GRACE HOPPER CELEBRATION

ANITA B.ORG

GRACE HOPPER CELEBRATION

ANITA B.ORG

SP713: Security Forecast: Is It Cloudy? #GHC19

Security Forecast: Is It Cloudy?

Using Serverless technologies to more effectively and efficiently secure your cloud environment

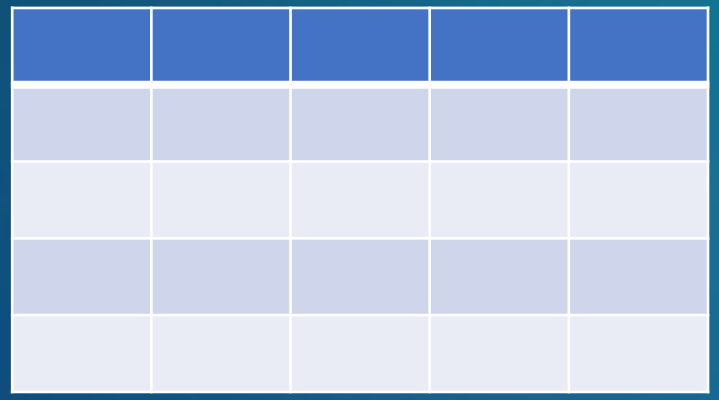
Brittany Doncaster
Principal Cloud Security Architect

Roadmap

- Traditional Security
- New Tech - Serverless
- Reference Architectures and Patterns

What is it?

Traditional Security



- Spreadsheets
- Standards Documents
- Checklists
- Tools, tools, and more tools

What makes it hard?

Traditional Security

- Manual
- Error Prone
- Expensive
- Not Enforceable

Often leads to….

Traditional Security

Move Fast

Secure

Automation!

What is Serverless?

New Tech - Serverless

Scalable

Reliable

No Management

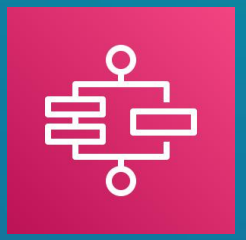
Serverless Services

New Tech - Serverless

AWS Lambda

Serverless Compute

- Supports multiple languages
- Executes on given trigger
- Limited run-time



AWS Step Functions

Serverless Orchestration

- Workflow around Lambda functions
- Error handling
- Traceability
- Various constructs for logic flows like parallel, choice and map

Serverless in Security

New Tech - Serverless

Allows us to perform security tasks with more:

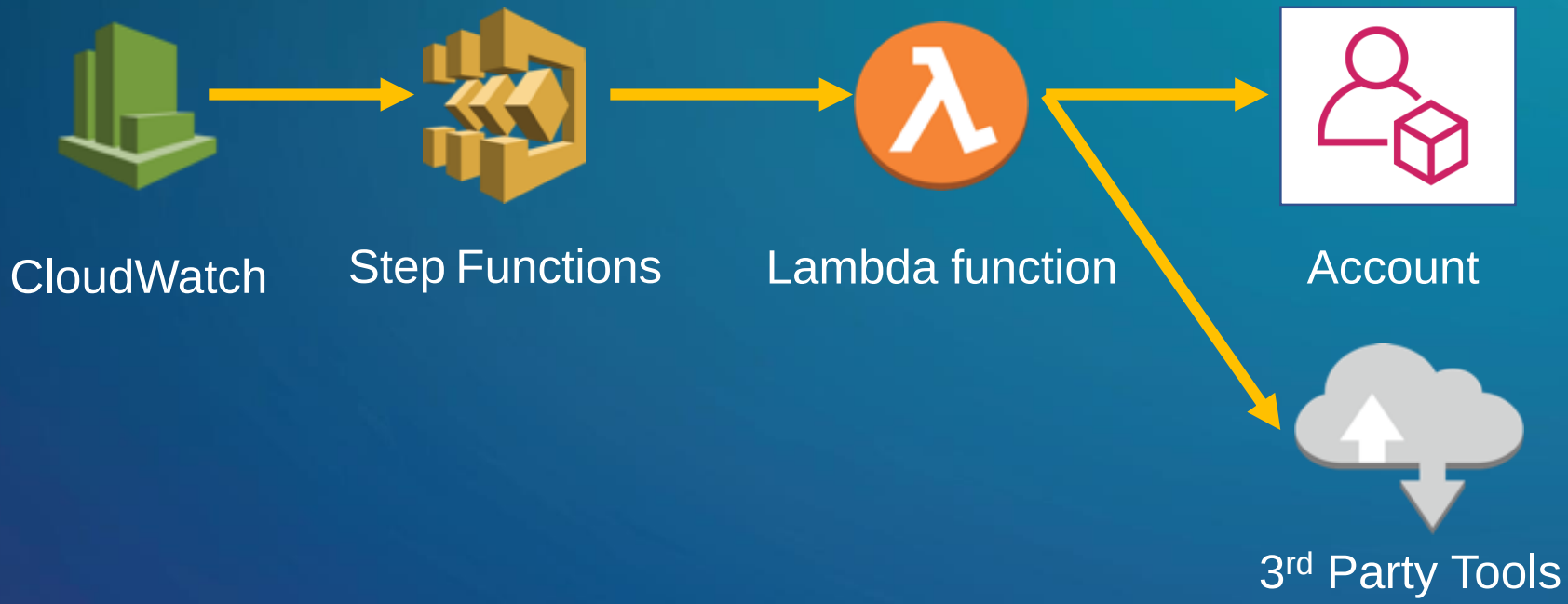
- Reliability
- Efficiency
- Scalability

