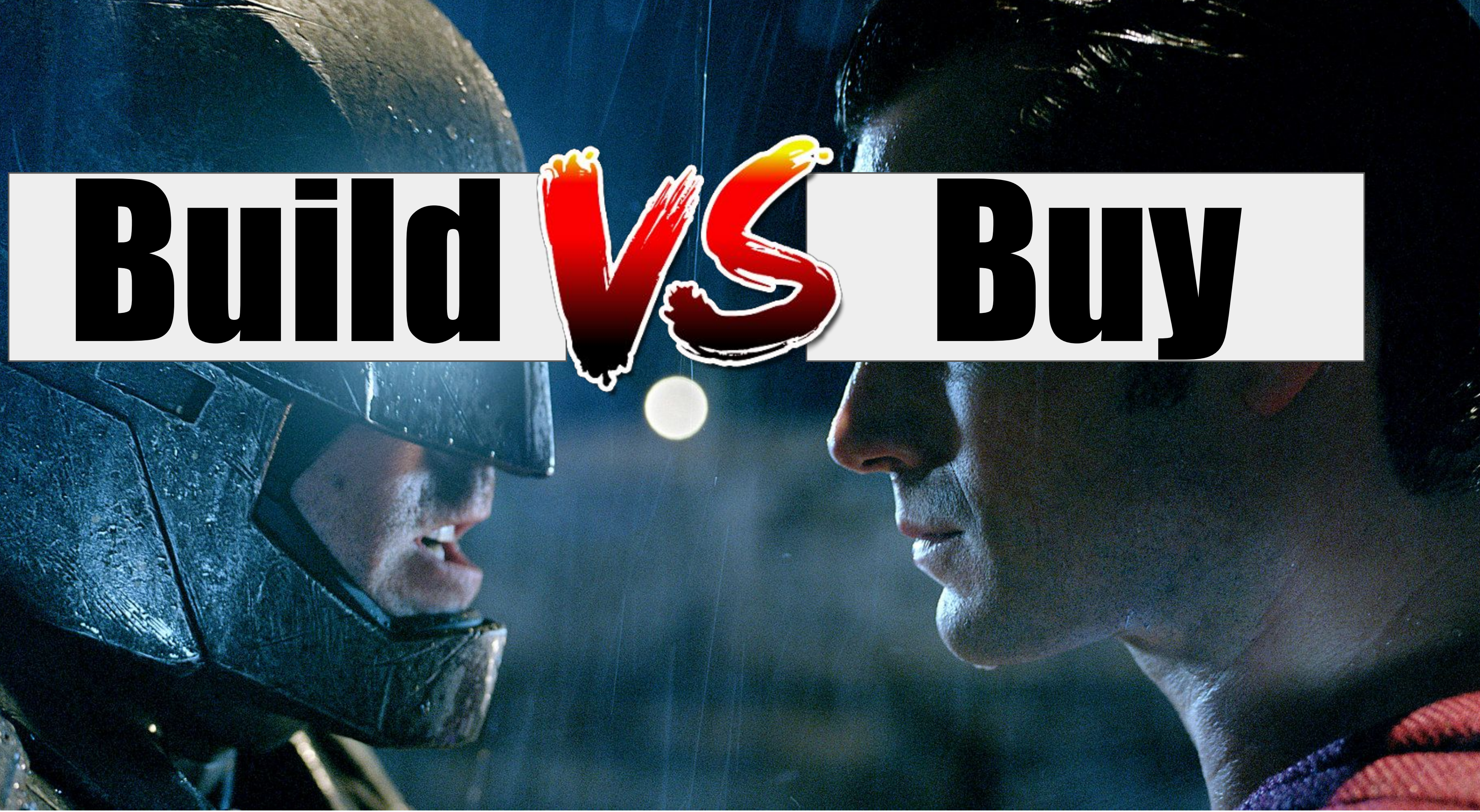
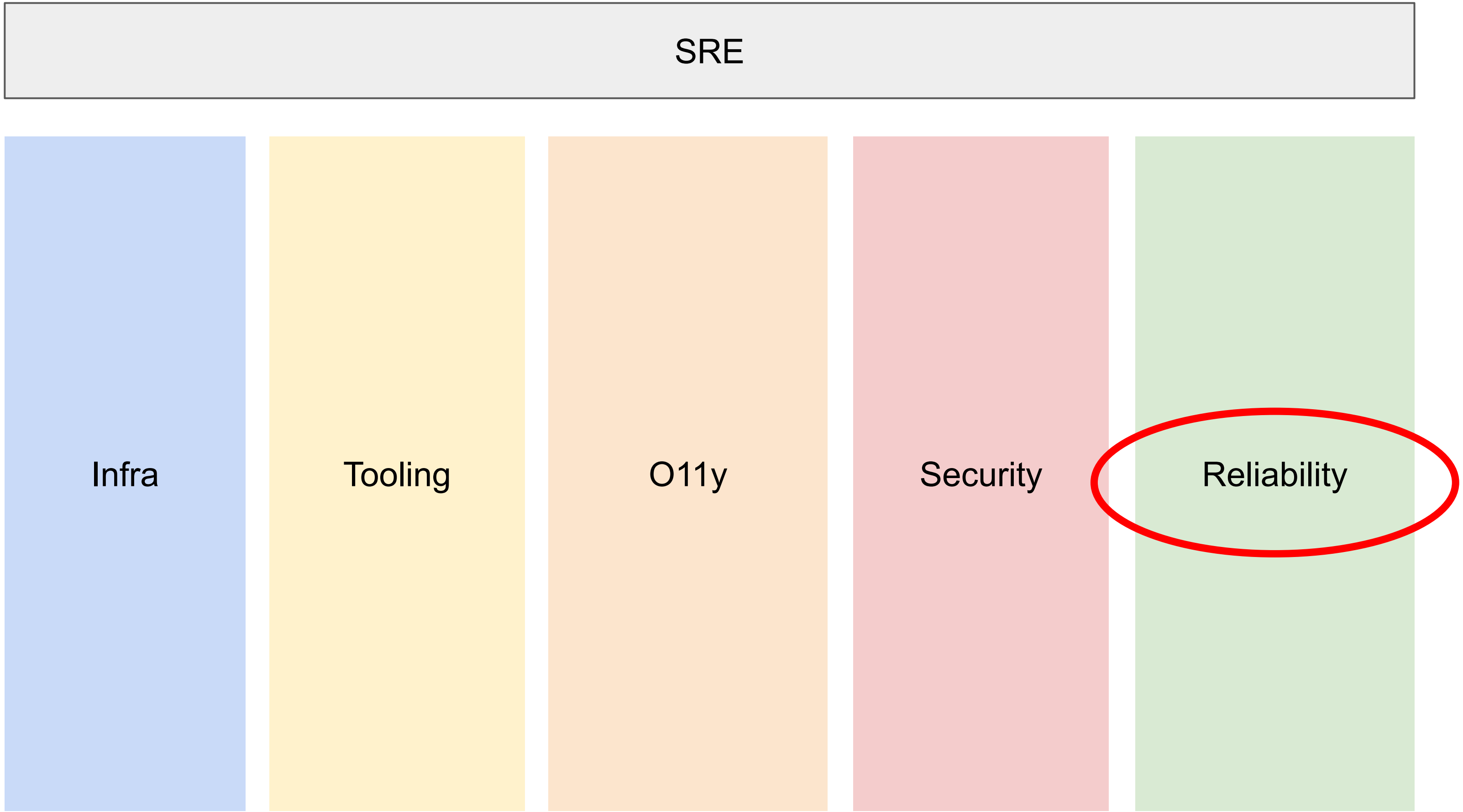
Build VS Buy



