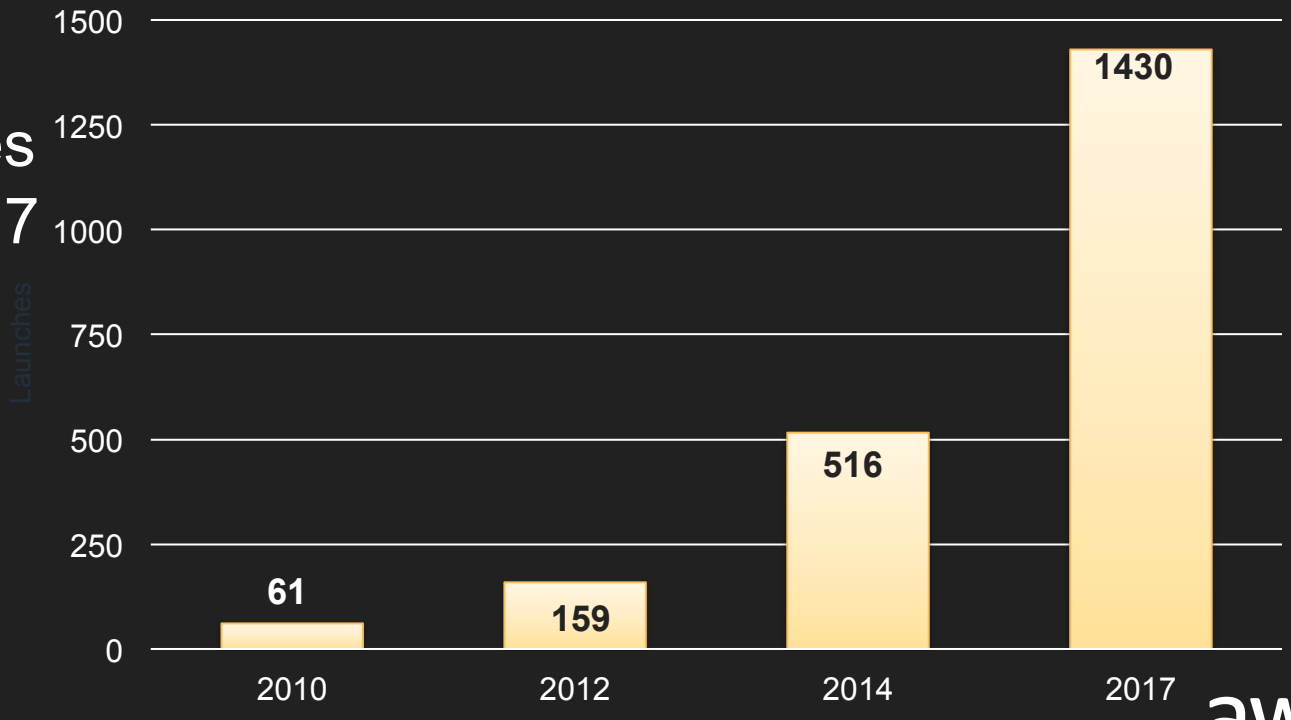
@MargoCronin
Senior Solutions Architect
Amazon Web Services

aws

AWS Pace of Innovation

1,430 new features/services launched in 2017



Deployments at amazon.com

11.6s	1,079	10,000	30,000
Mean time between deployments (weekday)	Max number of deployments in a single hour	Mean number of hosts simultaneously receiving a deployment	Max number of hosts simultaneously receiving a deployment

Terminology Disclaimer

```
import re
re.search('([Dd]ev[Ss]ec|[Ss]ec[Dd]ev|[Rr]ugged\s[Dd]ev)[Oo]ps')
```

=

Security automation

Terminology Disclaimer

```
import re
re.search('([Dd]ev[Ss]ec|[Ss]ec[Dd]ev|[Rr]ugged\s[Dd]ev)[Oo]ps')
```

=

Security automation

at scale

A fundamental principle of DevOps is **automation**!

People make mistakes

People bend the rules

People act with malice

Machines don't still

aws

4 steps to enable
Security automation
at scale

Step 1

Establish your level of Trust

Step 1 Establish your level of Trust….

