Building & Implementing a Robust Monitoring Strategy

Brian Carlson
Operational Excellence Lead
Well-Architected Program

10/18/2019

aws

Why are we here?

In order to help you…

- Gain insights for business & operations
- Achieve situational awareness
- Enable proactive courses of action
- Provide timely & effective responses
- Achieve their business outcomes

Why do you need a monitoring strategy?

Why do you need a monitoring strategy?

- Failing to plan is planning to fail…
- You cannot manage what you do not measure
- A monitoring plan defines what is measured

Does monitoring need your attention?

Have you ever…

…been asked how are you supposed to monitor in the cloud

…been asked how to get visibility into serverless workloads

…struggled with not knowing why a workload has issues

…seen the same operations issue happen regularly

…been asked which monitoring tool is better

Then you probably need to work on building a monitoring strategy.

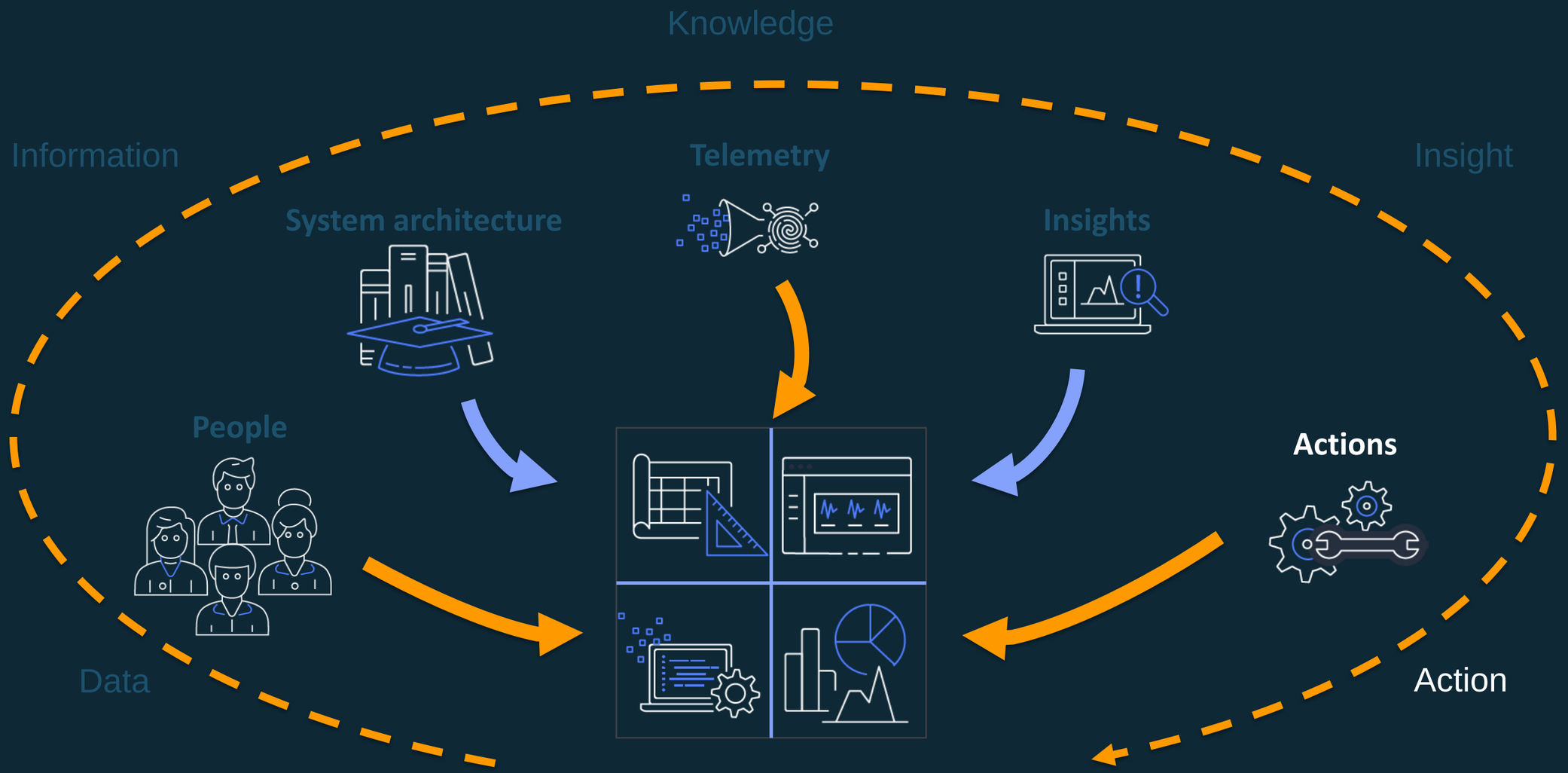
aws

What is a Monitoring Strategy?

