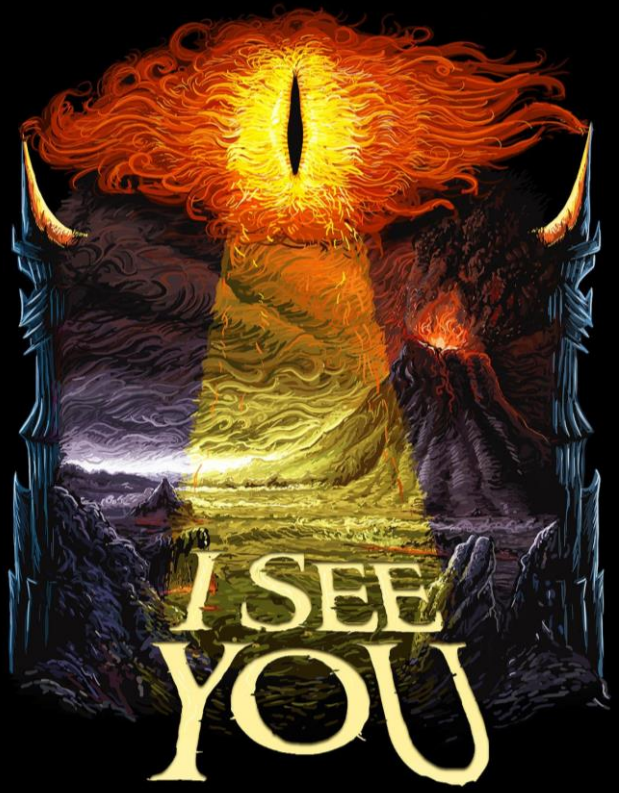
THE LORD OF THE METRICS

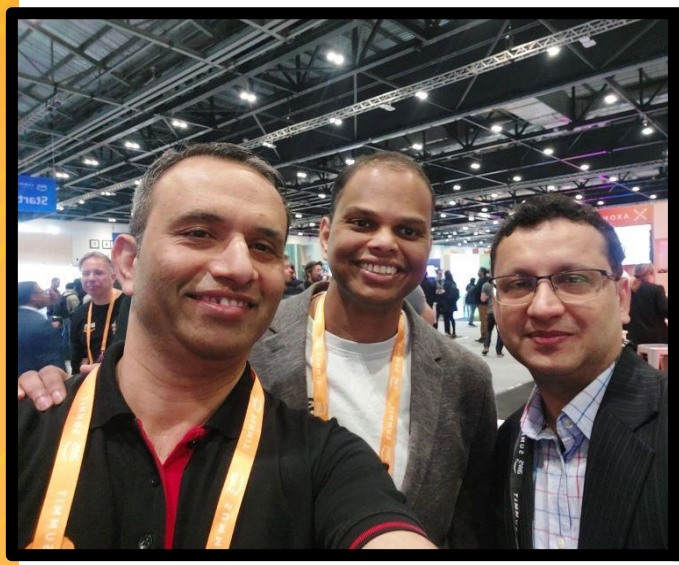
BeSA
Become a Solutions Architect

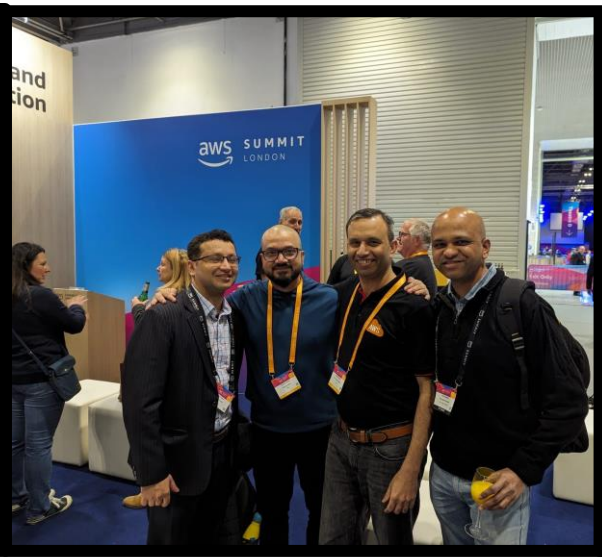


Week 04


Batch 05
Week 04
27-April
BeSA
Cloud Practitioner
Domain 4
Billing, Pricing, and Support

Thank you so much for meeting us at London Summit





Tentative Agenda

Week	Date	Certification Track	
01	06-Apr	Cloud Practitioner	Domain 1: Cloud Concepts
02	13-Apr		Domain 2: Security and Compliance
03	20-Apr		Domain 3: Cloud Technology and Services
04	27-Apr		Domain 4: Billing, Pricing, and Support
05	4-May	Solutions Architect Associate	Domain 1: Design Secure Architectures
06	11-May		
07	18-May		Domain 2: Design Resilient Architectures
08	25-May		
09	1-June		Domain 3: Design High-Performing Architectures
10	8-June		
11	15-June		Domain 4: Design Cost-Optimized Architectures
12	22-June		

Only for regulars

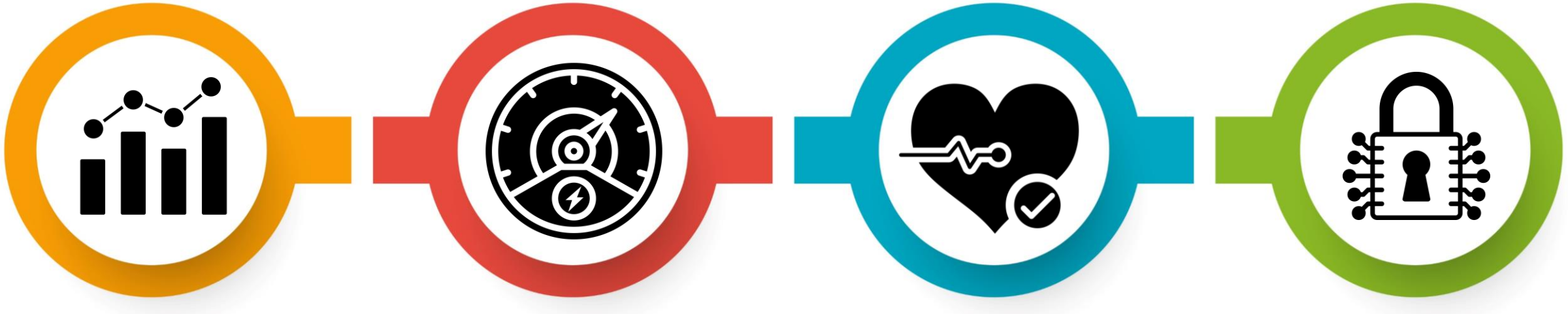
Well-Architected

Answer for your questions

- YouTube Shorts
  - 1 Minute Video
- Published every weekday
  - 5 Q&A in a week

SUBSCRIBE youtube.com/@AnalogiesCloud

Why monitoring is important?

