

Automated Incident Management

Ajuna Kyaruzi

 Skeptical



What do I mean when I say AI

Generative AI

AI Ops

Machine Learning

ChatGPT

AI Assistant

LLMs

Deep Learning

Mid Journey

Generative AI

AI Ops

Machine Learning

ChatGPT

AI Assistant

LLMs

Deep Learning

Mid Journey

AI Ops

Artificial intelligence for IT operations, or AIOps, is the application of artificial intelligence (AI) capabilities—such as natural language processing and machine learning models—to automate, streamline and optimize IT service management and operational workflows.

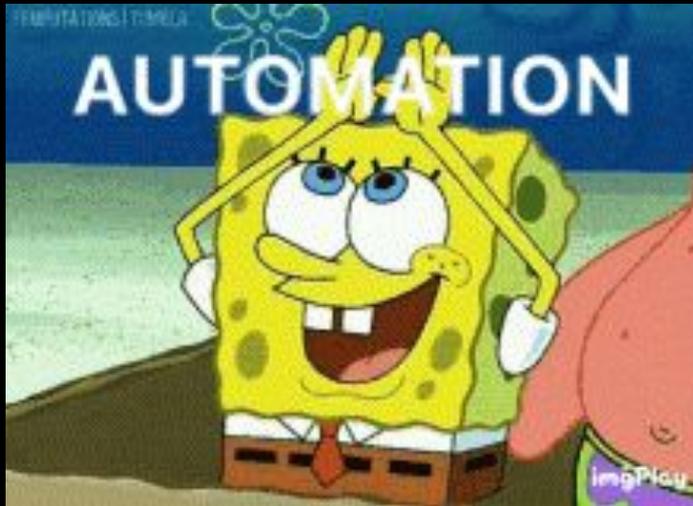
[IBM.COM/TOPICS/AIOPS](https://ibm.com/topics/aiops)



Is it a hammer?