And how do you build one?

aws

What goes into a monitoring strategy?



Categories of insight

Faults

Outcomes

Configuration

Accounting

User behavior

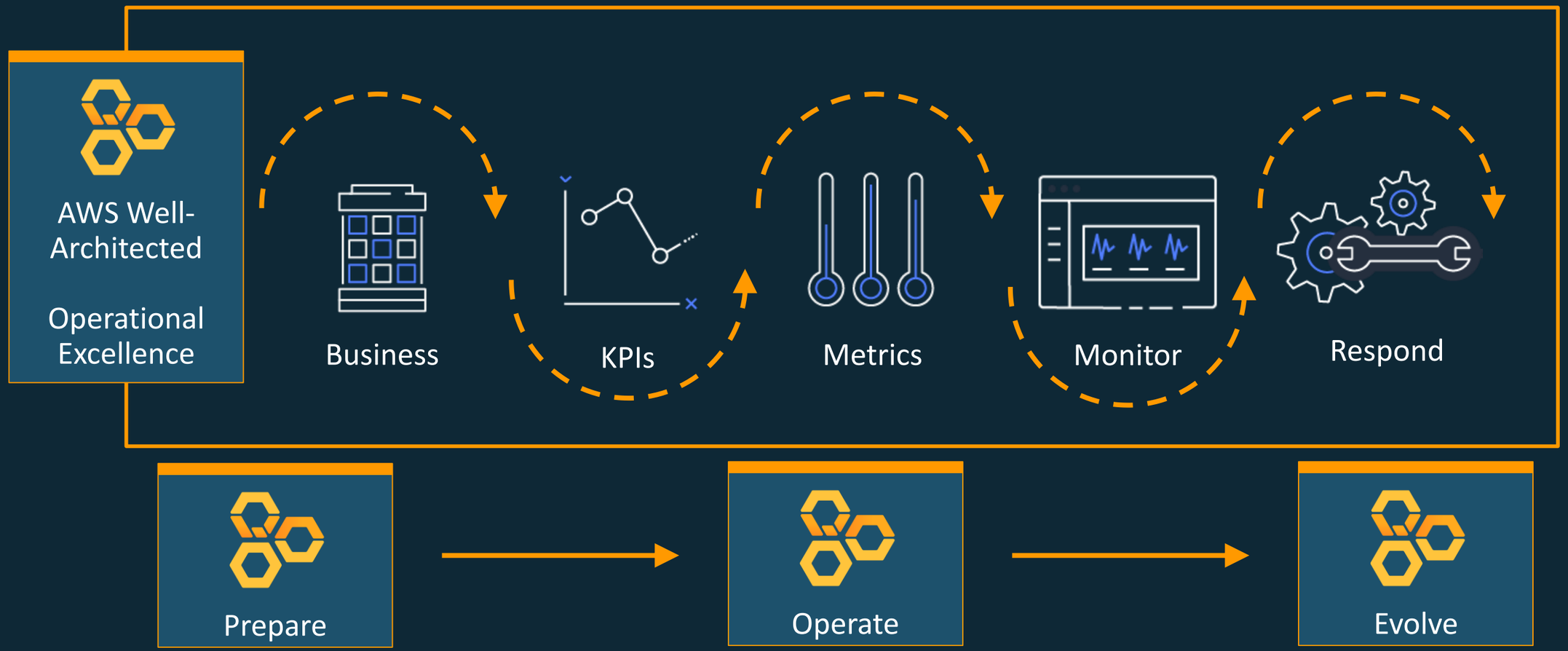
Performance

Security

Workload behavior

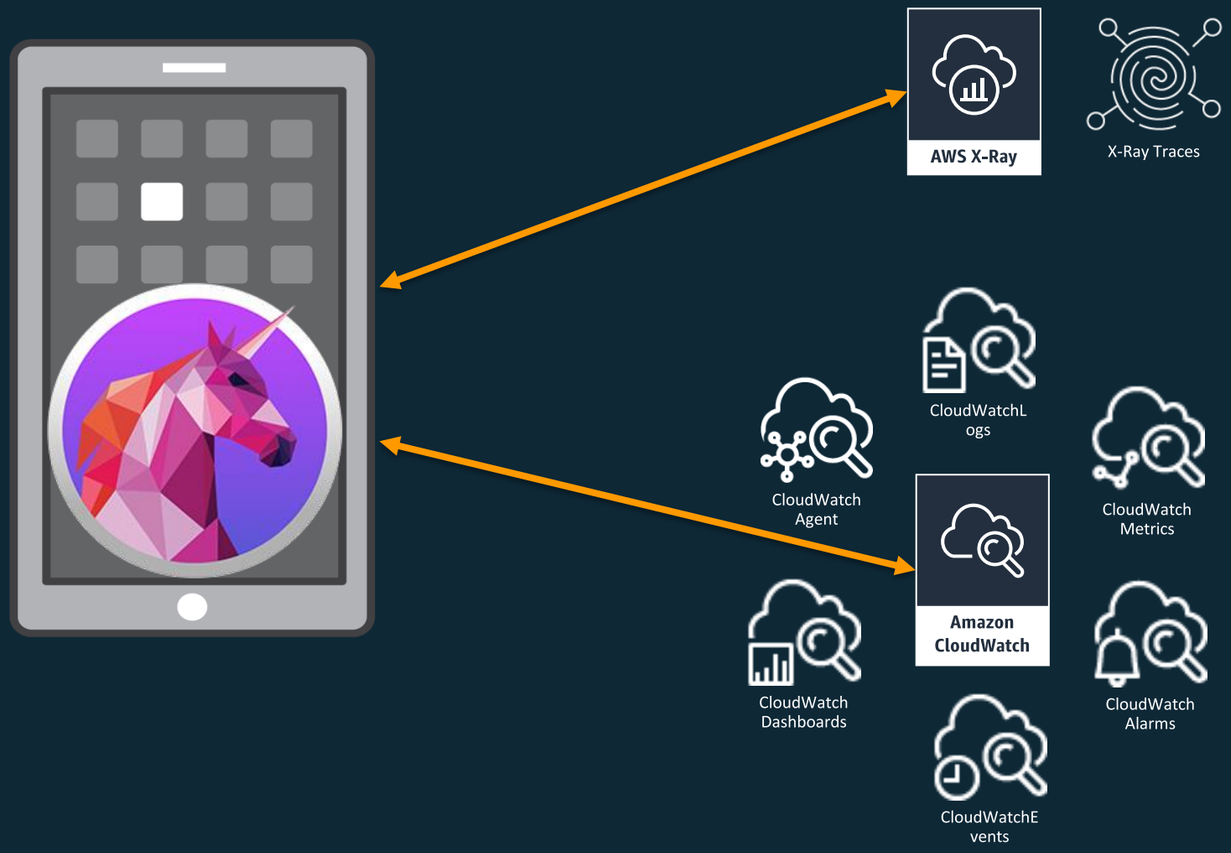
aws

What is the workflow to build a strategy?



Time for a quick poll

AWS services that support observability



AWS X-Ray

Amazon CloudWatch

Building a Monitoring Plan

Personas and requirements

Personas and Needs			
Role	**Contact**	**Responsibility**	**Requirements**
CEO	Isobel Rose	Funding	Business level view of operations
CIO	Henry Pomfret	Service Delivery	Application delivery and service availability
Infrastructure	Meloni Blank	Security and Reliability	Compliance
Application	Joanne Groan	Quality of the customer experience	Measures of application performance
InfoSec	Aki Nguyen	Infosec and Security	Compliance
DevOps	Roger Brandish	Application Health	Application health
DevOps	Sasha Batcliff	Monitoring and Incident Response	Effective alerts and responses
Security	Paco Simpson	Security	Security situational awareness
User	Cindy Logan-Matthew	Functional Features	Customer behavior
Financial	Cris Stamp	Opex	Spend
And many more…			

Key Performance Indicators

Key Performance Indicators (KPIs)						
Underpinning Business Outcome	**KPI**	**Desired Outcome**	**How it is measured**	**What good look like**	**Time to Action if KPI at risk**	**Action Taken**
Quality Customer Experience	Support Reponse Time	Response within 8 business hours	Time from first contact to first response	Response time less than 8 hours	4 hours after first contact	Escallation
Quality Customer Experience	Initial application launch time	Page load within 15 seconds	Page request to page delivery	Average Page load within 15 seconds over 5 minutes	Immediate	Raise an event
Quality Customer Experience	Application Response Time	Image analysis transaction response within 2 seconds	Initiation (click) to result presented	Avergage Transaction response within 2 seconds over 10 minutes	Immediate	Raise an event
Quality Customer Experience	Accuracy of Image and Text identification	90% confidence	Confiidence results from Rekognition	Average of 90% confidence over 1000 unique images	Next Development Sprint	Create issue
Quality Customer Experience	Image upload time	TBD	Initial to completion	Customer doesn't get frustrated	Monthly	Evaluate circuit capacity
And many more…						