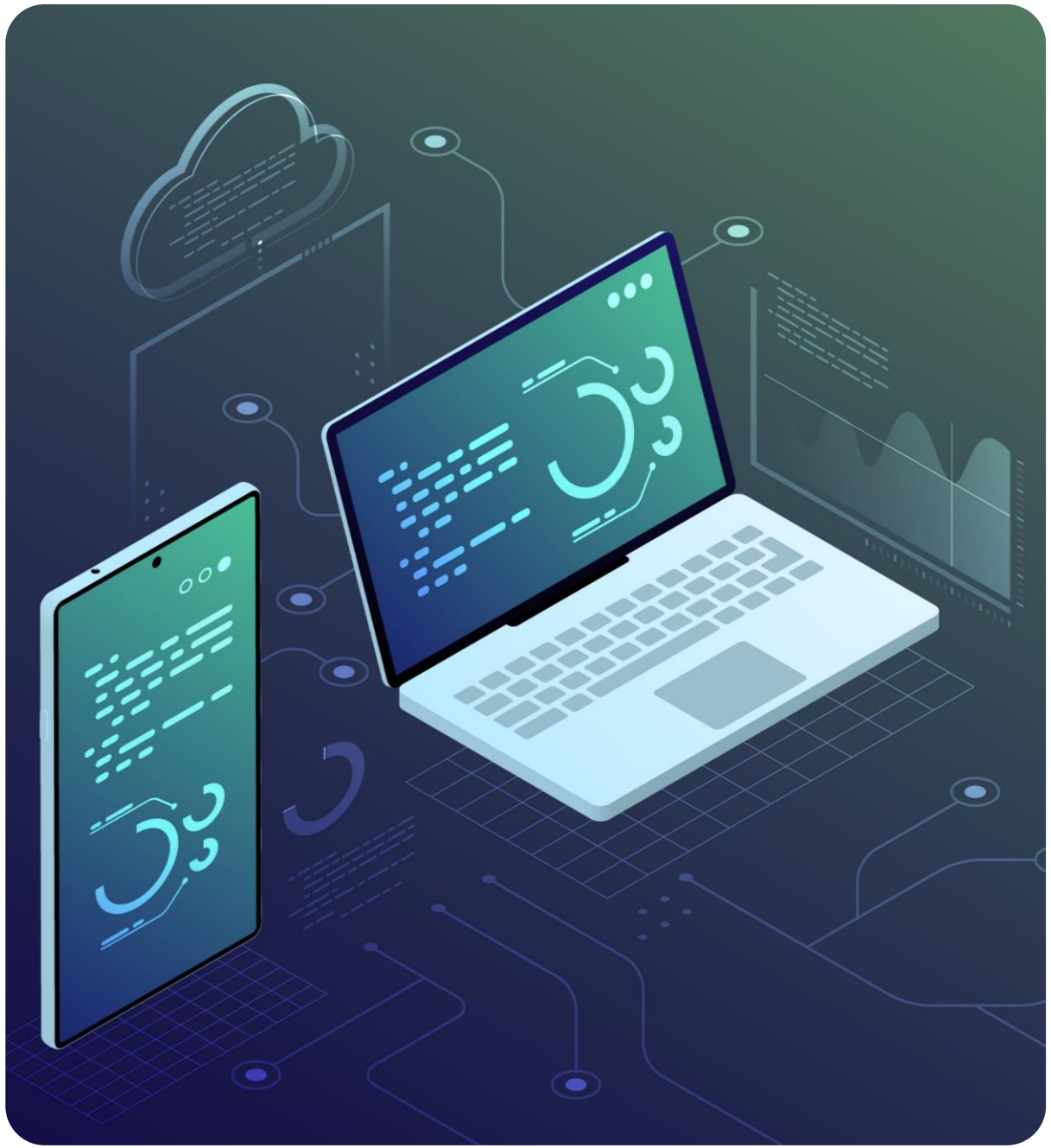


Performance

Utilization

Health

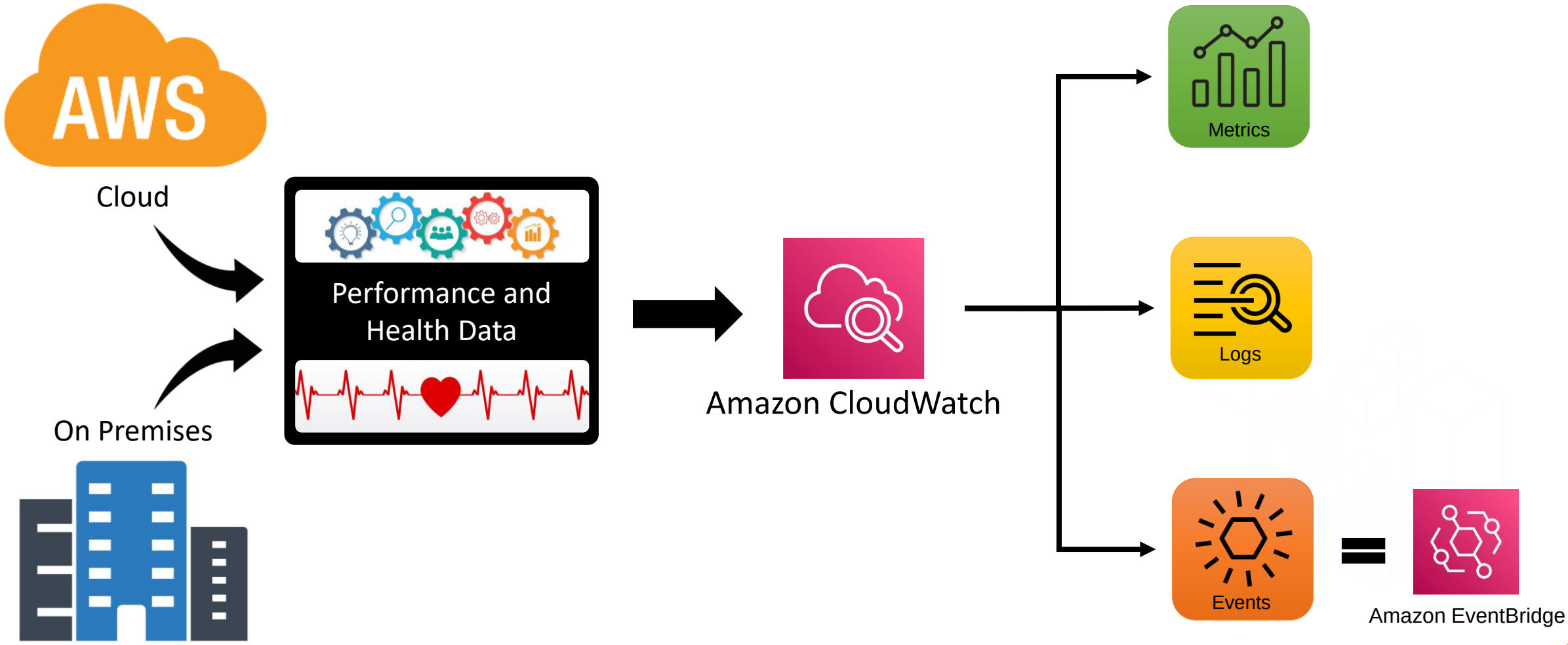
Security

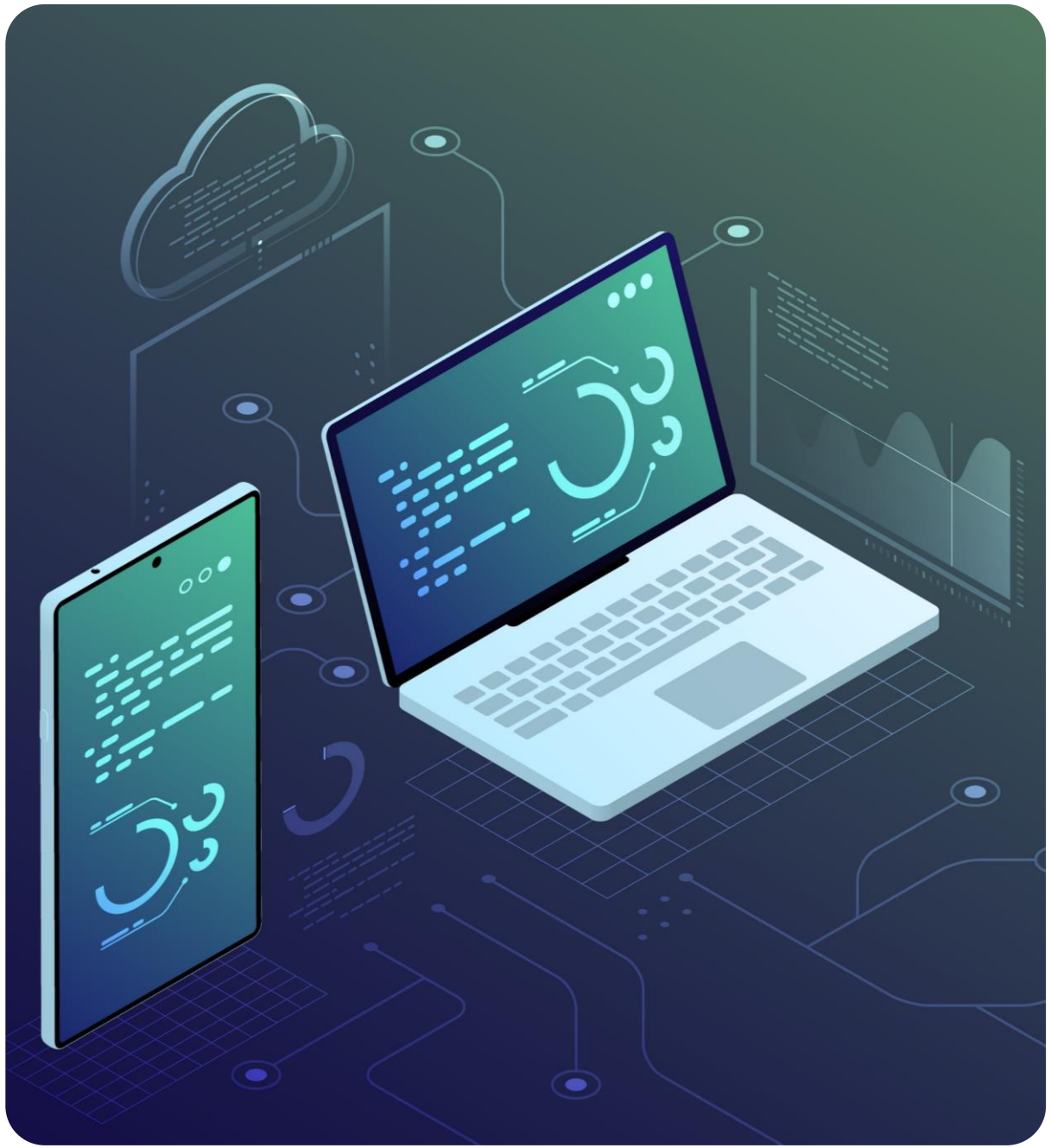


Amazon CloudWatch

Amazon CloudWatch

- Amazon CloudWatch allows you to collect, access, and correlate performance and health data of your application and infrastructure running on AWS and on-premises.