What kinds of tasks can serverless help with?

- Directive: controls establish the governance, risk, and compliance models on AWS.
- Preventive: controls protect your workloads and mitigate threats and vulnerabilities.
- Detective: controls provide full visibility and transparency over the operation of your deployments in AWS.
- Responsive: controls drive remediation of potential deviations from your security baselines.

Directive Controls

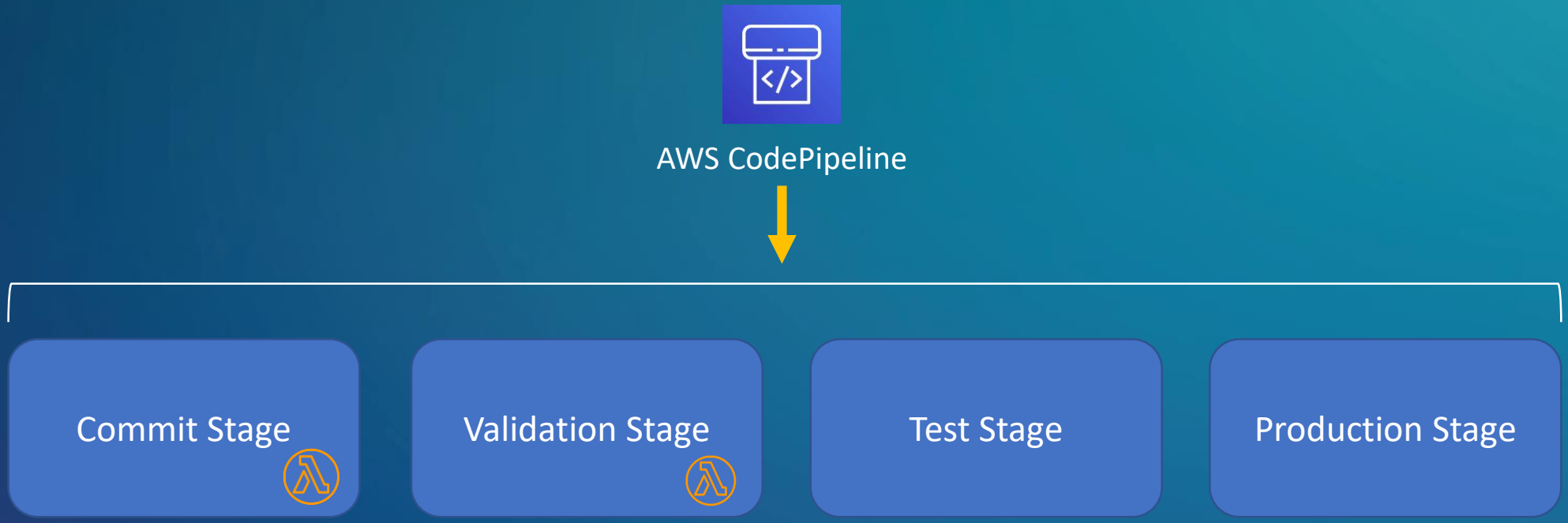
Reference Architectures and Patterns



Use Cases:

