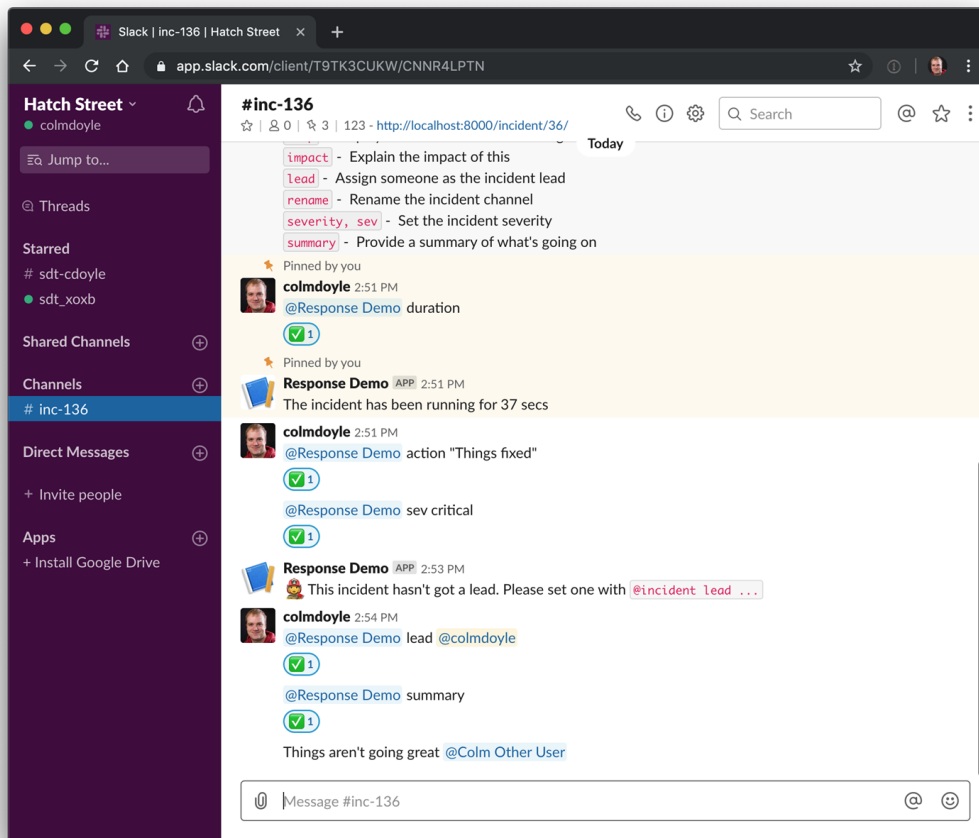
Rich summary
messages, with a
common format



A screenshot of a Slack web interface. The left sidebar shows the user 'colmdoyle' in the 'Hatch Street' workspace, with a list of channels including '# response-incidents'. The main area displays the '# response-incidents' channel. At the top, there are 'Edit' and 'Close' buttons. The channel content shows a message from 'colmdoyle' with a rich summary of incident details: 'things', 'Reporter: @colmdoyle', 'Incident Lead: @Colm Other User', 'Status: Resolved', 'Severity: Major', 'Document: Incident 35', and 'Comms Channel: #inc-135'. Below this is a 'Response Demo' message from 'colmdoyle' with a similar summary: 'Reporter: @colmdoyle', 'Incident Lead: @colmdoyle', 'Status: Live', 'Severity: Critical', 'Document: Incident 36', and 'Comms Channel: #inc-136'. At the bottom of the demo message, it says 'Need something else?' with 'Edit' and 'Close' buttons. The bottom of the screen shows a message input field with a placeholder 'Message #response-incidents' and '@' and emoji icons.