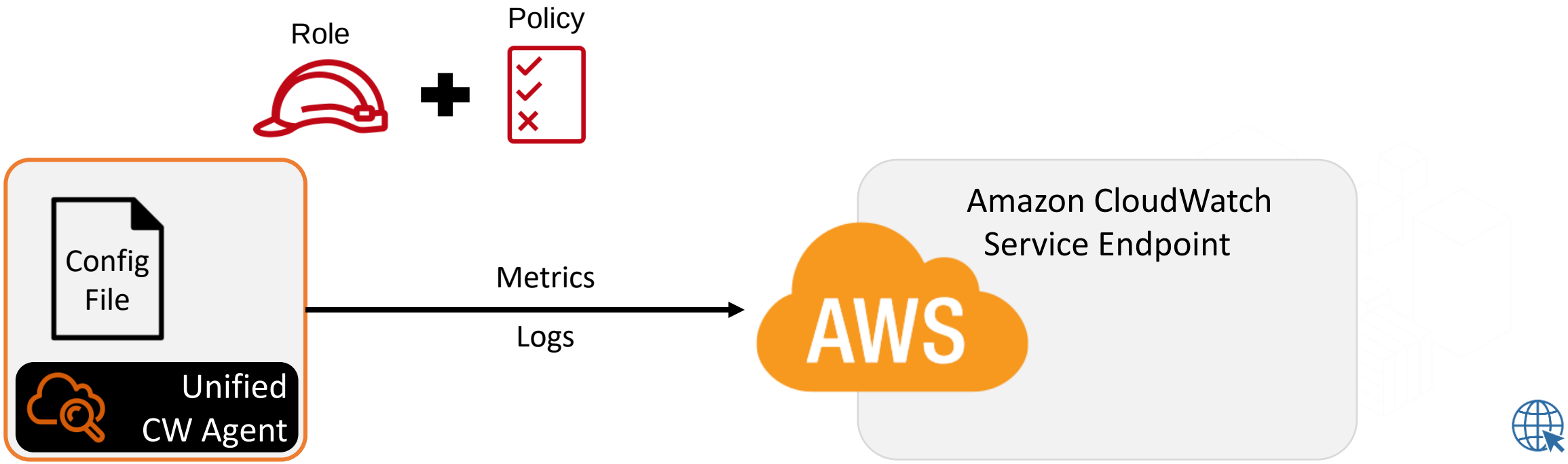


Custom Metrics

Custom Metrics

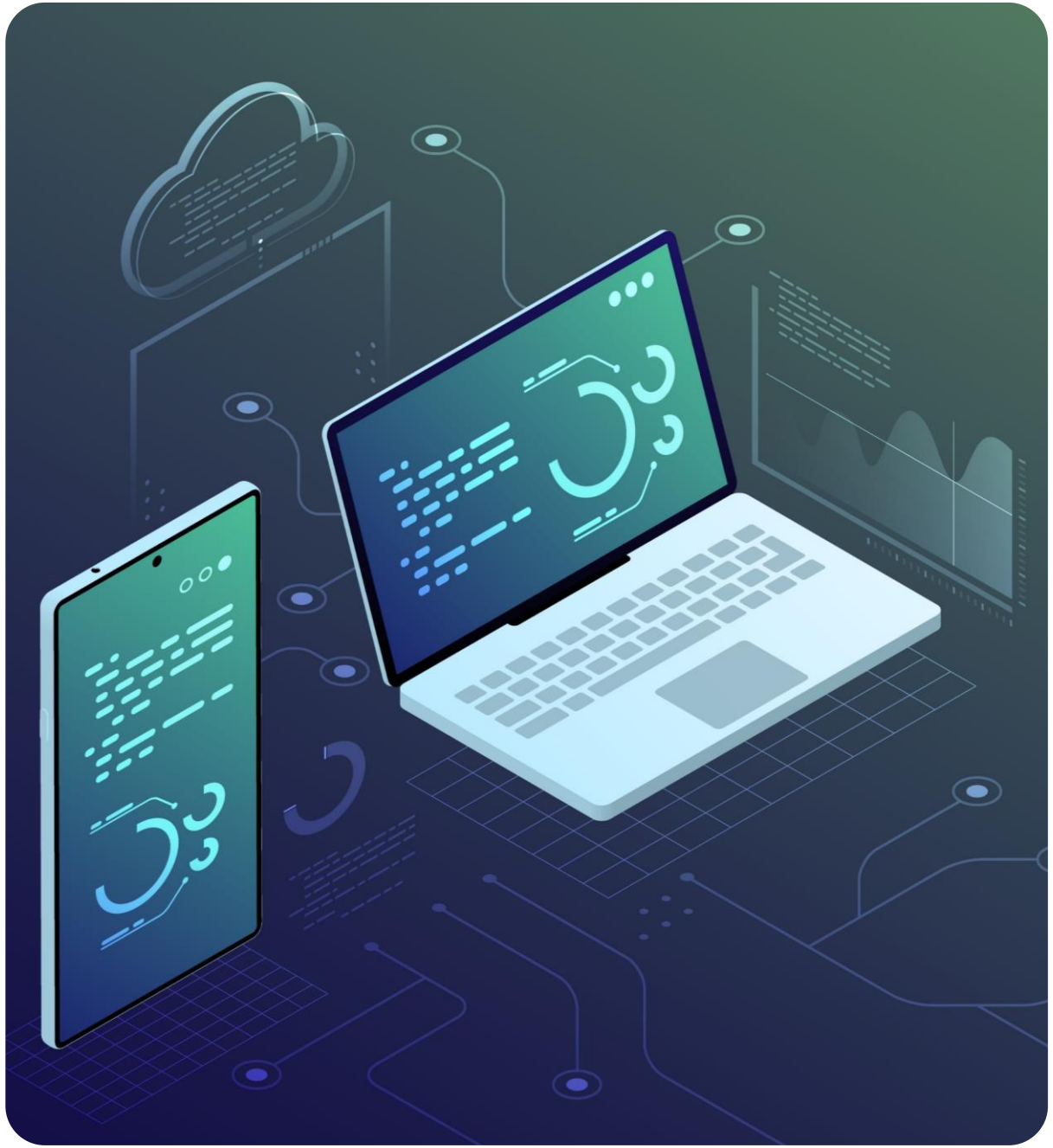
- You can publish custom metrics (your business and application metrics) to CloudWatch using the AWS CLI or an API.

- You can use the open source Unified CloudWatch agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers.



Configuring Custom Metrics

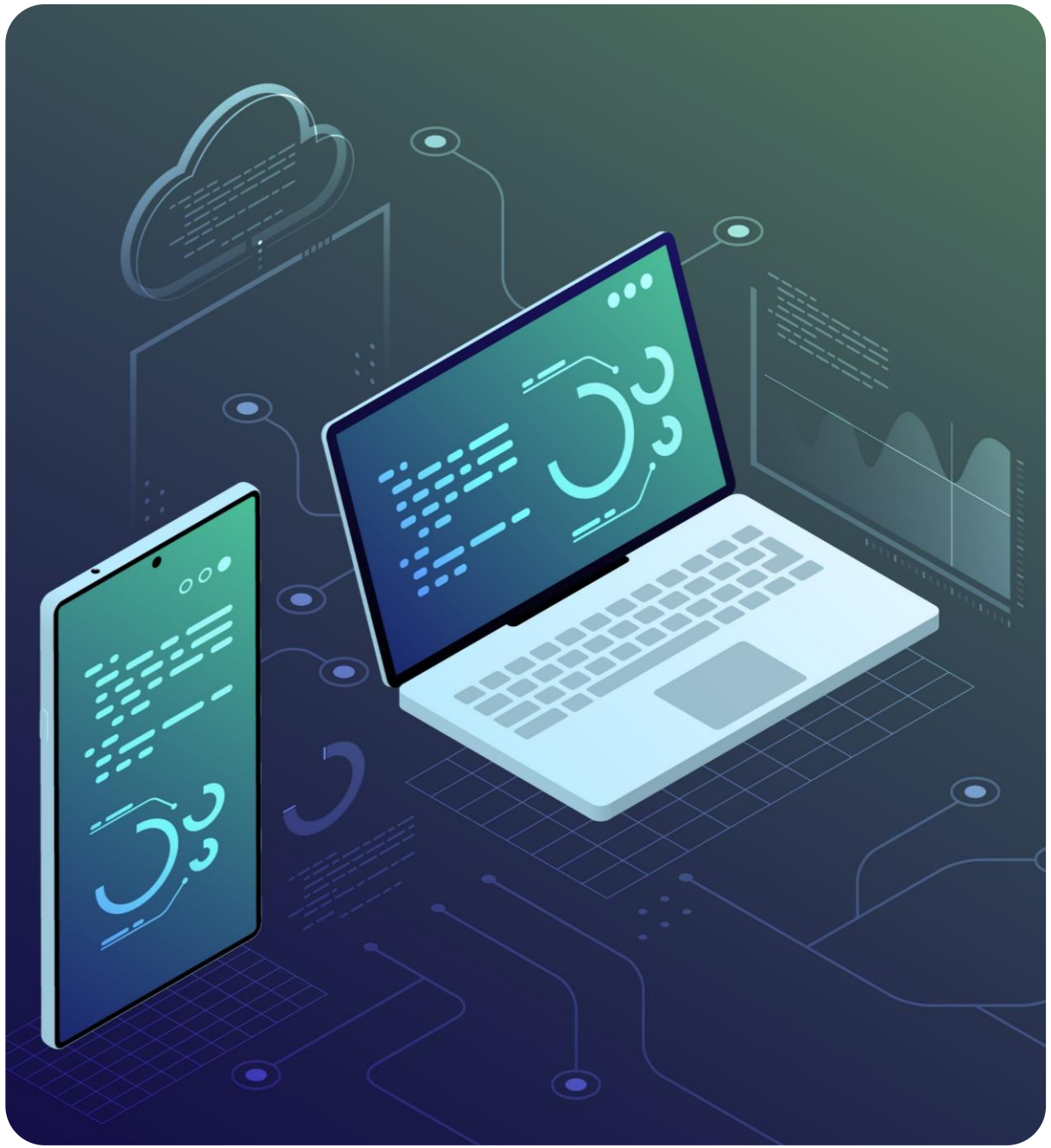
- Install Agent
  - sudo yum install amazon-cloudwatch-agent
- Configure it
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
- Create and associate IAM role (or user)
  - You use IAM roles on Amazon EC2 instances, and you use IAM users with on-premises servers.
- Start the agent
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -m ec2 -a status