Reginald Davis, Sr. SRE, Elastic

- SRE Resilience
- YouTube: @otherpeoplescomputer
- Twitter/X: @coolblknerd

2021



SRE

Infra

Tooling

O11y

Security

Reliability

H

Reliability Team

Services/Tools with obvious value

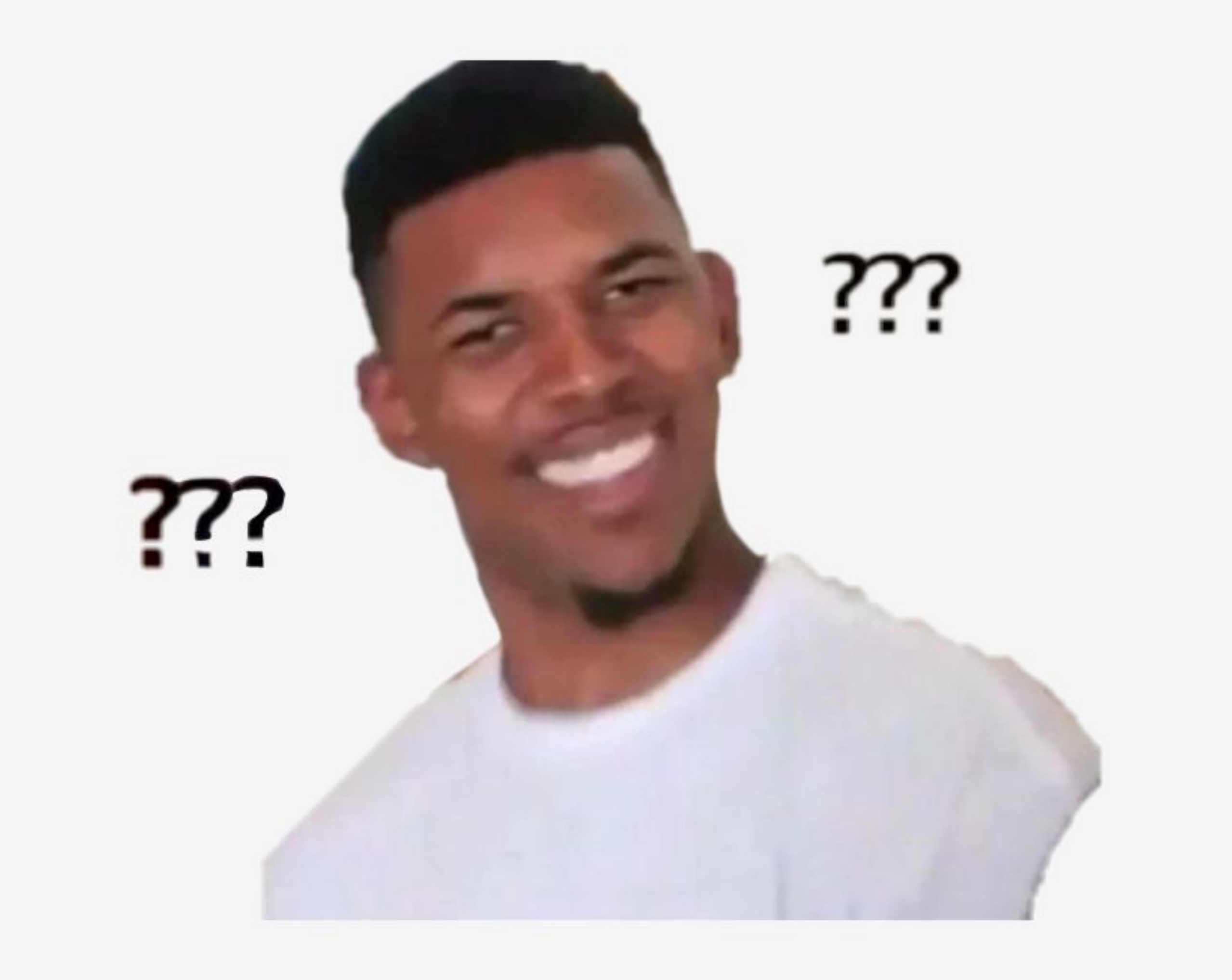