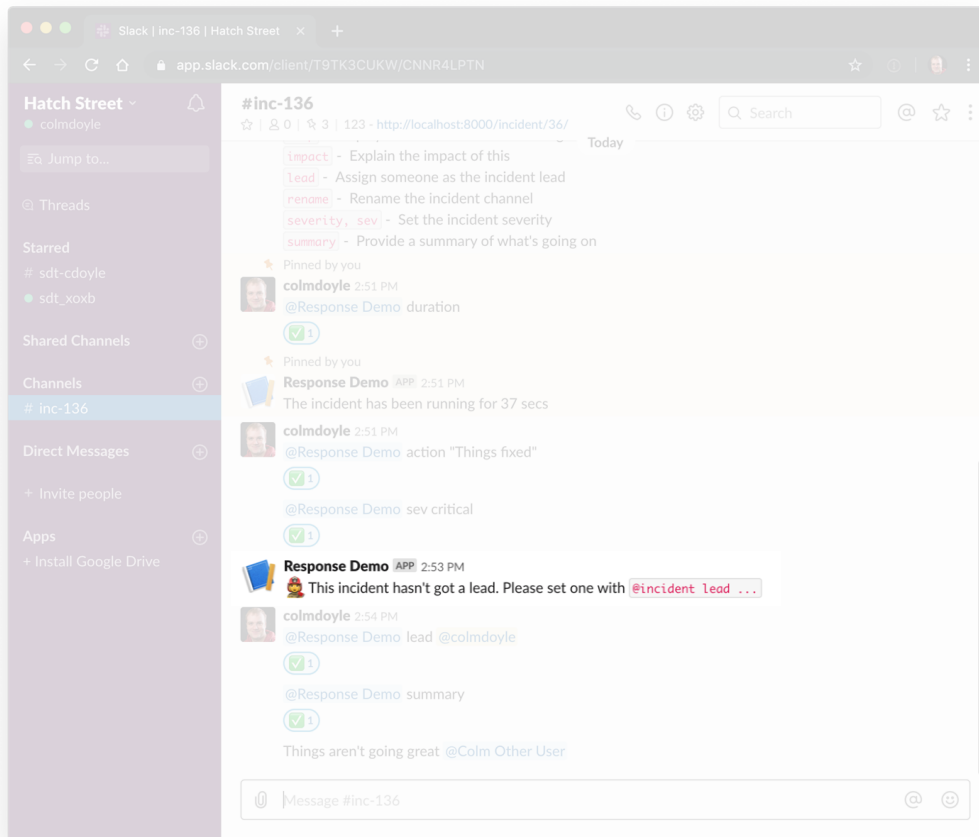
Response

A more ChatOps
style of interaction
with a bot user



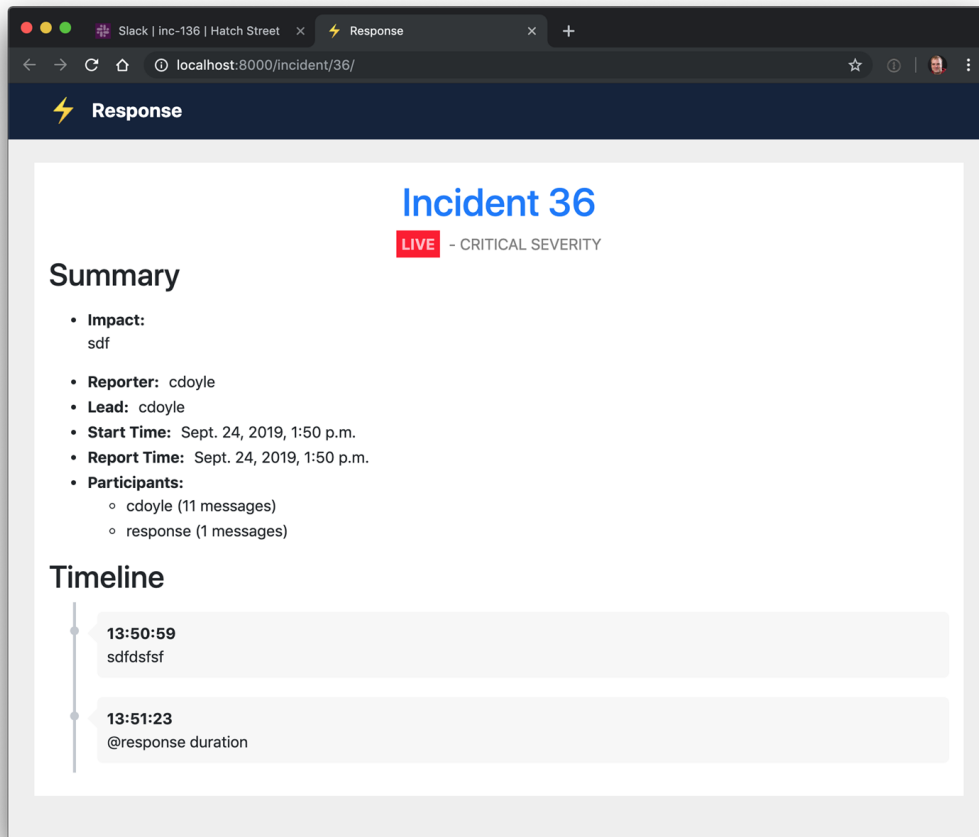
Response

**Nudges by the bot
to ensure important
information is
reported**



Response

Near automated
incident reports to
help with learning

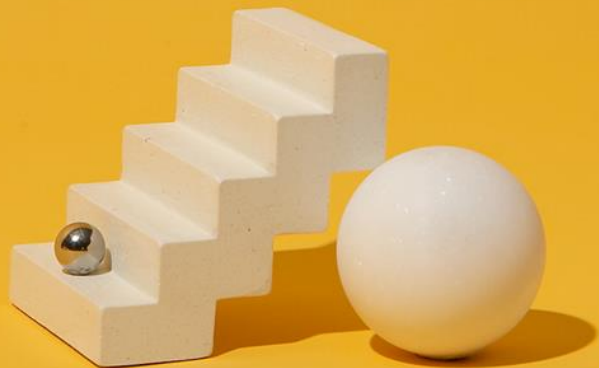
A screenshot of a web browser showing the Slack Response interface for Incident 36. The browser's address bar shows 'localhost:8000/incident/36/'. The interface has a dark blue header with a lightning bolt icon and the word 'Response'. The main content area is white and contains the following information:

- Incident 36** in blue text, with a red 'LIVE' badge and '- CRITICAL SEVERITY' below it.
- Summary** section with a bulleted list:
 - Impact:** sdf
 - Reporter:** cdoyle
 - Lead:** cdoyle
 - Start Time:** Sept. 24, 2019, 1:50 p.m.
 - Report Time:** Sept. 24, 2019, 1:50 p.m.
 - Participants:**
 - cdoyle (11 messages)
 - response (1 messages)
- Timeline** section with a vertical line and two entries:
 - 13:50:59**: sdfdsfsf
 - 13:51:23**: @response duration

This is just **one** example

Incident response at Slack

Learn more...





<https://response.pagerduty.com>

Some resources

- <https://api.slack.com>
- <https://slack.com/intl/en-ie/slack-tips/collect-incident-reports-in-real-time>
- <https://github.com/monzo/response>
- <https://github.com/Netflix/dispatch>

Q&A