What does

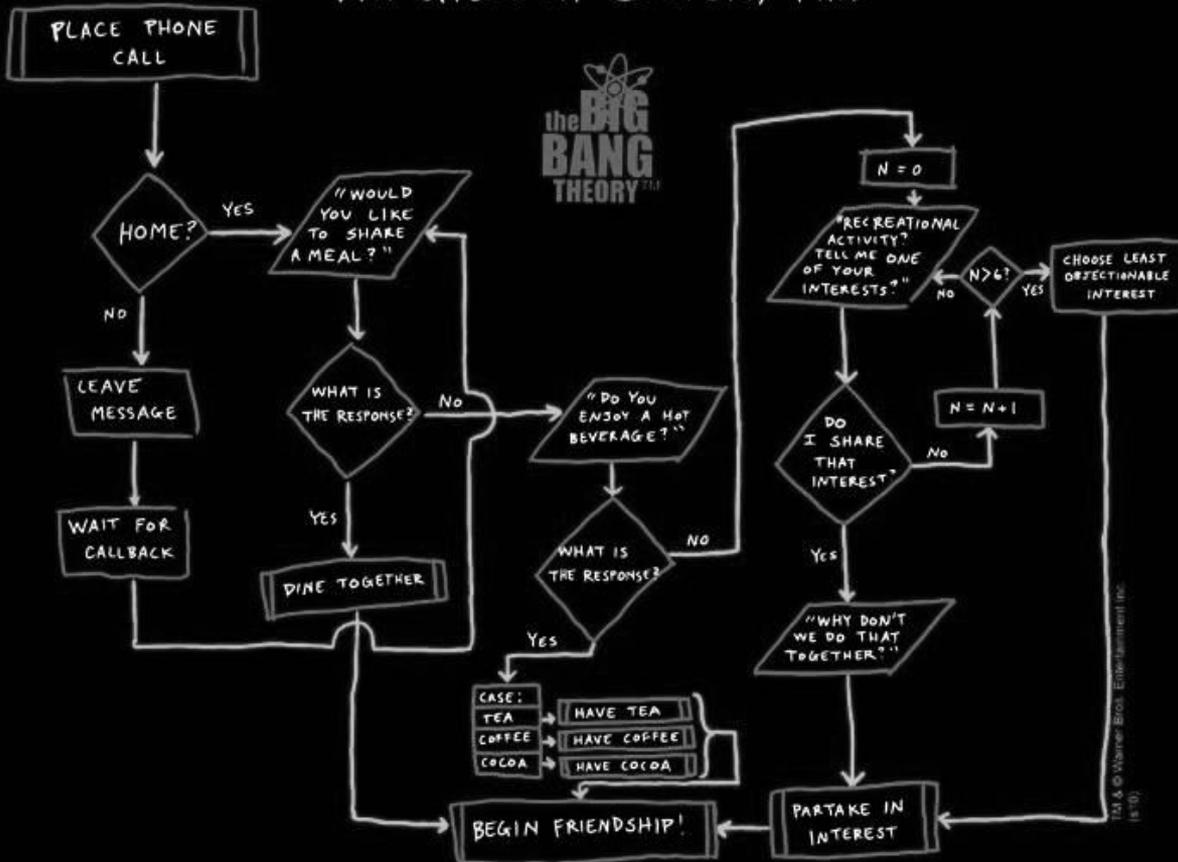


mean?



THE FRIENDSHIP ALGORITHM

DR. SHELDON COOPER, Ph.D



TM & © Warner Bros. Entertainment Inc. (s.10)

Incident Response Workflow



Detect



Declare



Manage



Document

Incident Response Workflow



Detect



Declare



Manage



Document

What are people using AI in
Organizations or even Incident
Management now doing?

Leveraging AI for efficient incident response

META

42% accuracy in identifying root causes for investigations at their creation time related to our web monorepo.

[ENGINEERING.FB.COM/2024/06/24/DATA-INFRASTRUCTURE/LEVERAGING-AI-FOR-EFFICIENT-INCIDENT-RESPONSE/](https://engineering.fb.com/2024/06/24/data-infrastructure/leveraging-ai-for-efficient-incident-response/)

👁 Only visible to you



Datadog APP 02:36

🌟🌟 **Here's a summary of the incident:**

Issue: Event-intake service experienced a spike to 100% error rate, possibly due to a suspected DDoS attack on API keys.

Impact: Customers may experience delays in events due to the spike in error rate.

Contributing Factors: Suspicion of a DDoS attack targeting API keys led to the identification of traffic from specific IPs.

Remediation: Actions taken included blocking the malicious IPs in Cloudflare, adding validations in HAProxy, and increasing the rate limit on the intake endpoint.

Here are some quick actions you can take on this incident. You can see all available actions anytime by typing '/datadog'

Incident Actions



Edit Incident



Edit Responders



View Web App



Page On-Call



Notify



Create CoScreen



Kai Xin Tai Jul 9th at 11:10

@Datadog Were there any recent incidents related to event-intake?

3 replies



Datadog APP Jul 9th at 11:10

Yes, there have been recent incidents related to the event-intake service:

Active Incidents:

- High error rate on event-intake service
- Potential DDOS attack on event-intake
- event-intake service spikes to 100% error

For more details, you can visit the [Incident Management page](#).



Kai Xin Tai Jul 9th at 11:11

@Datadog What was done to remediate the second incident?



Datadog APP Jul 9th at 11:11

To remediate the second incident (Potential DDOS attack on event-intake), the following actions were taken:

