AWS USER GROUP PUNE

"For the community, By the community!"

aws

COMMUNITY DAY

PUNE

23rd August 2025

Annual Edition

aws
COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws
USER GROUP
PUNE

From Logs to Locks : Using Observability to enhance Security posture

Sakshi Nasha & Zameer Fouzan

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

$whoami_

Sakshi Nasha

~~Senior s/w Engineer~~ Learner @Cohesity

- Community evan·gel·ist (AWS Community Builder)
- Innovator : Hackathons
- Athlete at heart : 🏃‍♀️🏀⚽🏸

Zameer Fouzan

Lead DevRel Engineer @newrelic

- AWS Community Builder
- Full Stack Tinkerer
- Open Telemetry Advocate

aws USER GROUP PUNE

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

Agenda

aws USER GROUP PUNE

01 Challenges: Why Cloud Security Often Fails

02 Reports: Real-World Breaches from Misconfigurations

03 The Missing Link: Observability in Security

04 Real world use cases with Architectural Diagrams

05 Best Practices & Shift Left, Respond Right

06 Resources


0:02
I am in
gifmemes.io

Challenges: Why Cloud Security Often Fails

- **IAM Misconfigurations :**

  Over-permissive policies (e.g. *:*) , Forgotten roles or unused keys still active / static credentials
- **Lack of Visibility into User Activity**:

  CloudTrail is noisy, hard to filter meaningful actions
- **Alert Fatigue:**

  Too many alerts from multiple tools → important ones missed
- **No Real-Time Action:**

  Logs are stored, but not monitored in real-time
- **Security ≠ Observability** (Traditionally) :

  Security teams and DevOps teams are often siloed

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws USER GROUP PUNE

When It Goes Wrong: Real Breaches from Small Mistakes

Capital One Breach (2019)

Cause

- IAM role allowed access via SSRF
- Logs showed suspicious activity weeks before detection

Impact : 100M records exposed + **$80M** fine

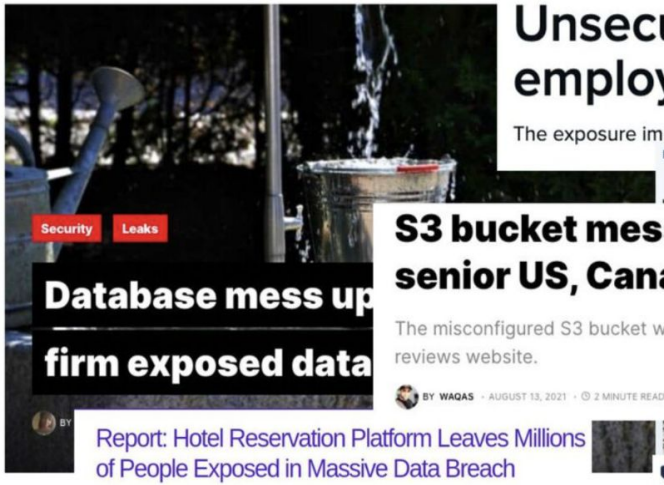
Uber (2022)

Cause

- Credentials hardcoded in a script
- Excessive IAM role privileges.
- CloudTrail logs existed but were never monitored in real-time

Impact : Admin access to Slack, AWS, Google

Open S3 Buckets and Other Exposed Data Stores



Unsecured AWS server exposed 3TB in airport employee records

The exposure impacted airport staff across Colombia and Peru

Breaches › Political History: How A Democratic Organization Leaked Six Milli

S3 bucket mess up exposed 182GB of senior US, Canada citizens data

The misconfigured S3 bucket was owned by SeniorAdvisor, a consumer ratings reviews website.

BY WAQAS · AUGUST 13, 2021 · 2 MINUTE READ

Home » Cybersecurity » Data Security » AWS S3 Bucket at Center of Data Breach, Again

AWS S3 Bucket at Center of Data Breach, Again

by Eric Kedrosky on February 1, 2022

Misconfigured S3 bucket

Gartner stated, "through 2022, at least 95 percent of cloud security failures will be the customer's fault." Unfortunately, today's news highlights an example of a data breach due to a simple, but harmful misconfiguration: an exposed AWS S3 bucket. The misconfigured AWS bucket reportedly did not require any authentication to access, yet contained two main datasets related to Securitas and airport employees. As an incredibly powerful service, AWS S3 remains a lightning rod for data breaches due to widespread security misconfigurations.

UpGuard Team
Published Sep 06, 2019

Report: Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach

Mark Holden November 06, 2020

Company: Prestige Software, based in Spain.