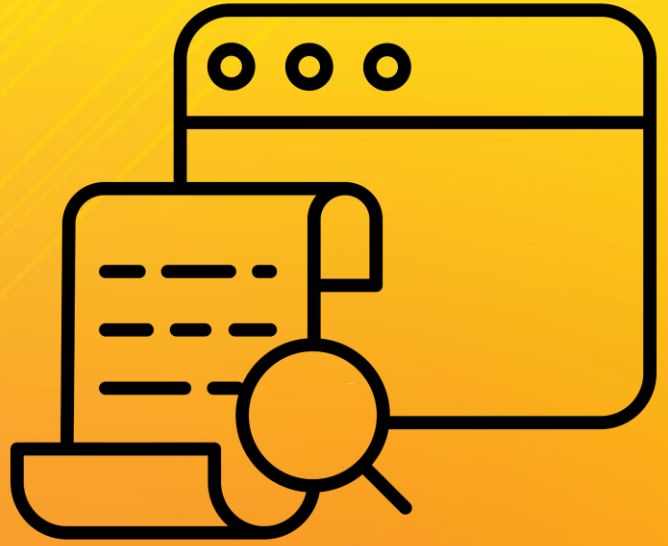


Alarms

Amazon CloudWatch Alarms

- An alarm watches a single metric over a specified time period, and performs one or more specified actions, based on the value of the metric relative to a threshold over time.
- You can use an alarm to automatically initiate actions on your behalf. The most common type of alarm action is to notify one or more people by sending a message to an Amazon Simple Notification Service topic.
- A metric alarm has the following possible states:
  - **OK** – The metric or expression is within the defined threshold.
  - **ALARM** – The metric or expression is outside of the defined threshold.
  - **INSUFFICIENT_DATA** – The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state.
- You can also add alarms to dashboards.