Interesting services/tools

Problem Management

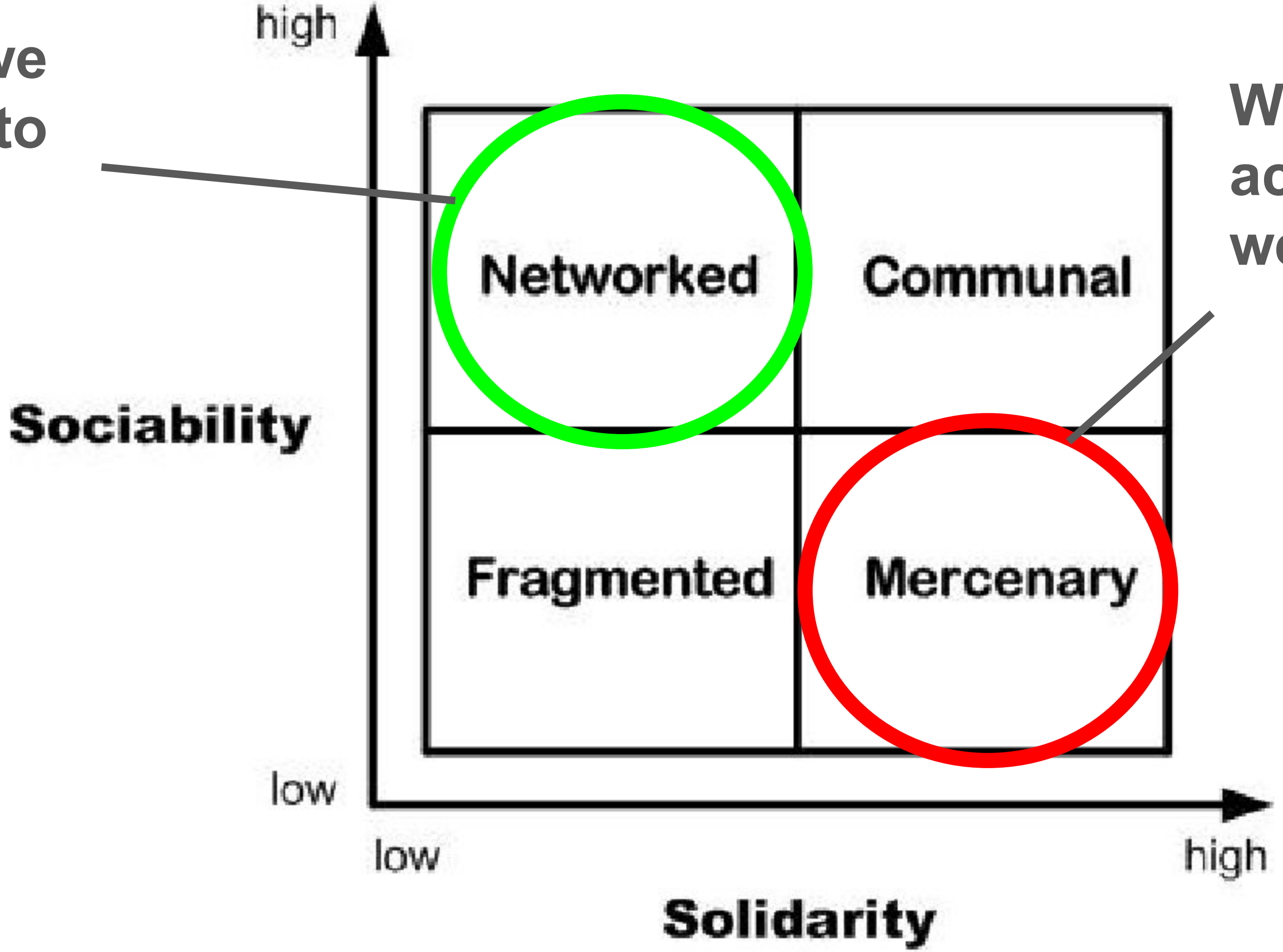
Incident Management

Alerting

Postmortems/RCAs



Where we wanted to be…



high

Networked

Communal

Sociability

Fragmented

Mercenary

low

low

high

Solidarity

Where we actually were