Severity: High

Size: 24.4 GB, totaling 10,000,000+ exposed files

Silicon.co.uk
insights for IT professionals

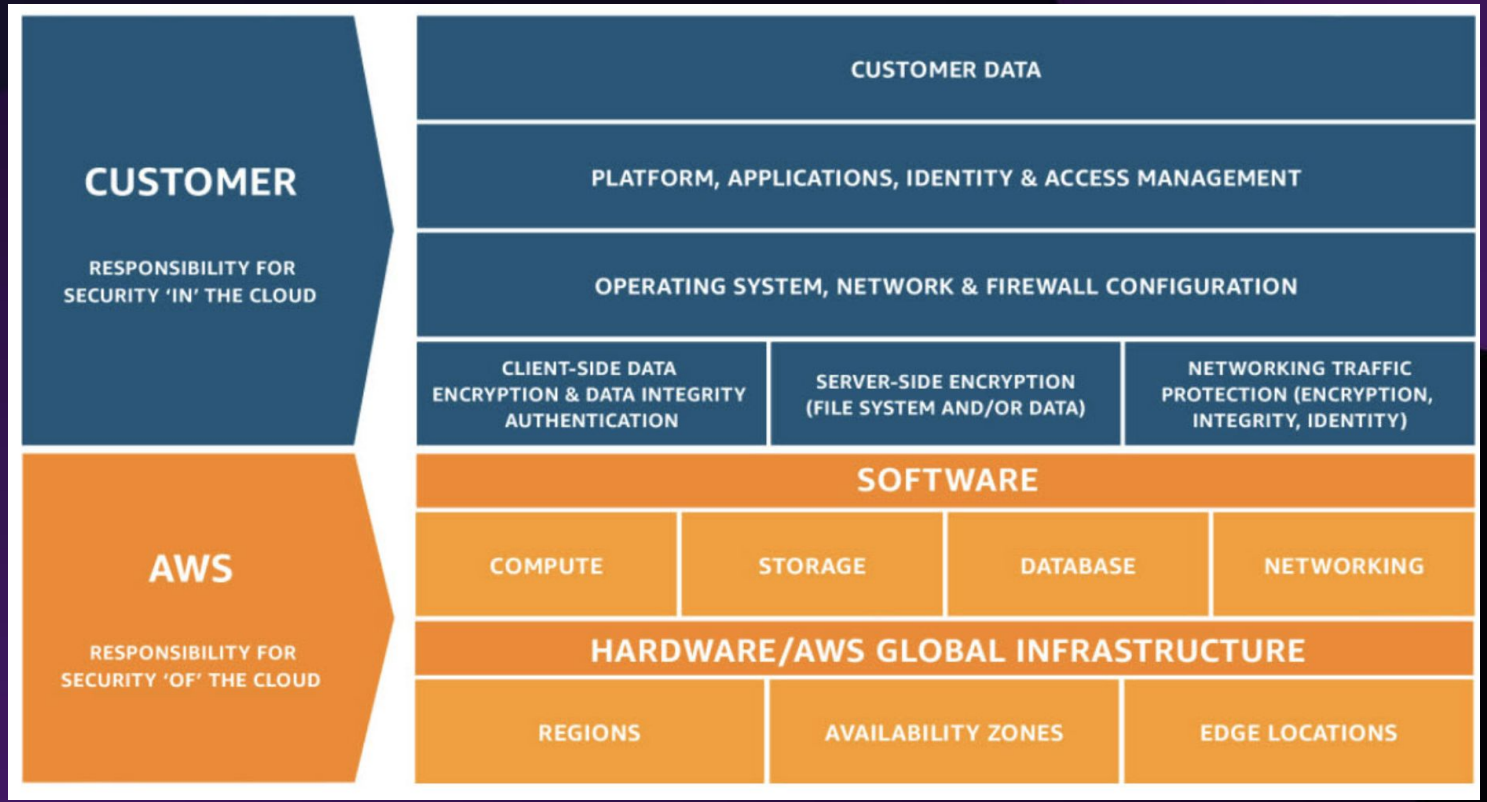
MENU CLOUD SECURITY BIG DATA IOT AI 5G BLOCK CHAIN EVENTS

British Passport Data Exposed On Unsecured AWS Bucket

“ Through 2025, Over 99% of cloud breaches will have a root cause of customer misconfiguration or mistakes by end users ”

- Gartner Report

Security as a Shared Responsibility



Logs Are Plentiful : Security Insights Are Not

- Logs (e.g., CloudTrail, VPC Flow Logs) are often collected but not analyzed for security
- Monitoring ≠ Alerting ≠ Incident Response → different maturity levels
- Traditional monitoring focuses on performance & uptime, not IAM anomalies or misuse
- Security teams are often siloed from DevOps/Infra teams using observability tools
- Without correlation, logs become post-incident forensics, not prevention