Customer Managed Keys
Hardware Security Module

0

?

Customer Managed Keys
AWS Key Management Service

AWS KMS
AWS Managed Keys
AWS Secret Manager
AWS CloudHSM

100

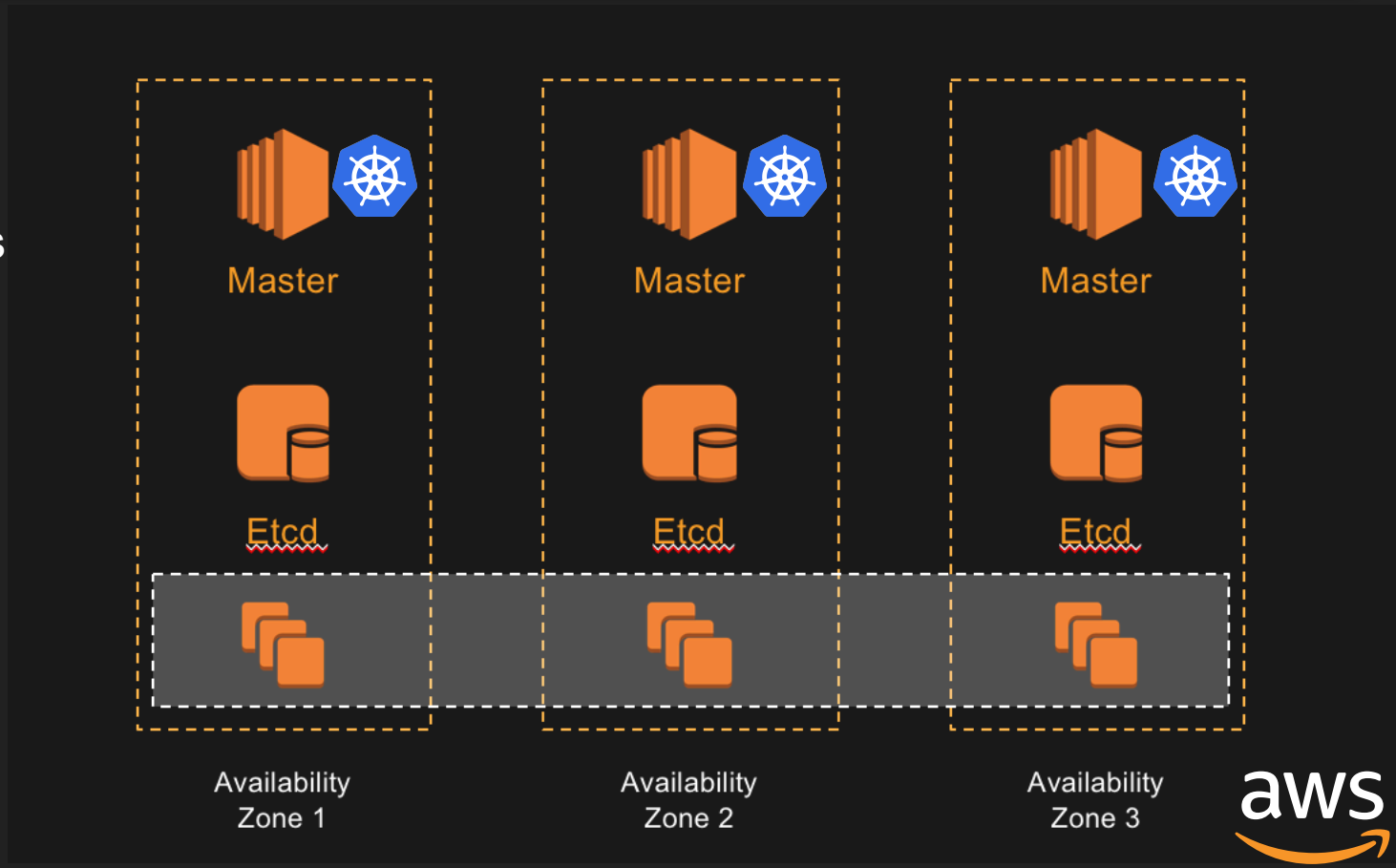
…. Select & configure your tools based on your level Trust