System architecture and insights

System Knowledge and Insights					
Workload	**Component**	**Sub-component**	**Insights**	**Telemetry**	**Source**
Imagetrends	Application Server	Operating System	Faults	logs	/var/log/message
Imagetrends	Application Server	Boot log	Faults	logs	/var/log/boot.log
Imagetrends	Application Server	CPU	Performance	standard metrics	CPU utilization
Imagetrends	Application Server	Memory	Performance	standard metrics	Memory utilization
Imagetrends	Application Server	Disk I/O	Performance	standard metrics	Disk I/O utilization
Imagetrends	Application	Errors	Security	logs	/opt/imagetrends-logs/ui/application.log
Imagetrends	Application	Warnings	Performance	logs	/opt/imagetrends-logs/ui/application.log
Imagetrends	Application	User activity	User behavior	logs	/opt/imagetrends-logs/ui/application.log
Imagetrends	Application	Production logs	Accounting	logs	/opt/imagetrends-logs/ui/production.log
Imagetrends	Network	Network activity	Security	VPC Flow Logs	VPC Flow Logs
And many more…					

aws

Thresholds for testing

Metrics and Thresholds "What does good look like?"						
Workload	**Component**	**Sub-component**	**Metric**	**Test**	**Thresholds**	**Source**
Imagetrends	Application Server	Operating System	non-kernel boot errors	successful boot	0 boot errors	/var/log/message
Imagetrends	Application Server	Boot log	unplanned reboot	unclean shutdown in logs	0 unclean shutdowns	/var/log/boot.log
Imagetrends	Application Server	CPU	max utilization	is CPU 100%	100% > 15 min	CPU utilization
Imagetrends	Application Server	Memory	memory available	% remaining	< 10% for more than 5 min	Memory utilization
Imagetrends	Application Server	Disk I/O	IOPs	IOPs > minimum app required	< 10,000 IOPs during write	Disk I/O utilization
Imagetrends	Application	Errors	number of errors	error uploading files	< 1 upload error per session	/opt/imagetrends-logs/ui/application.log
And many more…						

aws

Reporting

Reporting and Trending			
Subscribers / Personas	**Topic**	**Queries**	**Format(s)**
Finance, Budget Manager	Cost and Usage Reports	Billing alarms and projected usage	Business level view of operations
CEO, Sales, Ops Teams	User Activity and Volume	Active sessions and utilization	Application delivery and service availability
CEO, Ops Teams	Uptime Rating	Component availability & Overall Uptime	Compliance
Ops Teams, Dev Teams, QA	Session Latency	User transactions and tracing	Measures of application performance
CIO, App Owner, Bus. Owner, Ops Teams	Application Health	Current health check status on components	Application health
Bus. Owner, Ops Teams	Monitoring and Incident Response	Current alarms and open incidents	Effective alerts and responses
CISO, Audit, Compliance, CIO	Security & Compliance Status	Patch compliance status and violations	Security situational awareness
And many more…			