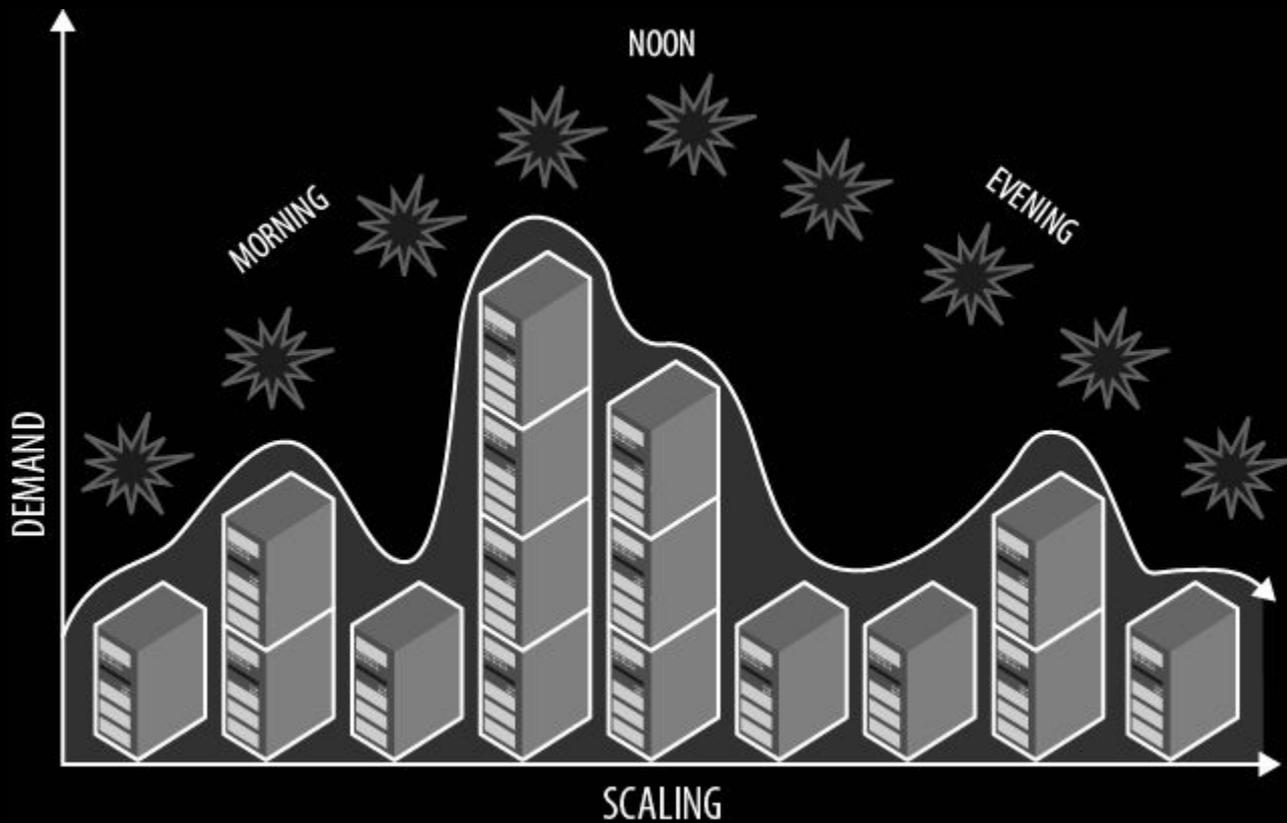
- Implemented specific filtering rules.
- Scaled up downstream services to mitigate impact.
- Reassessing load balancing strategy for future incidents.

For a more detailed overview, you can visit...
[See more](#)

Anomaly Monitor

Overview

Anomaly detection is an algorithmic feature that identifies when a metric is behaving differently than it has in the past, taking into account trends, seasonal day-of-week, and time-of-day patterns. It is suited for metrics with strong trends and recurring patterns that are hard to monitor with threshold-based alerting.



IMG: CH4, CLOUD ARCHITECTURE PATTERNS BY BILL WILDER, O'REILLY





“AI Assistant is at BEST
a junior engineer”