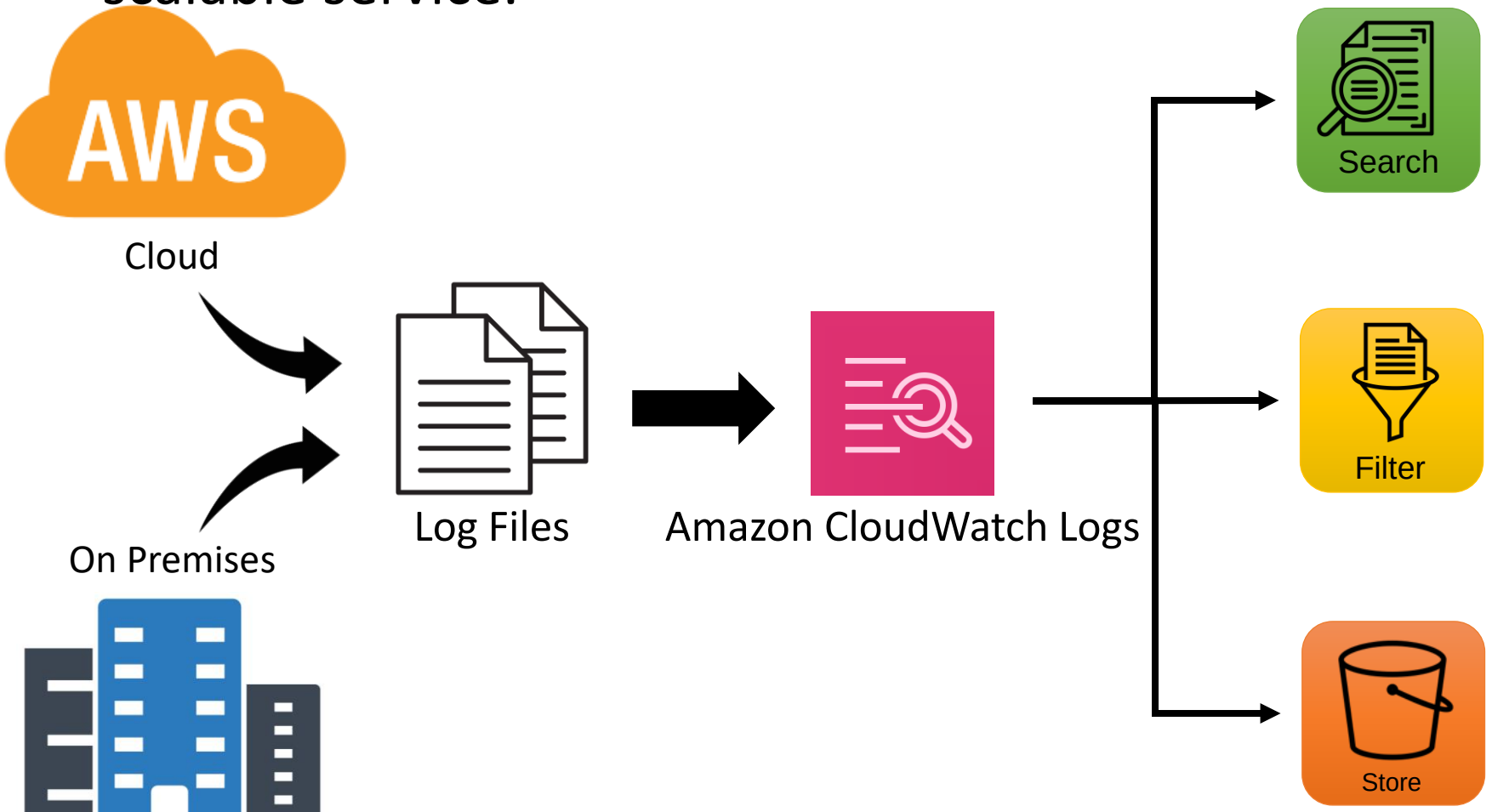




Amazon CloudWatch Logs

Amazon CloudWatch Logs

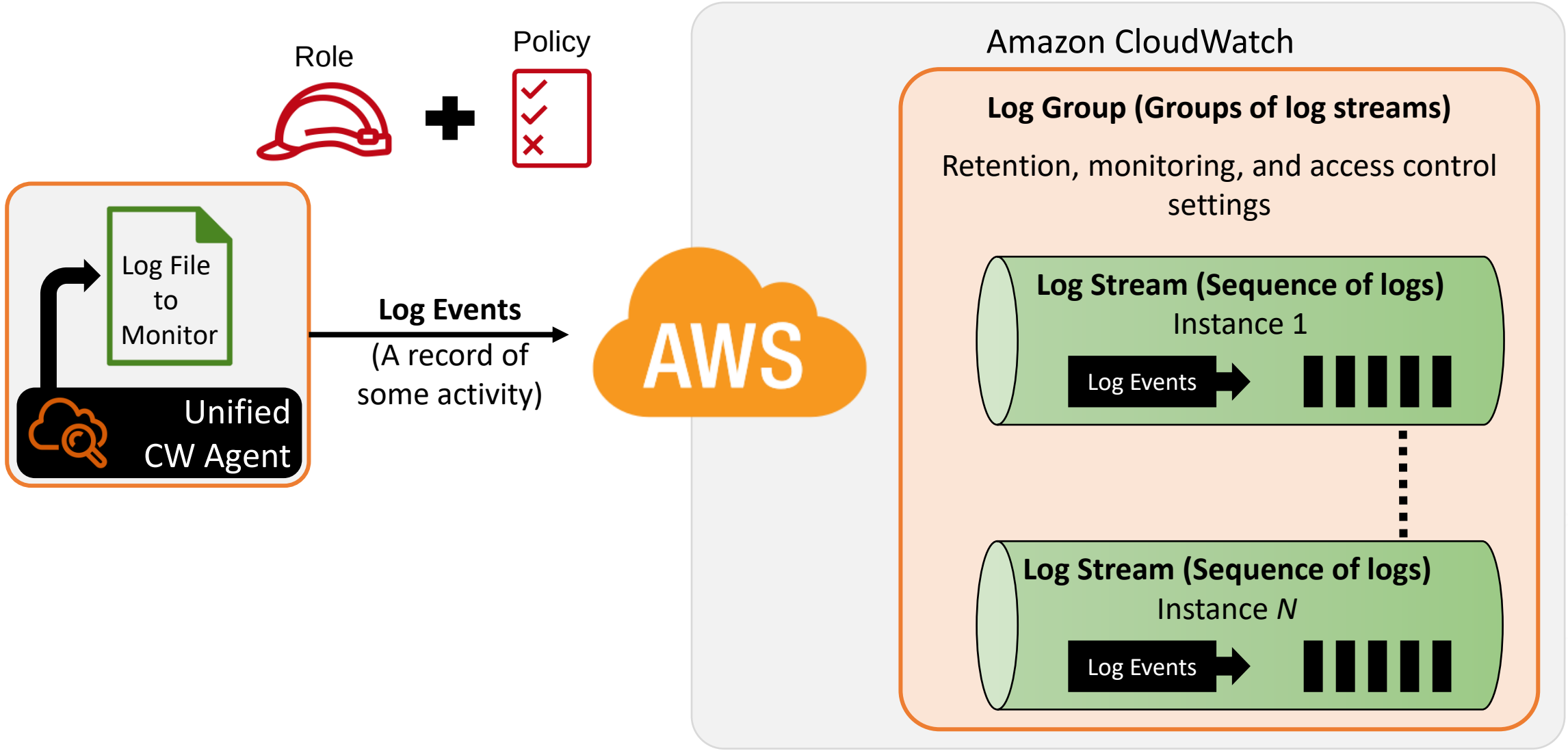
- CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service.



- You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis.

Publishing Logs

- You can publish logs to CloudWatch Logs using the unified agent.



Amazon CloudWatch Logs concepts

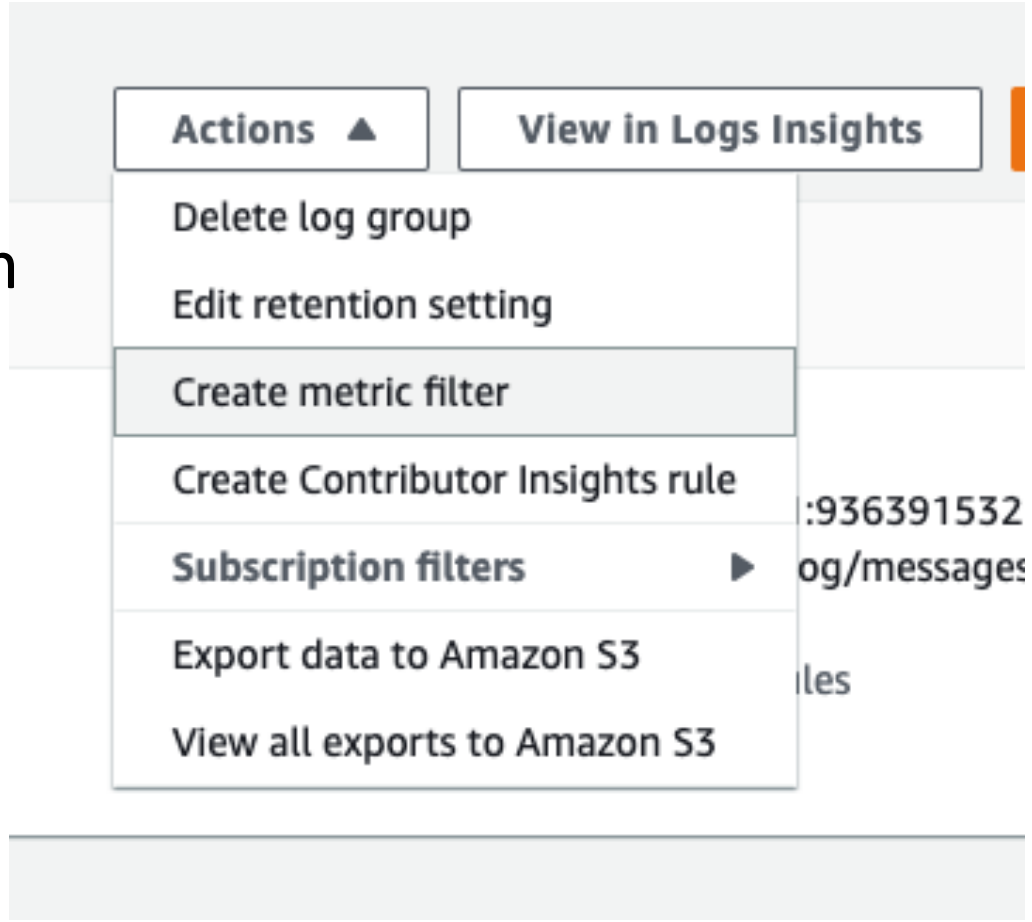
- Log events
  - A log event is a record of some activity recorded by the application or resource being monitored. The log event record that CloudWatch Logs understands contains two properties: the timestamp of when the event occurred, and the raw event message. Event messages must be UTF-8 encoded.
- Log streams
  - A log stream is a sequence of log events that share the same source. More specifically, a log stream is generally intended to represent the sequence of events coming from the application instance or resource being monitored. For example, a log stream may be associated with an Apache access log on a specific host.
- Log groups
  - Log groups define groups of log streams that share the same retention, monitoring, and access control settings. Each log stream has to belong to one log group. For example, if you have a separate log stream for the Apache access logs from each host, you could group those log streams into a single log group called MyWebsite.com/Apache/access_log.

Publishing Logs

- Install Agent
  - sudo yum install amazon-cloudwatch-agent
- Configure it by providing detail of log file to monitor
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
- Create and associate IAM role (or user)
  - You use IAM roles on Amazon EC2 instances, and you use IAM users with on-premises servers.
- Start the agent
  - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -m ec2 -a start

CloudWatch Metric Filter

1. Create a Filter
2. Test the pattern
3. Add it to and Alarm
4. Get notified



aws workshop studio

Reference:

FAQs

Amazon CloudWatch

What?

- Amazon CloudWatch allows you to collect, access, and correlate metrics, logs, and events data on a single platform from across all your AWS resources, applications, and services running on AWS and on-premises.

Why?

- Amazon CloudWatch helps you to detect anomalous behavior in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly.
- It also helps to break down data silos to better understand the health and performance of your resources.

When?

- You want to use a single platform for observability and to collect metrics of AWS and on premises resources.
- You also want to improve operational performance and resource optimization, get operational visibility and insight to derive actionable insights from logs.

Where?

- Amazon CloudWatch is a regional service but you can create cross-account, cross-region dashboards too.
- Through an agent deployed on on-premises system you can also collect metric.

Who?

- It natively integrates with more than 70 AWS services.
- You can create alarms based on metric value thresholds, or use alarms that can watch for anomalous metric behaviour.
- You can install a unified CloudWatch agent to collect logs and metrics.

How?