EXIT

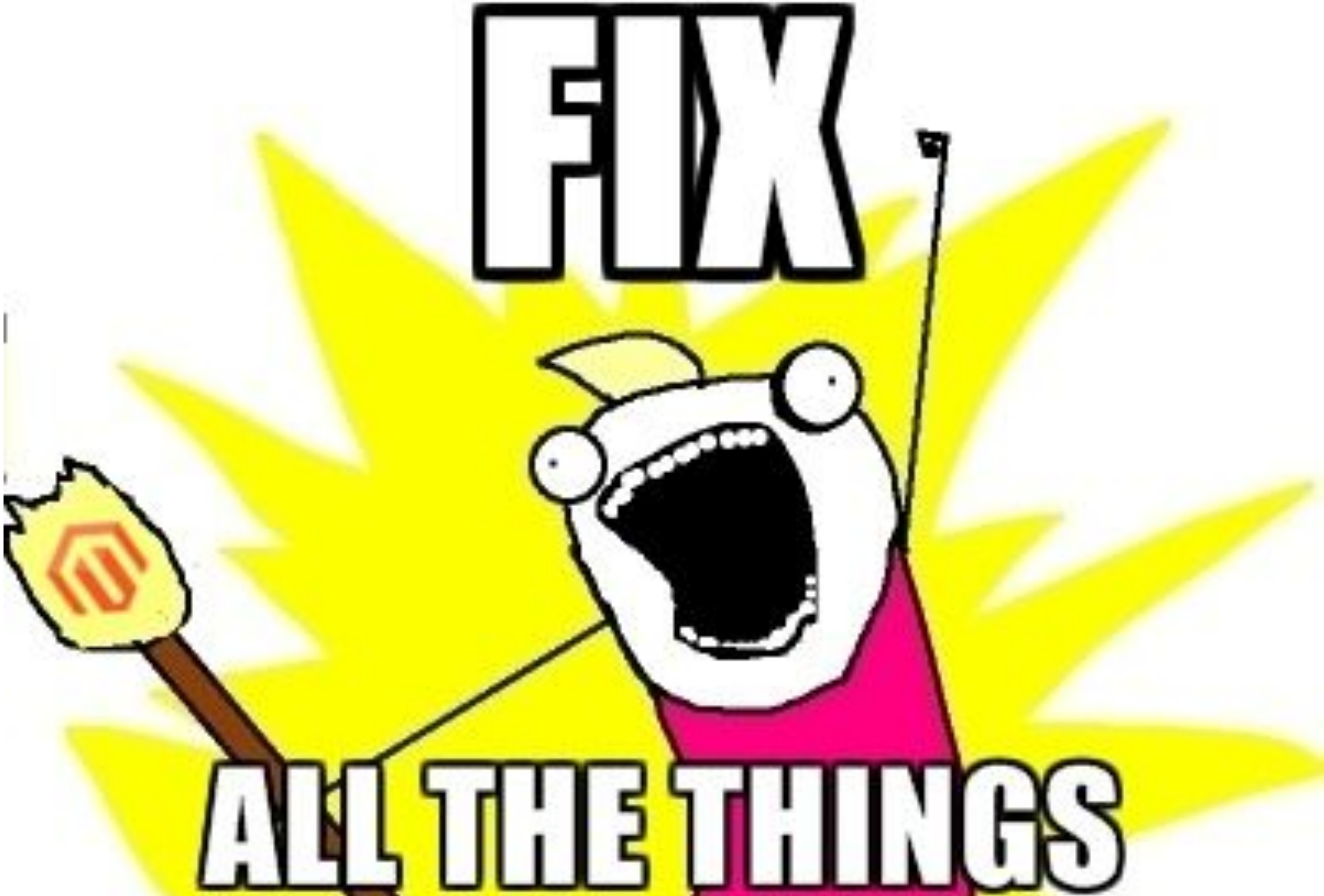
Dealing with the leftovers…

5:00 DEADLINE!
IMAGE SOURCE ROYALTY FREE
IMAGE SOURCE ROYALTY FREE

How many Incidents did we have this week?

How can we read the RCA’s?

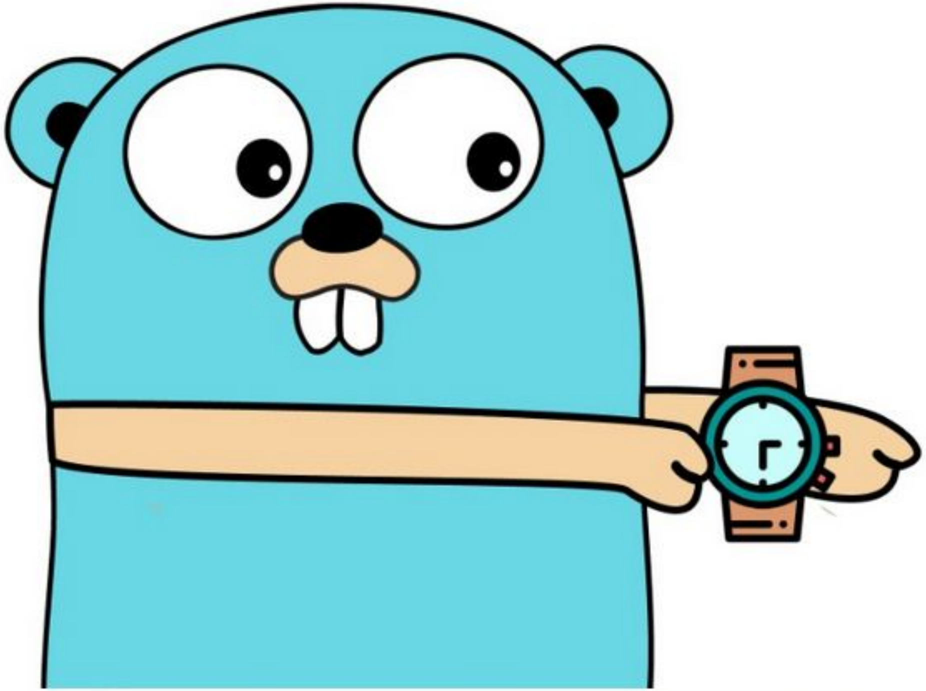
WTF is going on?