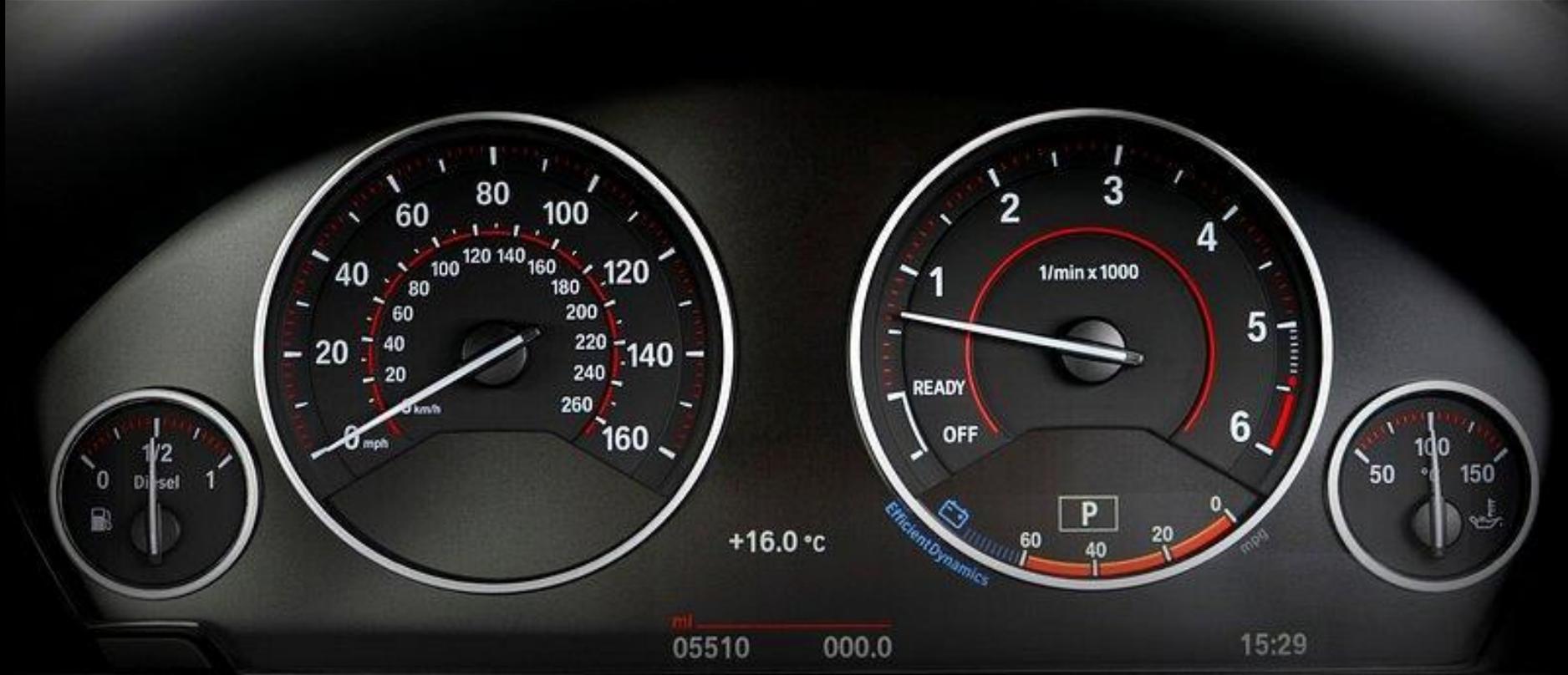
We aren't at Jarvis... yet

What does a junior engineer do?

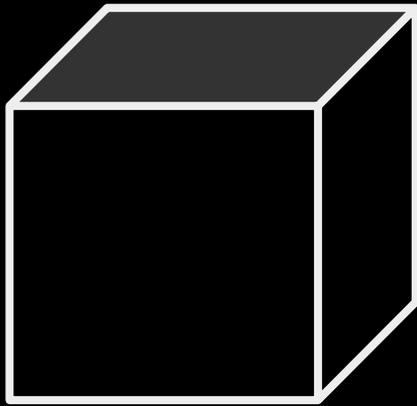
Duties may vary between engineering specialties due to their different focus. Many junior engineers complete common tasks regardless of their specialty. Common duties for junior engineers include:

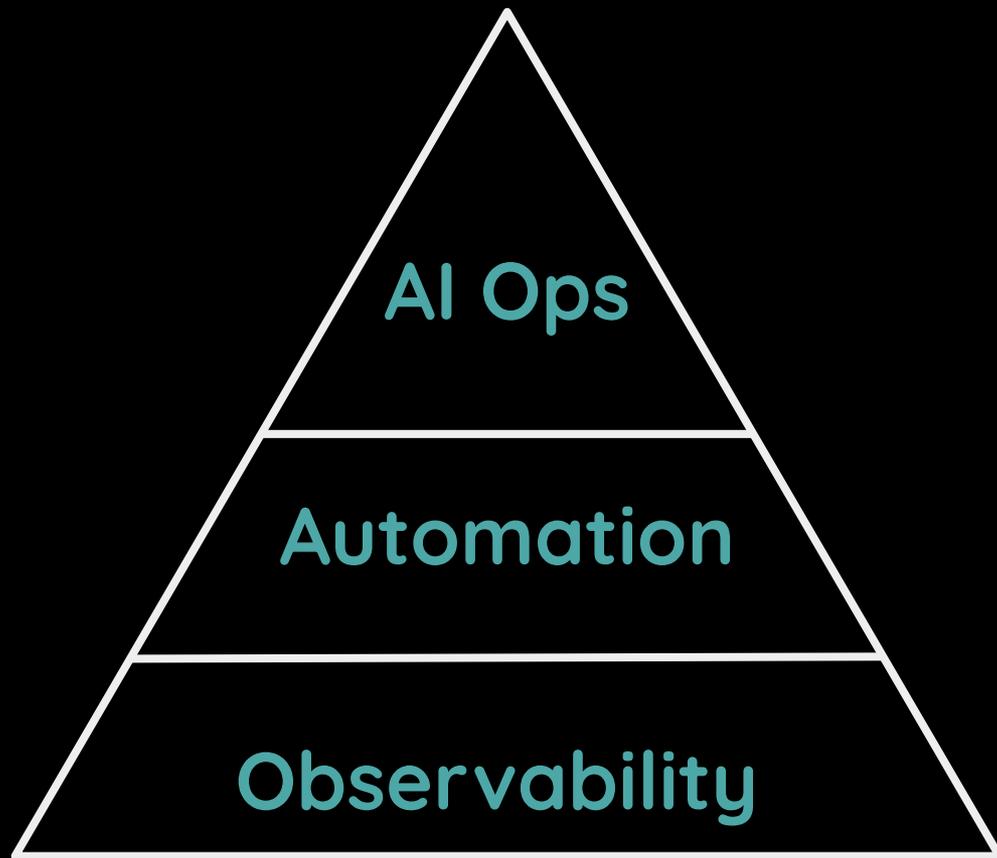
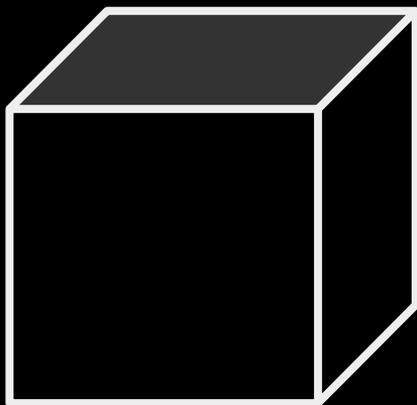
- Testing engineering components
- Identifying potential project obstacles
- Developing actionable solutions
- Collaborating with other engineers

[INDEED.COM/CAREER-ADVICE/FINDING-A-JOB/HOW-TO-BECOME-JUNIOR-ENGINEER](https://www.indeed.com/career-advice/finding-a-job/how-to-become-junior-engineer)



A need for observability





Service management provides you with the tools and processes to maintain your services, manage incidents, and improve them



- Consult car manual to investigate what could be wrong
- Bring in mechanic/skilled experts to help fix issues
- Change tire, refuel, ...



- Investigate issues with **Case Management**
- Bring in the right teams to handle critical incidents w/ **On-Call** and **Incident Management**
- Auto-remediate with **Workflow Automation**



DATADOG

Go to...