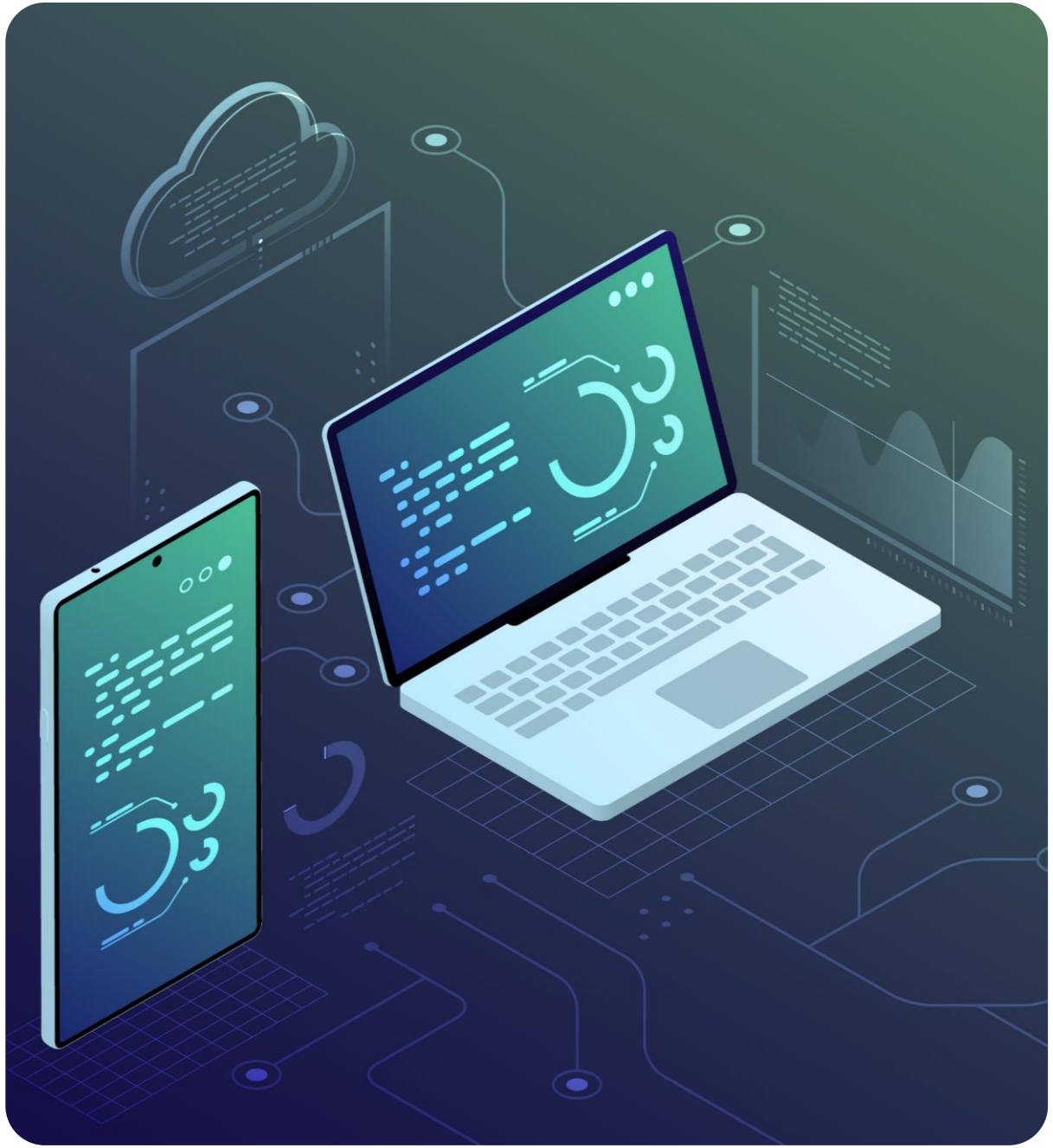
- CloudWatch is basically a metrics repository. It correlates your metrics and logs to better understand the health and performance of your resources.
- Create alarms based on metric value thresholds, or alarms for anomalous metric behavior based on ML algorithms.

Category:

Management and Governance

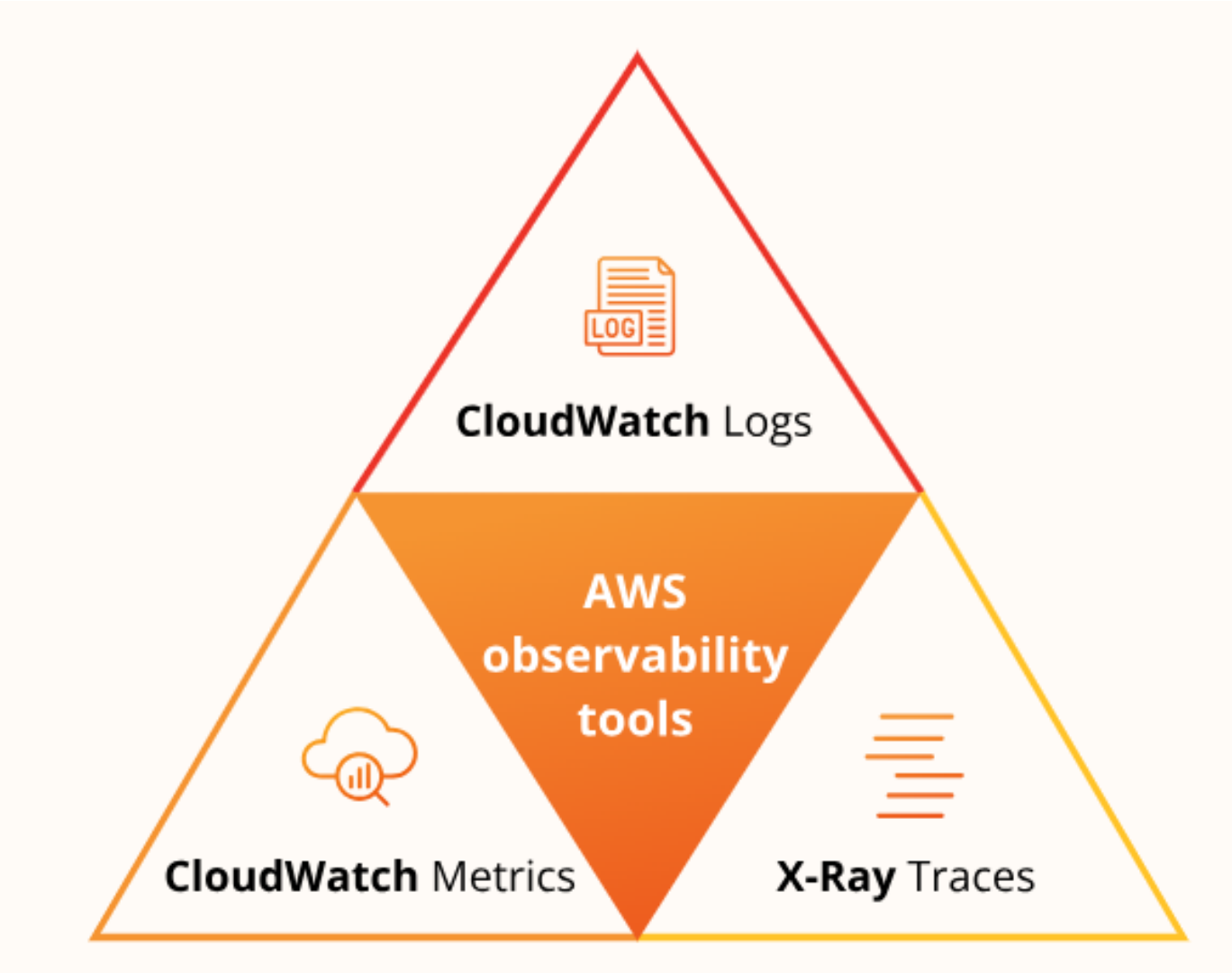
How much?

- Charges are calculated for number of Metrics (includes detailed and custom metrics), APIs, Logs Ingested, Log Storage/Archival, Logs Insights Queries (analyse Log Data), Events, dashboards, alarms, Contributor Insights, Lambda Insights and Canaries.



Observability

Observability in AWS



Tracking

Your tracking information

For barcode 3412404922978249

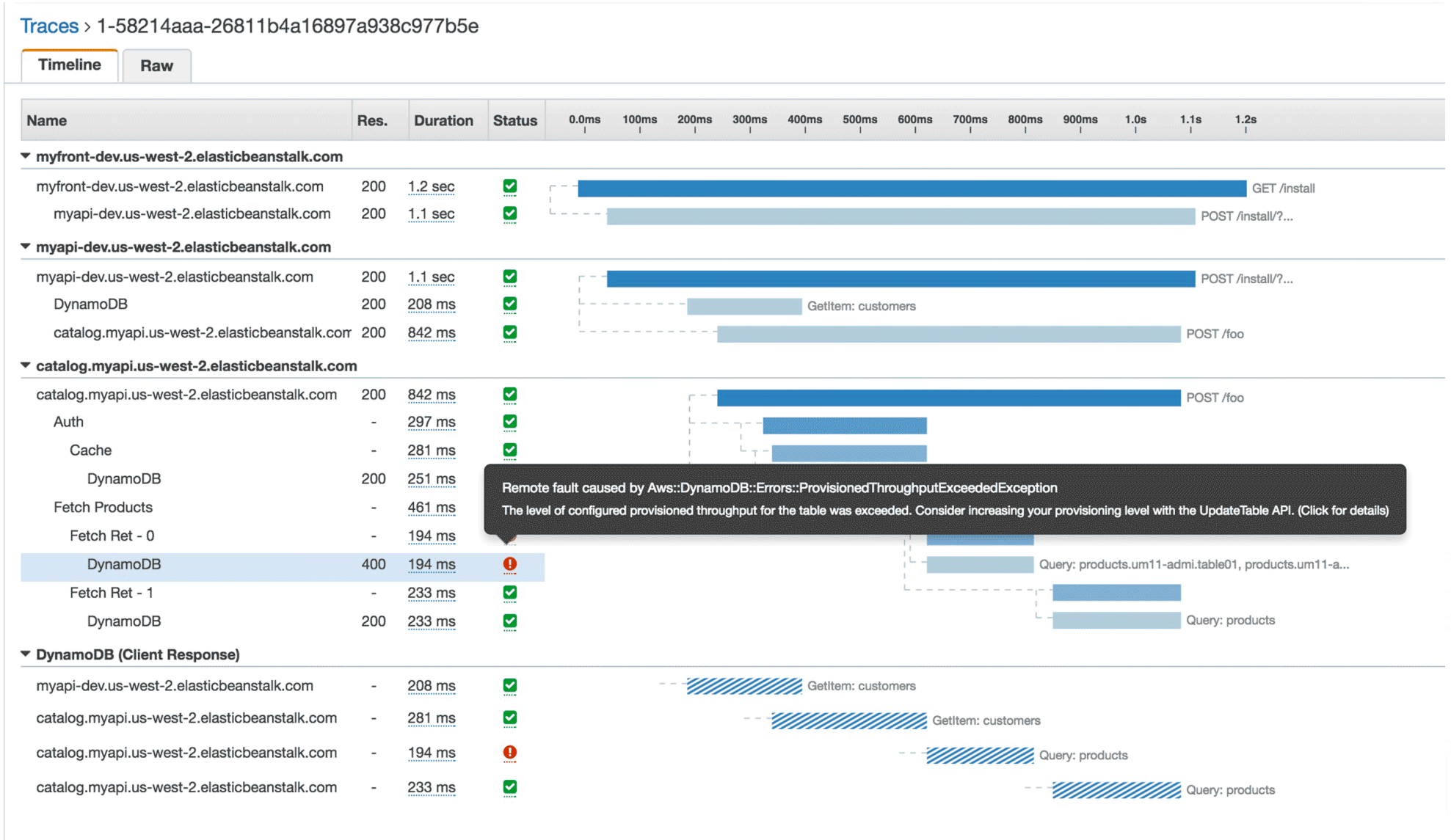
Date	Time	Tracking status
05/01/2019	16:28	Dropped off at the ParcelShop
02/12/2018	06:25	On its way back to the retailer
01/12/2018	17:01	Entered the Hermes network
30/11/2018	17:02	Missing Pre-Advice
30/11/2018	17:02	Dropped off at the ParcelShop