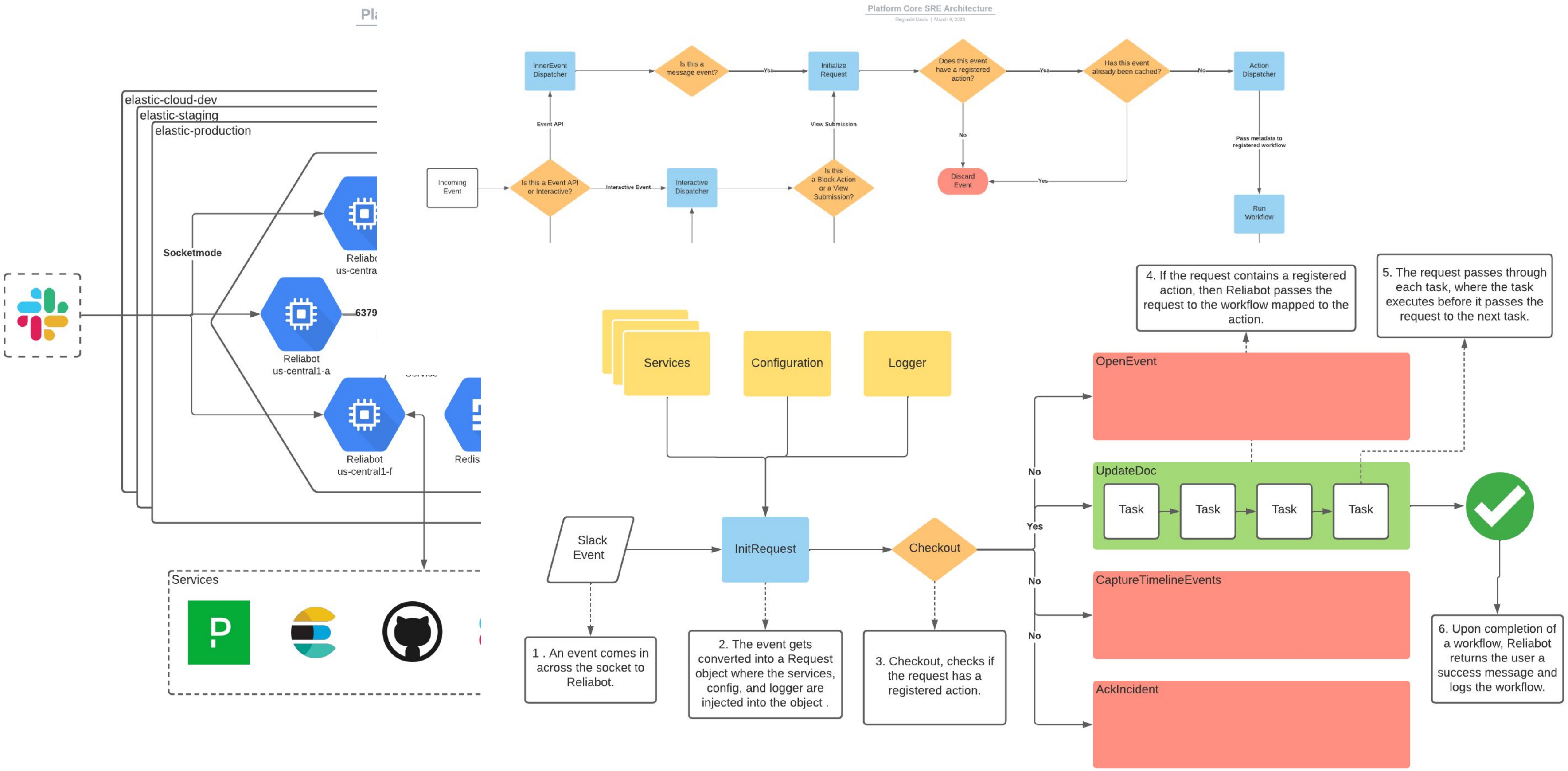

FIX
ALL THE THINGS

How the “Building” Went Wrong

2022

It’s Go Time





1 . An event comes in across the socket to Reliabot.