Recent

Dashboards

Monitors

Watchdog

Service Mgmt

Infrastructure

APM

Digital Experience

Software Delivery

Security

LLM Observability

Errors

Metrics

Logs

Integrations

Bits AI

Screen Share

Summary

Total Incidents

107

w/ Customer Impact

6

% of Total Incidents

6%

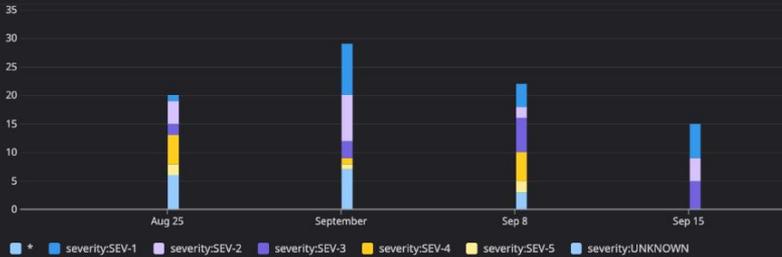
Mean Customer Impact Duration

2.22 days

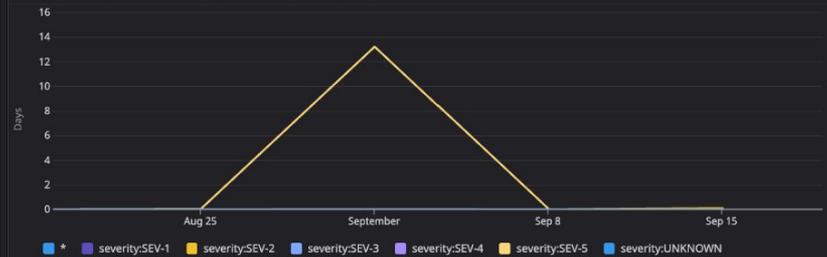
Top Incident Count by Severity



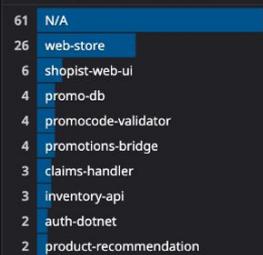
Weekly Incident Count by Severity



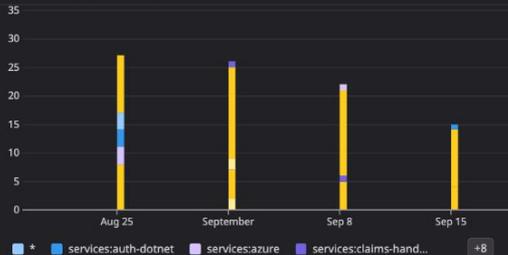
Weekly Mean Customer Impact Duration by Severity



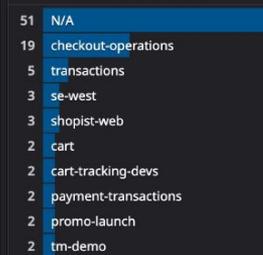
Top Incident Count by Service



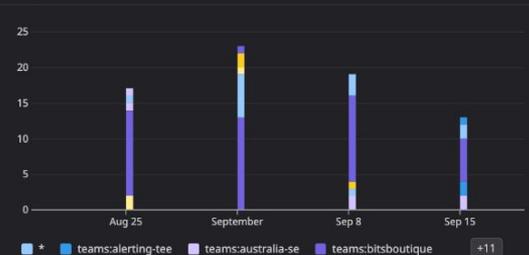
Weekly Incident Count by Service



Top Incident Count by Team



Weekly Incident Count by Team





DATADOG

Go to... + K

Recent

Dashboards

Monitors

Watchdog

Service Mgmt

Infrastructure

APM

Digital Experience

Software Delivery

Security

LLM Observability

Errors

Metrics

Logs

Integrations

Bits AI

CI Visibility

Pipelines

Pipeline Executions

Dashboard

+ Add Pipeline

CI Pipelines Dashboard

Pipeline Success Rate

77.58%

Stage Success Rate

98.12%

Job Success Rate

96.38%

Top Slowest Pipelines

99.9	ad-server-dns
94.9	fraud-prevention-api
30.5	api-payment.com
30.1	corp-site
27.2	email-api-py
23.7	auth-dotnet-postgres
22.3	ad-auction-tcp
18.9	ad-server-redis

Top Slowest Stages

2.42	binary_build
2.30	functional_test
1.93	image_build
1.62	package_build
1.59	qa
1.27	image_scan
1.24	source_test
1.20	prepare

Top Slowest Jobs

1.26	docs-link links
1.13	docs-link markdown
1.06	translations
1.05	check-license-headers
1.04	codeprotect
1.04	codequality
1.02	testlinux
1.00	testmac