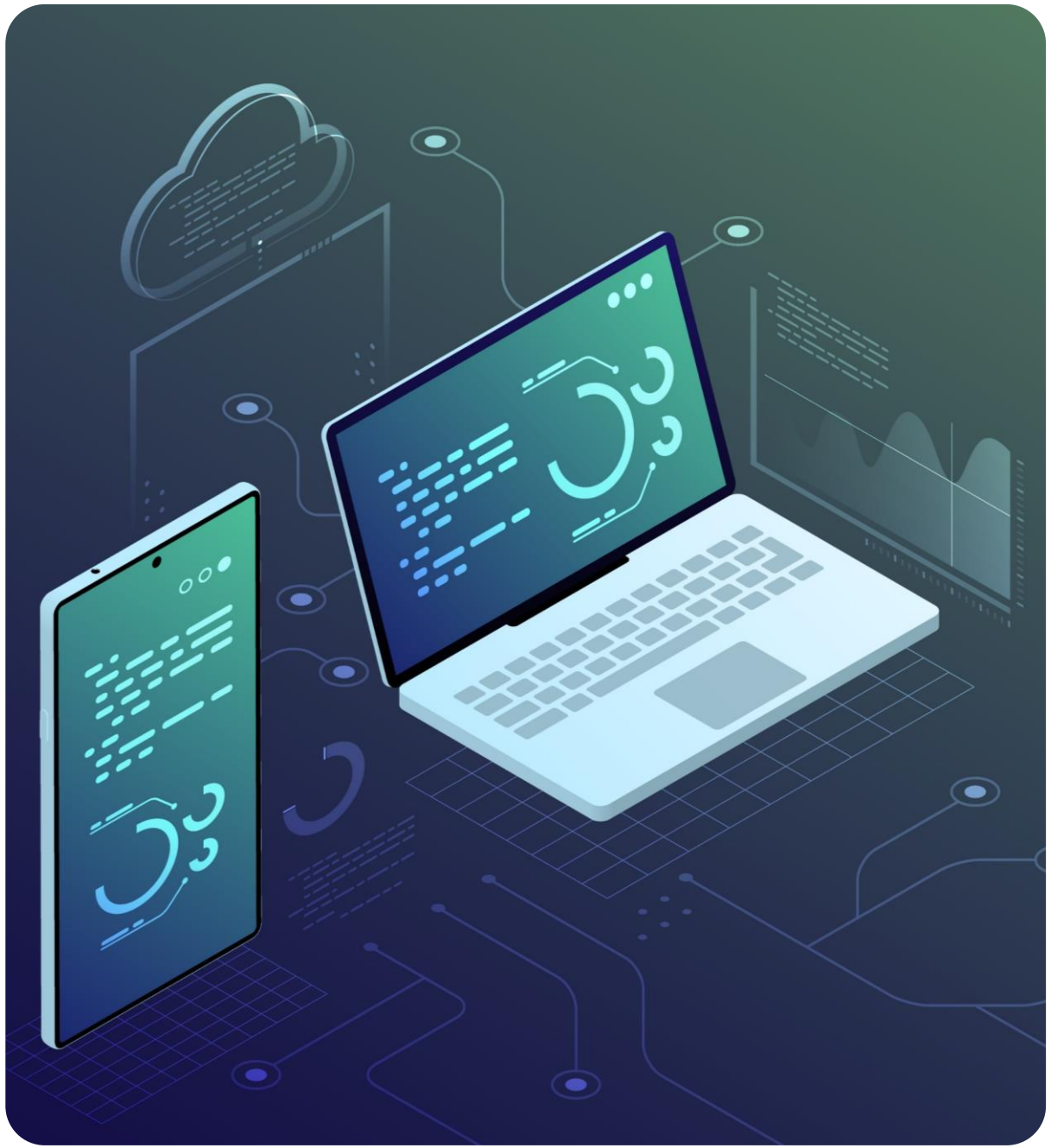
For barcode 34977079780722284

AWS X-Ray


Service map
Clients
avg. 625ms
18 t/min
selfies-processor-demo
AWS::Lambda
avg. 26.3s
34 t/min
selfies-processor-demo
AWS::Lambda::Function
avg. 39.6s
19 t/min
selfies-table2
AWS::DynamoDB::Table
avg. 2.28s
34 t/min
AmazonRekognition
AWS::AmazonRekognition

AWS X-Ray Traces

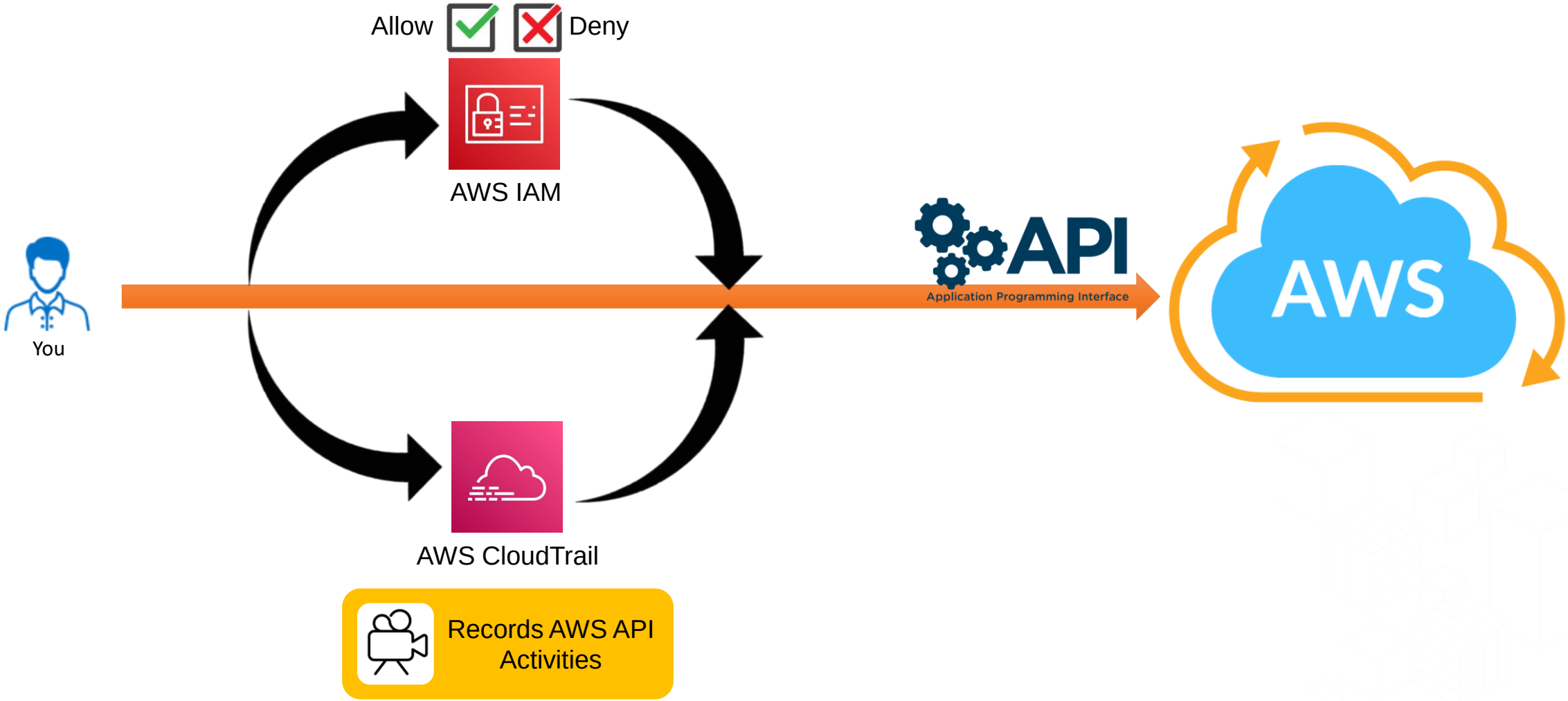




AWS CloudTrail

Security Camera

Flow of a request to AWS



AWS CloudTrail

- CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, SDKs, CLI, and other AWS services.