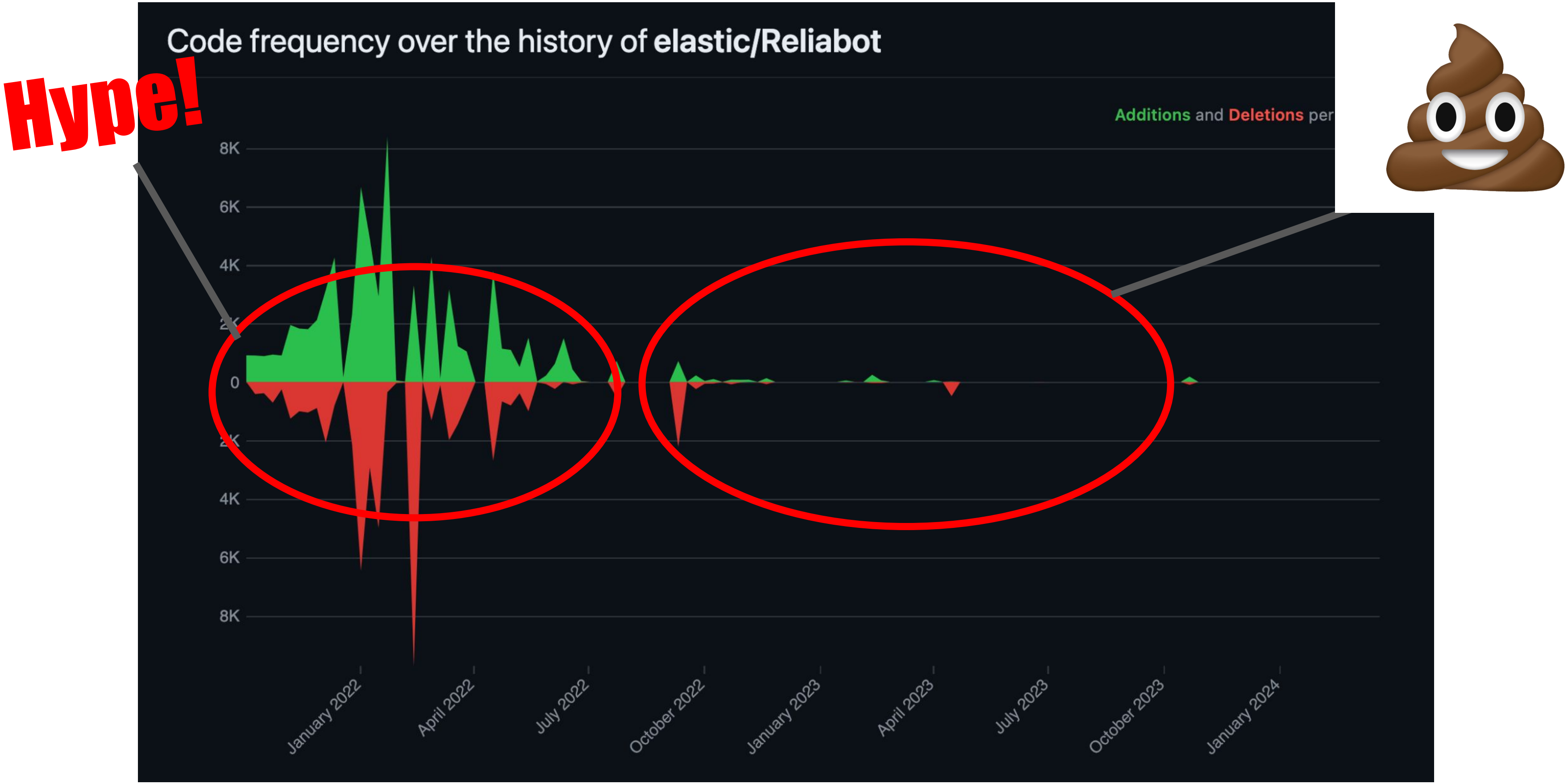
2. The event gets converted into a Request object where the services, config, and logger are injected into the object .

3. Checkout, checks if the request has a registered action.

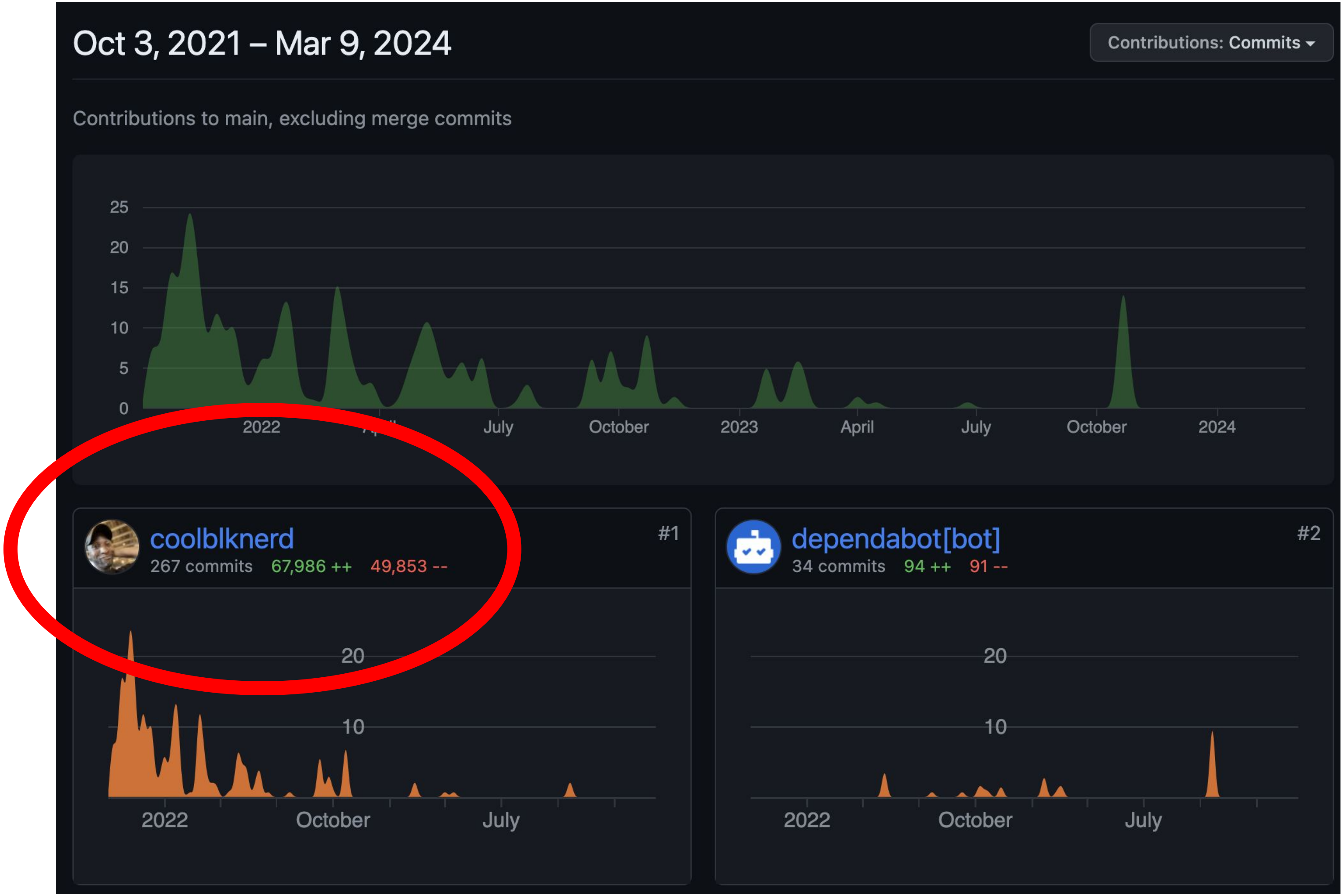
4. If the request contains a registered action, then Reliabot passes the request to the workflow mapped to the action.