Challenges: Why Cloud Security Often Fails

MELT ⏩ MELTX

Metrics

Events

Logs

Traces

Configuration

Policy Changes

User Behaviour

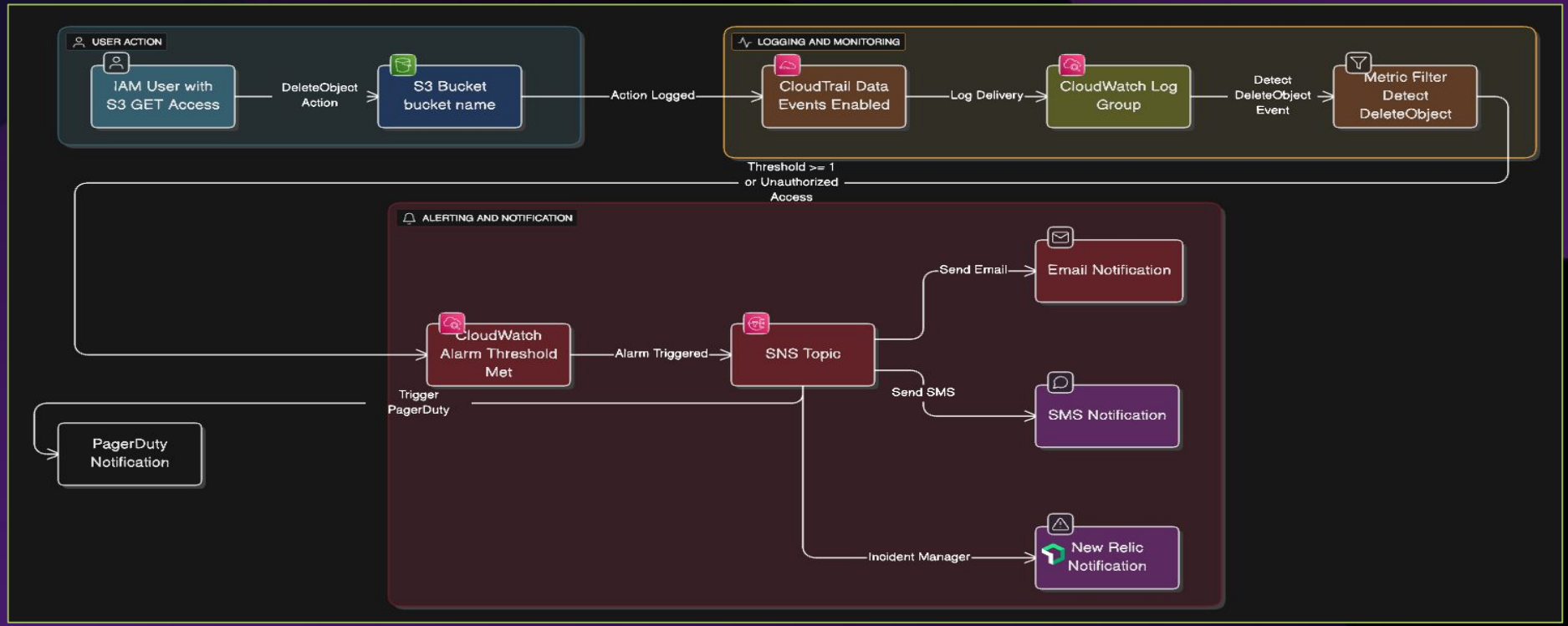
Identity

Threats

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws USER GROUP PUNE

From Logs to Locks - Building a Security Signal Pipeline

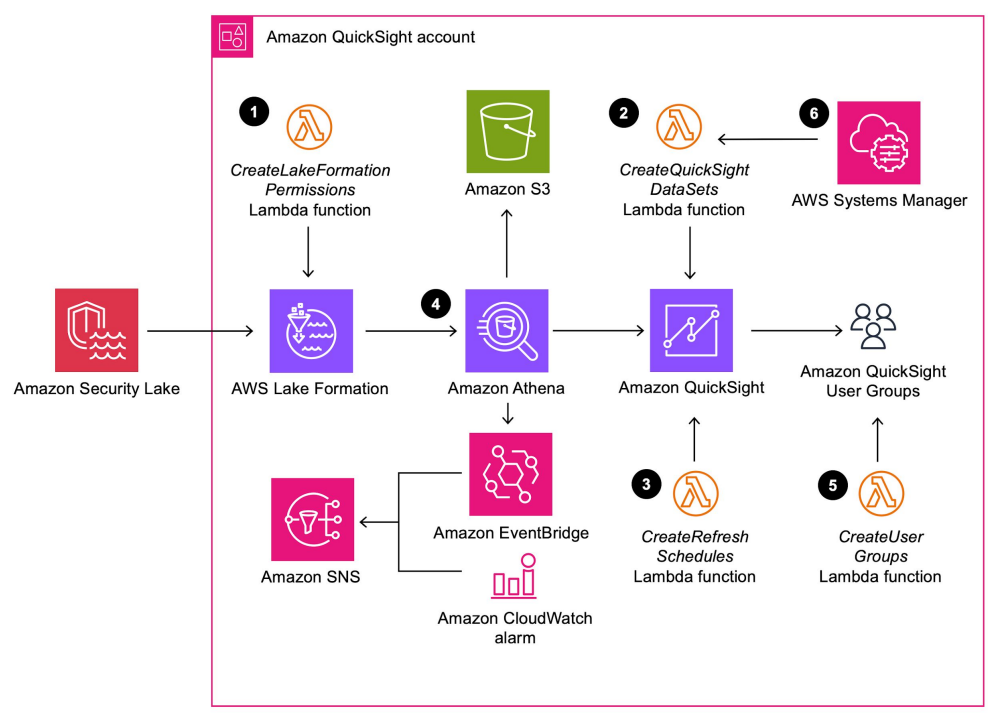



DEMO TIME!
38
... WHAT COULD POSSIBLY GO WRONG
makeameme.org

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws USER GROUP PUNE