Get started with CI Visibility

- Slice and dice your pipeline, stage, and job data to the exact needs of your team
- View the health of your pipelines and quickly identify your most problematic stages and jobs
- A Flame Graph view for every pipeline gives you the information you need to alleviate bottlenecks and optimize performance

[Learn More](#)

Env * Teams Select up to 5 Teams

1w Past 1 Week

Search By pipeline name

Showing 1-50 of 97 pipelines

Some pipelines are excluded Options

PIPELINE	DEFAULT BRANCH	EXECUTIONS	FAILURES	FAILURE %	MEDIAN	MEDIAN CHANGE	LAST BUILD	DURATION	LAST RUN
DataDog/cart-tracking test_and_deploy_cart	main	52	46	88.5%	1 h 8 min	-2 min 26 s	ERROR	25 min 31 s	6 minutes ago
DataDog/DevOps/cart-tracking test_and_deploy_cart	main	6	5	83.3%	23 min 14 s	-	ERROR	24 min 3 s	6 minutes ago
DataDog/payments-backend	main	40	33	82.5%	37 min 18 s	-1 min 16 s	ERROR	38 min 10 s	11 minutes ago
DataDog/shopist-web-ui Staging Build Deploy and Test	prod	330	1	0.3%	6 min 19 s	+6.26 s	SUCCESS	6 min 15 s	13 minutes ago
DataDog/shopist-serverless shopist-returns load testing	main	329	329	100%	0 ns	-	ERROR	35 min 59 s	13 minutes ago
DataDog/payments-backend test_and_deploy_paym_b	main	45	34	75.6%	37 min 38 s	-9.00 s	ERROR	38 min 16 s	17 minutes ago



DATADOG

Go to... ⌘ + K

Recent

Dashboards

Monitors

Watchdog

Service Mgmt

Infrastructure

APM

Digital Experience

Software Delivery

Security

LLM Observability

Errors

Metrics

Logs

Integrations

Workflow Automation

All Workflows

Blueprints

Action Catalog

Connections

Private Action Runners BETA

Dashboard

USE CASES

Change Management

Collaboration

DevOps

Incident Management

Remediation

Security

ACTION TYPES

AWS

Azure

CircleCI

Cloudflare

Data Transformation

Datadog

Fastly

GitHub

GitLab

GreyNoise

HTTP

Jira

Search blueprints by name, category or integration

Change Management 8 blueprints



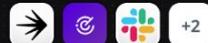
Periodically Update Allowlist With Datadog IPs

This workflow retrieves Datadog IP addresses and adds them to an...



Ask for Approval of Merge Requests Older than 2 Weeks

Automate approving merge requests in GitLab via Slack



Release New Features Incrementally with...

Roll out your feature to a small percentage of contexts and...



Add an Existing Okta User to a Group

Automate how Okta users are added to Okta Groups.



Mitigate Costs From Unused EBS Volumes

Trigger from a cost monitor to detach and delete unused EBS...



Declare PagerDuty Incident via Slack

Manage PagerDuty Incident creation via Slack responses.



Detach and Delete a List of EBS Volumes

Detach & delete EBS volumes after taking snapshots if needed.



AWS IAM Create User and Add to a IAM group

Add newly created IAM Users to the right IAM Group.

Collaboration 7 blueprints



Periodically Update Allowlist With Datadog IPs

This workflow retrieves Datadog IP addresses and adds them to an...



Ping Last Committer in GitHub

Identify and send Slack notifications to team members...



Send Slack Message with All Open Merge Requests from...

Get all open merge requests from GitLab in Slack



Incident and Alert Routing with PagerDuty and Slack

Escalate alerts to the right slack channels and assign Incidents to...



Add an Existing Okta User to a Group

Automate how Okta users are added to Okta Groups.

Narrative and expectations

Incident Response Workflow



Detect



Declare



Manage



Document



“The important thing is not to stop questioning.
Curiosity has its own reason for existing.”

- Albert Einstein

Questions?

Ajuna Kyaruzi
Senior SRE & DevOps
Advocate

ajuna@datadog.com