5. The request passes through each task, where the task executes before it passes the request to the next task.

6. Upon completion of a workflow, Reliabot returns the user a success message and logs the workflow.



Hype!
Code frequency over the history of elastic/Reliabot
Additions and Deletions per
8K
6K
4K
2K
0
2K
4K
6K
8K
January 2022
April 2022
July 2022
October 2022
January 2023
April 2023
July 2023
October 2023
January 2024



Oct 3, 2021 – Mar 9, 2024

Contributions: Commits

Contributions to main, excluding merge commits

coolblknerd #1

267 commits 67,986 ++ 49,853 --

dependabot[bot] #2

34 commits 94 ++ 91 --

What we built...

What we missed...

	New Problem	Old Problem
New Tool	**Slow**	**Moderate**
Old Tool	**Moderate**	**Fast**

The Pivot

THIS IS FINE

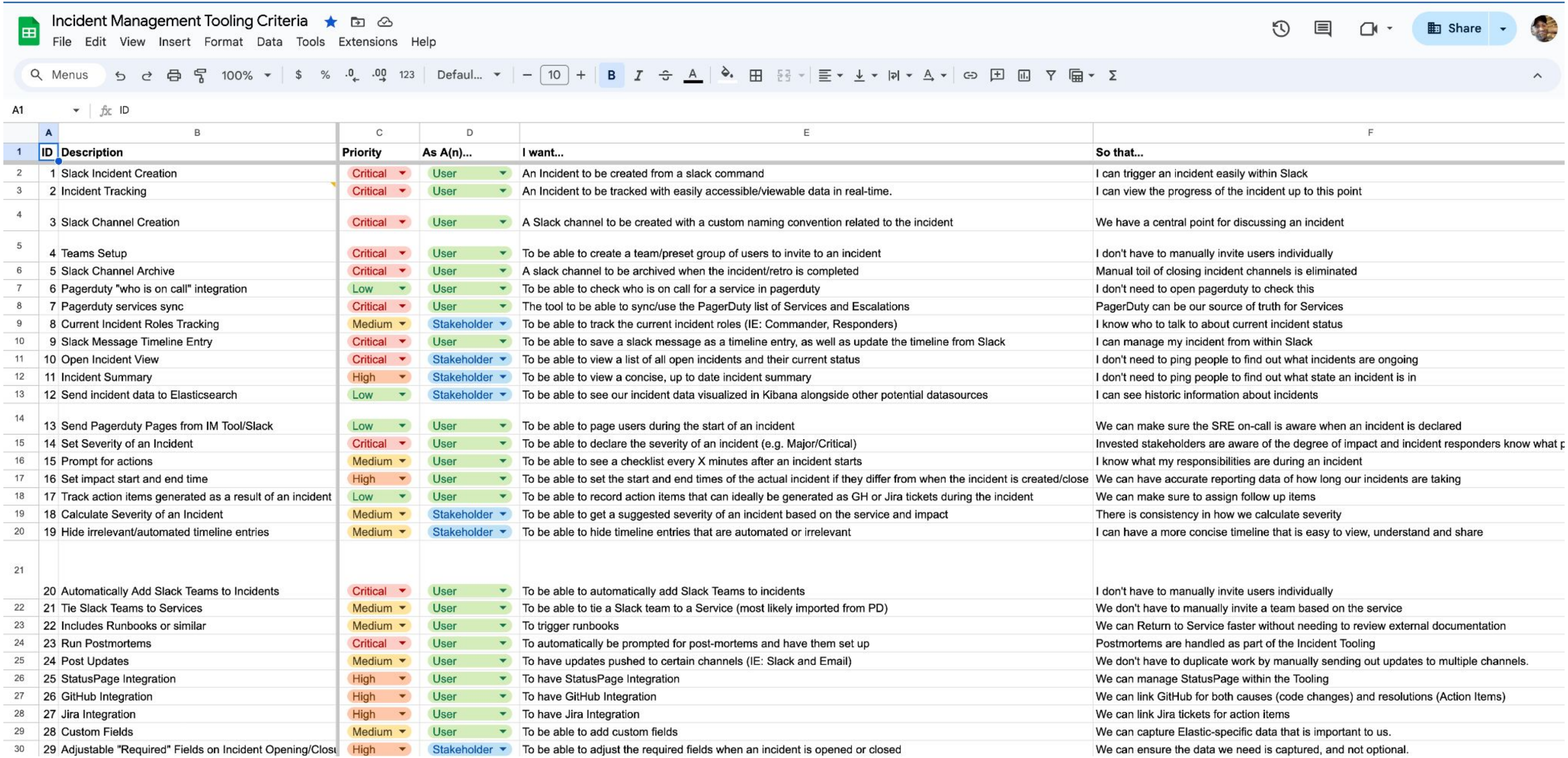
Google
Google Search
I'm Feeling Lucky

No one will be here In 5 years...