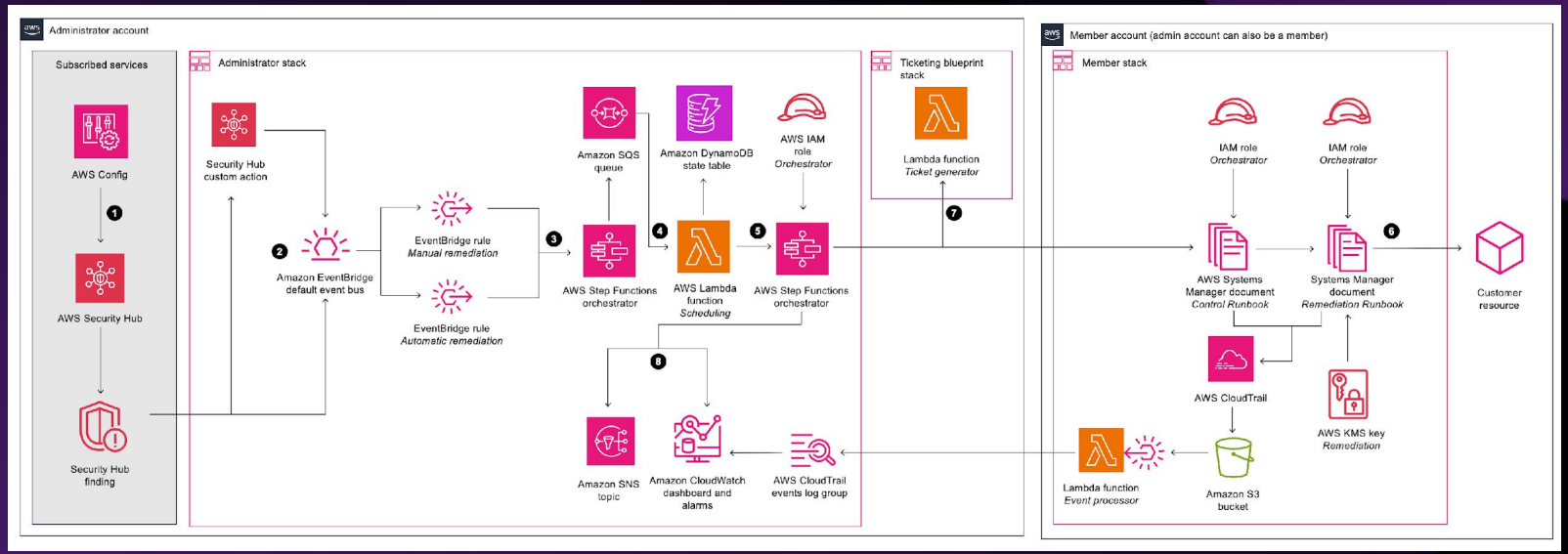
From Logs to Locks — Building a Security Signal Pipeline



aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws USER GROUP PUNE

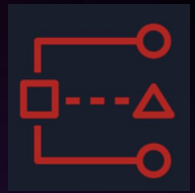
From Logs to Locks — Building a Security Signal Pipeline



aws
COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws
USER GROUP
PUNE

Security Best Practices



IAM Access Analyzer

Switch to Dynamic Creds

Least Privilege Principle

Solving problems, fixing errors, software security are a fact of a developer's life.