- CloudTrail helps identify who or what took which action, what resources were acted on, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

- Logs API call to AWS endpoints
  - Success and Failure
  - Can store logs information in Amazon S3 bucket
  - Supports cross account, cross region

Concepts

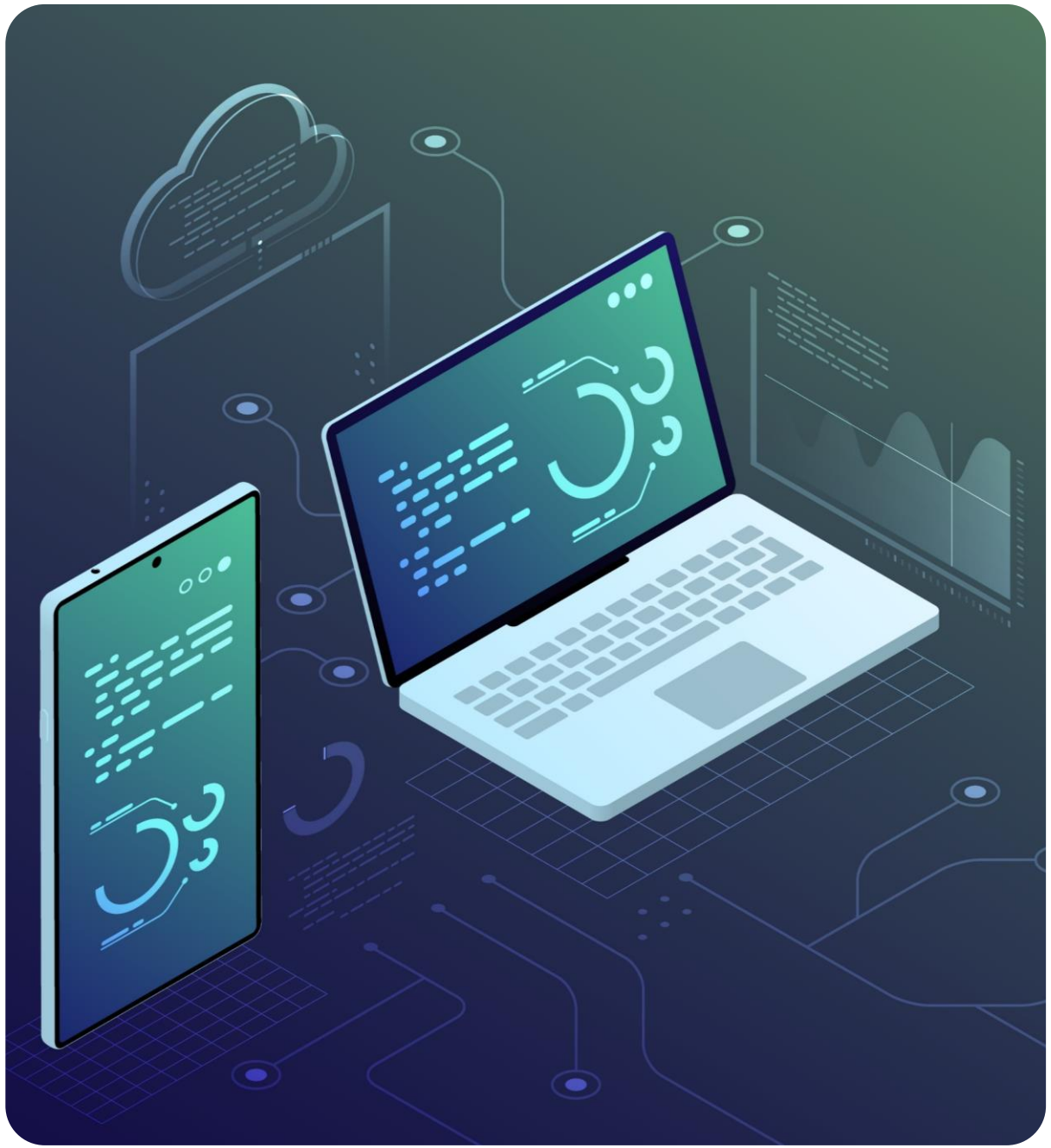
- Events - An event in CloudTrail is the record of an activity in an AWS account.
  - There are three types of events that can be logged in CloudTrail:
    - Management events – Control Plane operations
    - Data events – Data plane operations performed on supported resource
    - CloudTrail Insights events – Capture unusual activity in your AWS account

- Trails - A trail is a configuration that helps deliver events to an S3 bucket that you specify.
  - You can also deliver and analyze events in a trail with CloudWatch Logs and CloudWatch Events.

CloudTrail Tutorial 

Best Practices

- Configure CloudTrail Logs to be delivered to a central S3 bucket in a separate AWS account.
- Configure MFA-delete on the Amazon S3 bucket storing log files.
- Configure versioning on the Amazon S3 bucket storing log files.
- Configure server-side encryption for CloudTrail log files.
- Configure log file validation for CloudTrail.

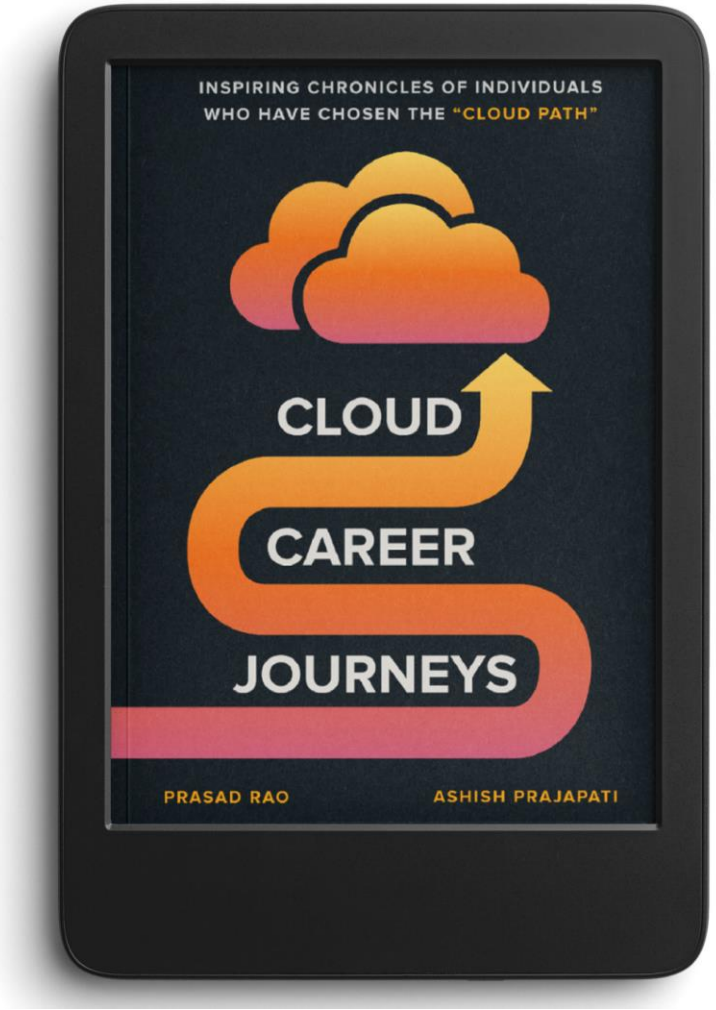


Pricing in AWS

How do you pay for AWS?

- Pay-as-you-go
- Save when you commit
- Pay less by using more

Giveaway Sponsors



and WHIZLABS

Giveaways

Limited to first 50 buyers

- 50% discount on – Cloud Career Journeys – eBook
- 50% discount on – Cloud Career Journeys – Starter Kit
  - **(QR Code displayed at the end of the session)**

Weekly Giveaways **(Selection based on engagement)**

- 1 x Cloud Career Journeys – eBook
- 10 x Whizlabs Sandbox Access for 3 months

12th Week Giveaways (Selection from regular participants)

- 10 x Whizlabs Premium Plus Subscription for 12 months

Week 03 Winners

Cloud Career Journey ebook	• Shreya Singh
Whizlabs 3 months AWS Sandbox Access	• Omotola Agbomabiwon • Asma Akram • Abhishek Vishwakarma • Smitanjali Mishra • Afeez (Olalekan) Azeez • Carlos Arriaga Luna, MS. • Omolade Akinwumi • YouTube handle - @0512g • YouTube handle - @hyderabadperlmongers3654

Note to winners: Please **reach out to besaprogram2022@gmail.com** with your preferred email address so we can facilitate your access.