- Your other controls – preventive, detective, responsive
- Tool integration– notification of new accounts

Preventive Controls



Example Use Cases:

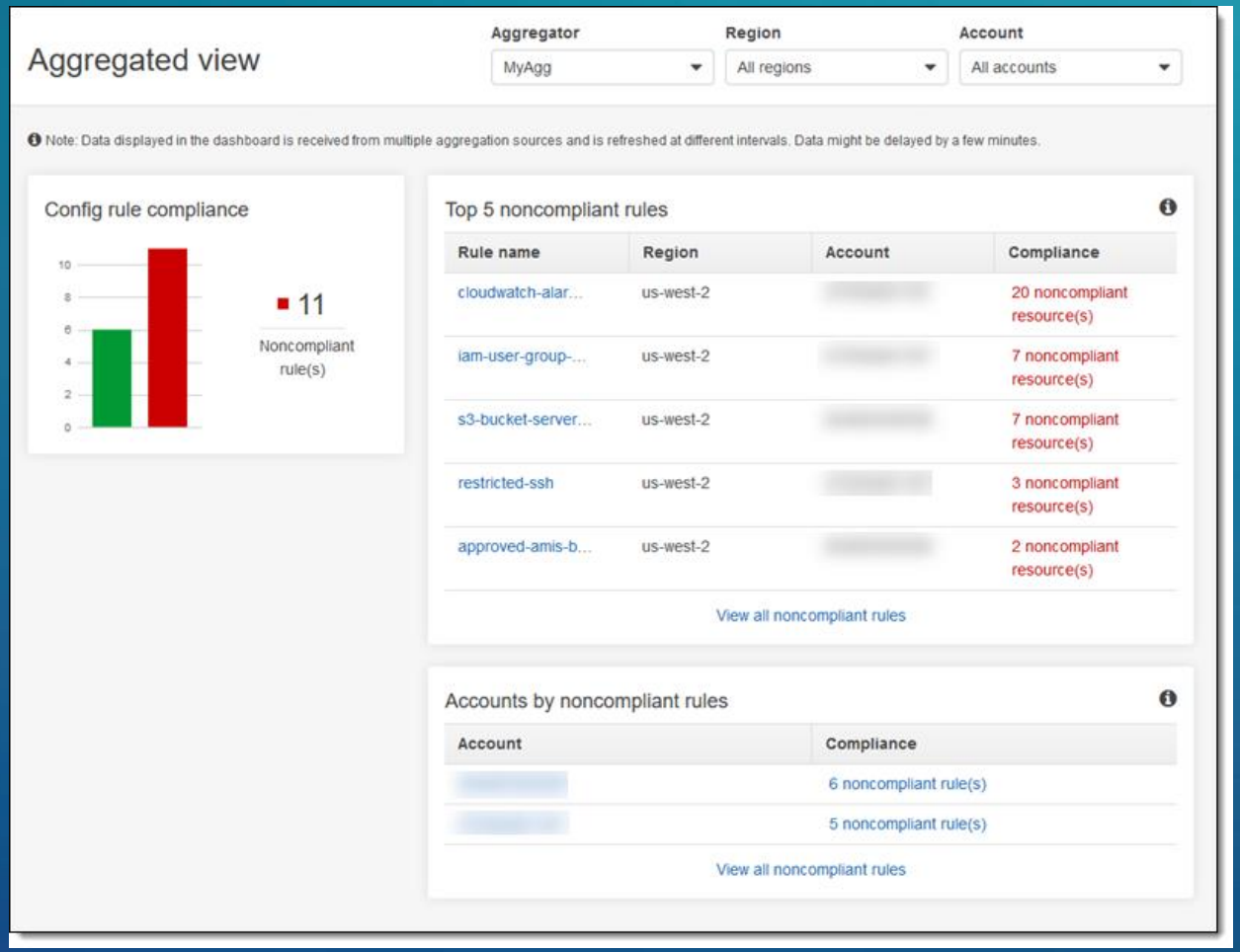
- Static Code Analysis
- Compliance with Security Policies (firewall rules, encryption, IAM user restrictions, access policies)