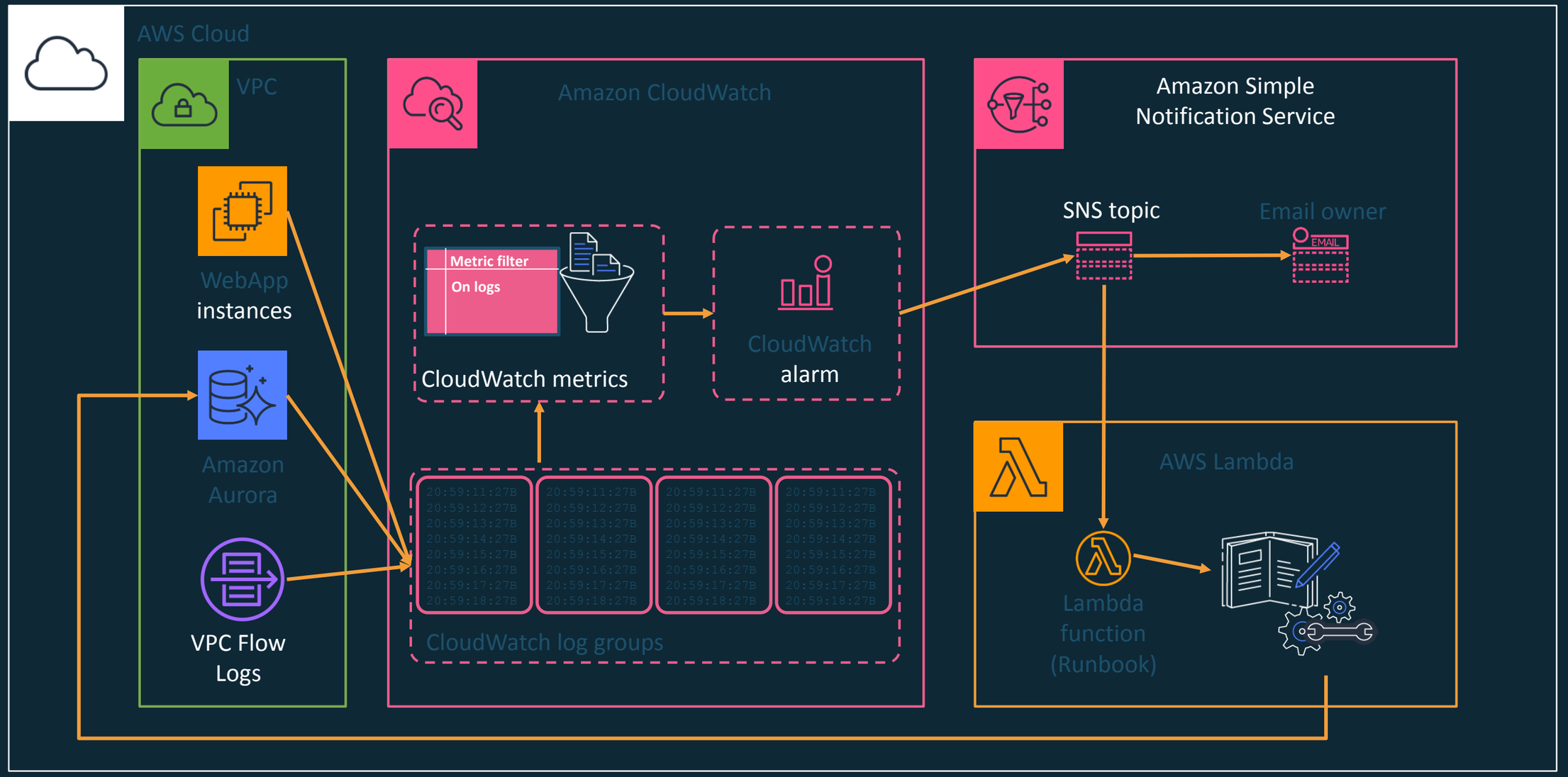
Alerts and actions

Events and Alerts					
Component	**Area**	**Criticality**	**Condition to Alert on**	**Owner**	**Action**
Application	Fault	Critical	More than 0 image errors	Ops	Delete the bad image
Application	Fault	High	Investigate Error	Dev	Event management/determine if a further response is required
Application	Security	Normal	Investigate Warning	Dev/Security	Event management/determine if a further response is required
Application	Accounting	Medium	Trending to Exceed Budget	Dev/Ops/LOB	Determine why and then determine action
Application	Performance	Normal	Investigate cause	Dev/LOB	Prioritize backlog
And many more…					

Time for a quick poll

Implementing Monitoring

Workflow of monitoring action for Imagetrends



The Lab

https://workshop.aws-management.tools/cloudwatch/

Time for a quick poll

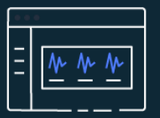
Establishing metrics

- Configure logs to be centralized

- Setup filters aligned to business outcomes

- Generate logs through user activity

- **Verify the metrics are working as designed**



aws

Alerts and notifications

- **Alerts should be tied to business outcomes**

- Only alarm *when actions are required*

- Actions *must* be documented (runbooks)

- Runbooks should be reviewed & updated

aws

Responding to events

- Document known issues with workload

- Determine the corrective action(s)

- **Build a runbook for corrective action(s)**

- Automate the corrective action runbook(s)

aws

What have you learned and what should you do now?

Plan

- Recognize the signs that monitoring strategy needs improvement
- Focus on understanding business outcomes first
- Walk through each of the steps to develop a monitoring plan

Do

- Implement the plan to gain insight into the workload
- Ensure there is understanding of when business outcomes are at risk
- Improve MTTD and MTTR through automation

Q&A

Thank you!

Brian Carlson