Leverage knowledge over skills

Deliver value to our stakeholders within a quarter

2023



Incident Management Tooling Criteria

	A	B	C	D	E	F
1	ID	Description	Priority	As A(n)...	I want...	So that...
2	1	Slack Incident Creation	Critical	User	An Incident to be created from a slack command	I can trigger an incident easily within Slack
3	2	Incident Tracking	Critical	User	An Incident to be tracked with easily accessible/viewable data in real-time.	I can view the progress of the incident up to this point
4	3	Slack Channel Creation	Critical	User	A Slack channel to be created with a custom naming convention related to the incident	We have a central point for discussing an incident
5	4	Teams Setup	Critical	User	To be able to create a team/preset group of users to invite to an incident	I don't have to manually invite users individually
6	5	Slack Channel Archive	Critical	User	A slack channel to be archived when the incident/retro is completed	Manual toil of closing incident channels is eliminated
7	6	Pagerduty "who is on call" integration	Low	User	To be able to check who is on call for a service in pagerduty	I don't need to open pagerduty to check this
8	7	Pagerduty services sync	Critical	User	The tool to be able to sync/use the PagerDuty list of Services and Escalations	PagerDuty can be our source of truth for Services
9	8	Current Incident Roles Tracking	Medium	Stakeholder	To be able to track the current incident roles (IE: Commander, Responders)	I know who to talk to about current incident status
10	9	Slack Message Timeline Entry	Critical	User	To be able to save a slack message as a timeline entry, as well as update the timeline from Slack	I can manage my incident from within Slack
11	10	Open Incident View	Critical	Stakeholder	To be able to view a list of all open incidents and their current status	I don't need to ping people to find out what incidents are ongoing
12	11	Incident Summary	High	Stakeholder	To be able to view a concise, up to date incident summary	I don't need to ping people to find out what state an incident is in
13	12	Send incident data to Elasticsearch	Low	Stakeholder	To be able to see our incident data visualized in Kibana alongside other potential datasources	I can see historic information about incidents
14	13	Send Pagerduty Pages from IM Tool/Slack	Low	User	To be able to page users during the start of an incident	We can make sure the SRE on-call is aware when an incident is declared
15	14	Set Severity of an Incident	Critical	User	To be able to declare the severity of an incident (e.g. Major/Critical)	Invested stakeholders are aware of the degree of impact and incident responders know what p
16	15	Prompt for actions	Medium	User	To be able to see a checklist every X minutes after an incident starts	I know what my responsibilities are during an incident
17	16	Set impact start and end time	High	User	To be able to set the start and end times of the actual incident if they differ from when the incident is created/close	We can have accurate reporting data of how long our incidents are taking
18	17	Track action items generated as a result of an incident	Low	User	To be able to record action items that can ideally be generated as GH or Jira tickets during the incident	We can make sure to assign follow up items
19	18	Calculate Severity of an Incident	Medium	Stakeholder	To be able to get a suggested severity of an incident based on the service and impact	There is consistency in how we calculate severity
20	19	Hide irrelevant/automated timeline entries	Medium	Stakeholder	To be able to hide timeline entries that are automated or irrelevant	I can have a more concise timeline that is easy to view, understand and share
21	20	Automatically Add Slack Teams to Incidents	Critical	User	To be able to automatically add Slack Teams to incidents	I don't have to manually invite users individually
22	21	Tie Slack Teams to Services	Medium	User	To be able to tie a Slack team to a Service (most likely imported from PD)	We don't have to manually invite a team based on the service
23	22	Includes Runbooks or similar	Medium	User	To trigger runbooks	We can Return to Service faster without needing to review external documentation
24	23	Run Postmortems	Critical	User	To automatically be prompted for post-mortems and have them set up	Postmortems are handled as part of the Incident Tooling
25	24	Post Updates	Medium	User	To have updates pushed to certain channels (IE: Slack and Email)	We don't have to duplicate work by manually sending out updates to multiple channels.
26	25	StatusPage Integration	High	User	To have StatusPage Integration	We can manage StatusPage within the Tooling
27	26	GitHub Integration	High	User	To have GitHub Integration	We can link GitHub for both causes (code changes) and resolutions (Action Items)
28	27	Jira Integration	High	User	To have Jira Integration	We can link Jira tickets for action items
29	28	Custom Fields	Medium	User	To be able to add custom fields	We can capture Elastic-specific data that is important to us.
30	29	Adjustable "Required" Fields on Incident Opening/Closi	High	Stakeholder	To be able to adjust the required fields when an incident is opened or closed	We can ensure the data we need is captured, and not optional.

rootly

Don’t reward the code, reward the solution

Understand what kind of road you’re paving.

Accept your reality before trying to build a new one

Thank you for your time!