Detective Controls

AWS Config Lambda function

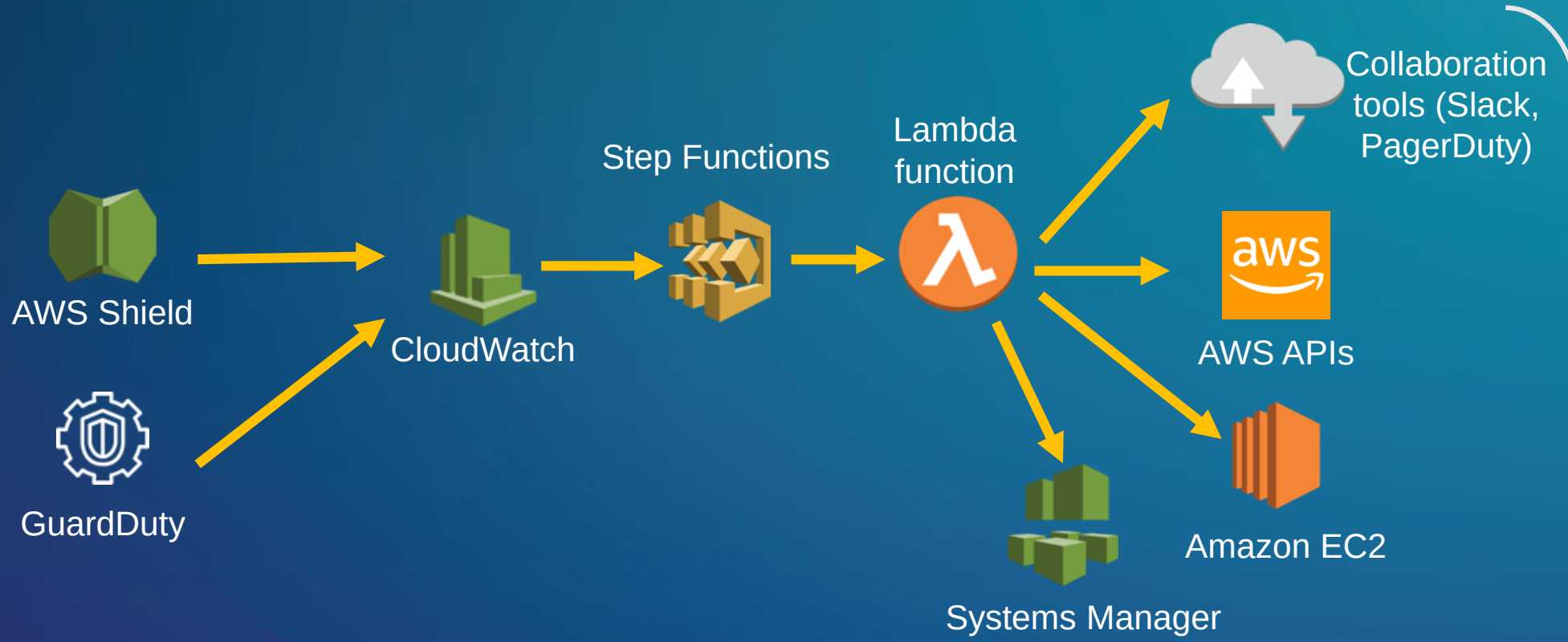
Example Use Cases:

- Custom continual compliance checks
  - Check for encryption on databases, messaging streams, etc. with custom keys
  - IAM access key rotation/usage
- Event-driven or scheduled



Responsive Controls

Reference Architectures and Patterns



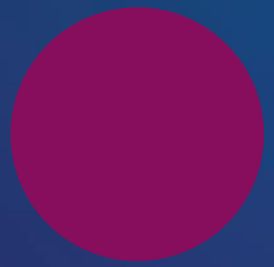
Example Use Cases:

- Notify DRT team of DDoS attack
- Shutdown access to a compromised EC2 instance, revoke compromised IAM privileges
- Isolate a compromised EC2 instance and use Systems Manager to capture memory and save it off for forensics
- With Step Functions do multiple at a time (alert personnel, enact countermeasures, start forensics capture)

Remember…

Automation is Key

Security engineering is no longer spreadsheets, it's code!



Serverless makes it easier

Using Serverless lets you automate without adding to your operational burden

Controls, Controls, Controls

Look for ways to automate your controls whether they are directive, preventive, detective or responsive.

Please remember to complete the session survey in the mobile app.

THANK YOU

@britdoncaster

brittany-doncaster

GRACE HOPPER CELEBRATION

ANITA B.ORG

#GHC19