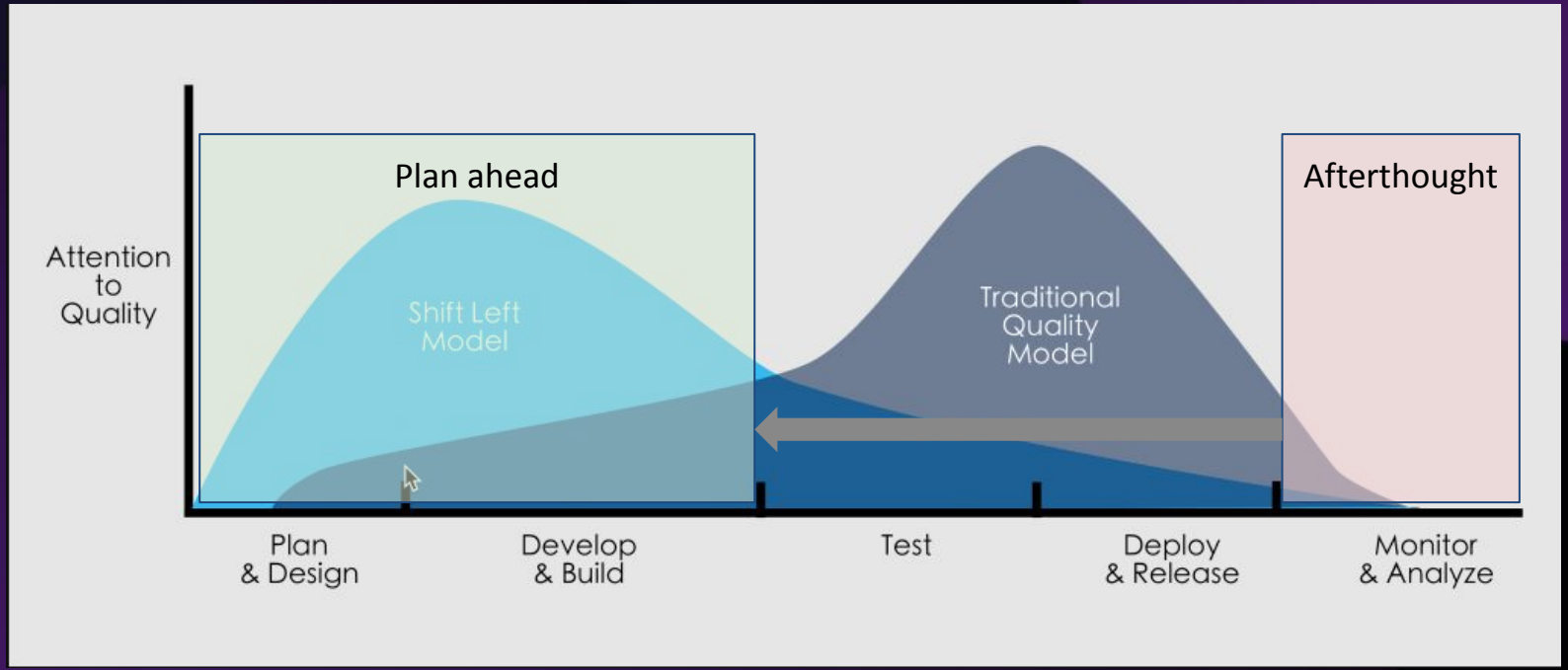
(unfortunately)

Mostly Reactive

Too Much Noise

Not Enough Context

Shift Left → Respond Right



aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

Shift Left → Respond Right

Outcome:

Faster detection → reduced risk → CONTINUOUS SECURITY & improved MTTx in fast-moving cloud environments.

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

Connect with us!

aws USER GROUP PUNE

Sakshi Nasha

Zameer Fouzan

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

Resources

Security Best Practices

AWS IAM Access Analyzer

AWS Cloud Security Weekly

AWS Weekly Podcast

aws
COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws
USER GROUP
PUNE

SAFETY FIRST

aws COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

Thank you to AWS UG Pune

Back to 2023

Back to 2024

aws COMMUNITY DAY PUNE 23rd August 2025 Annual Edition

Thank you to AWS UG Pune

today 2025 and many more…

aws
COMMUNITY DAY
PUNE
23rd August 2025
Annual Edition

aws
USER GROUP
PUNE

Q&A, Bring it on!