aws

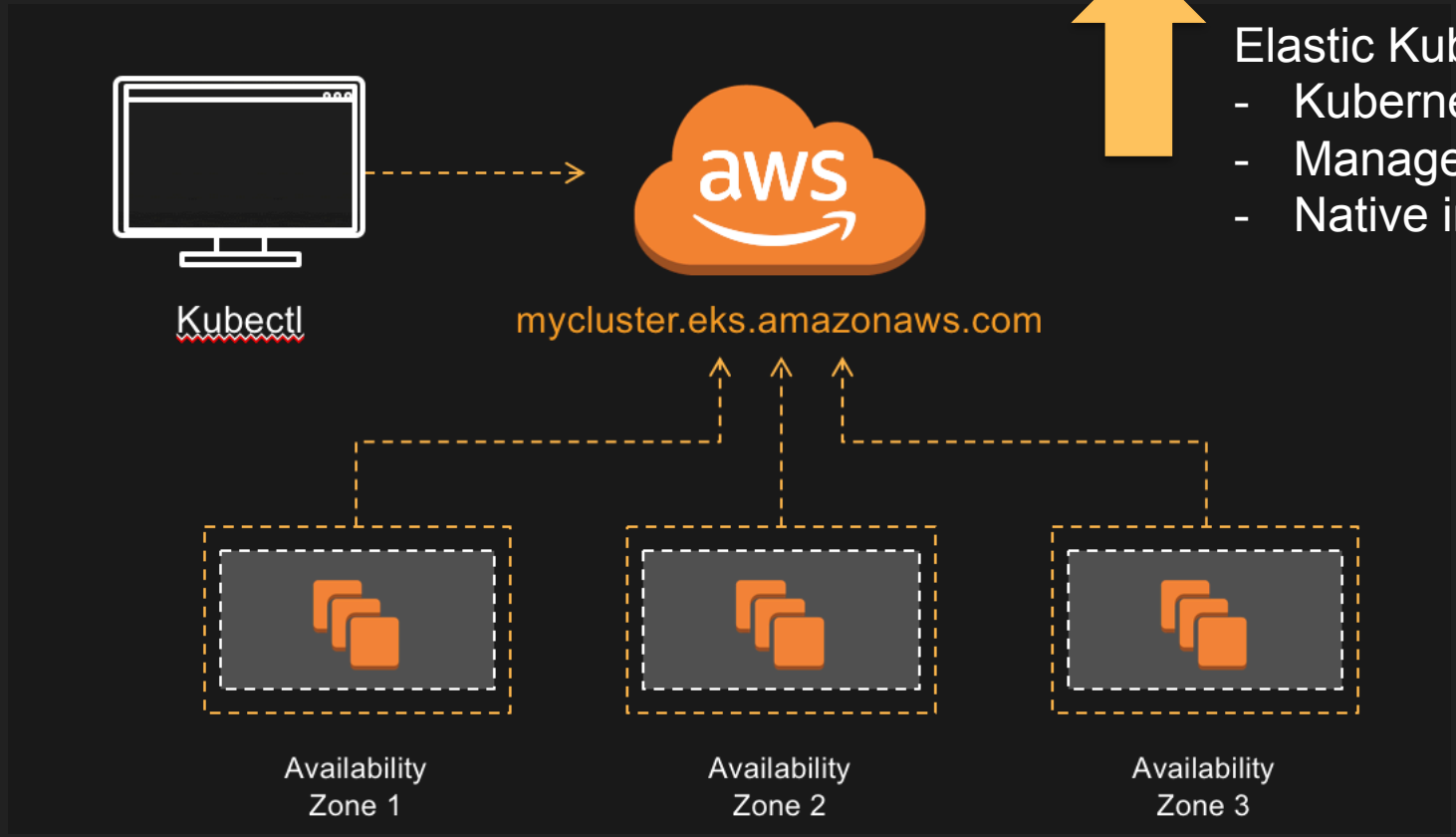
TRUST

0

Deploy Kubernetes Natively
You manage:
- Etcd
- Worker nodes
- Masters

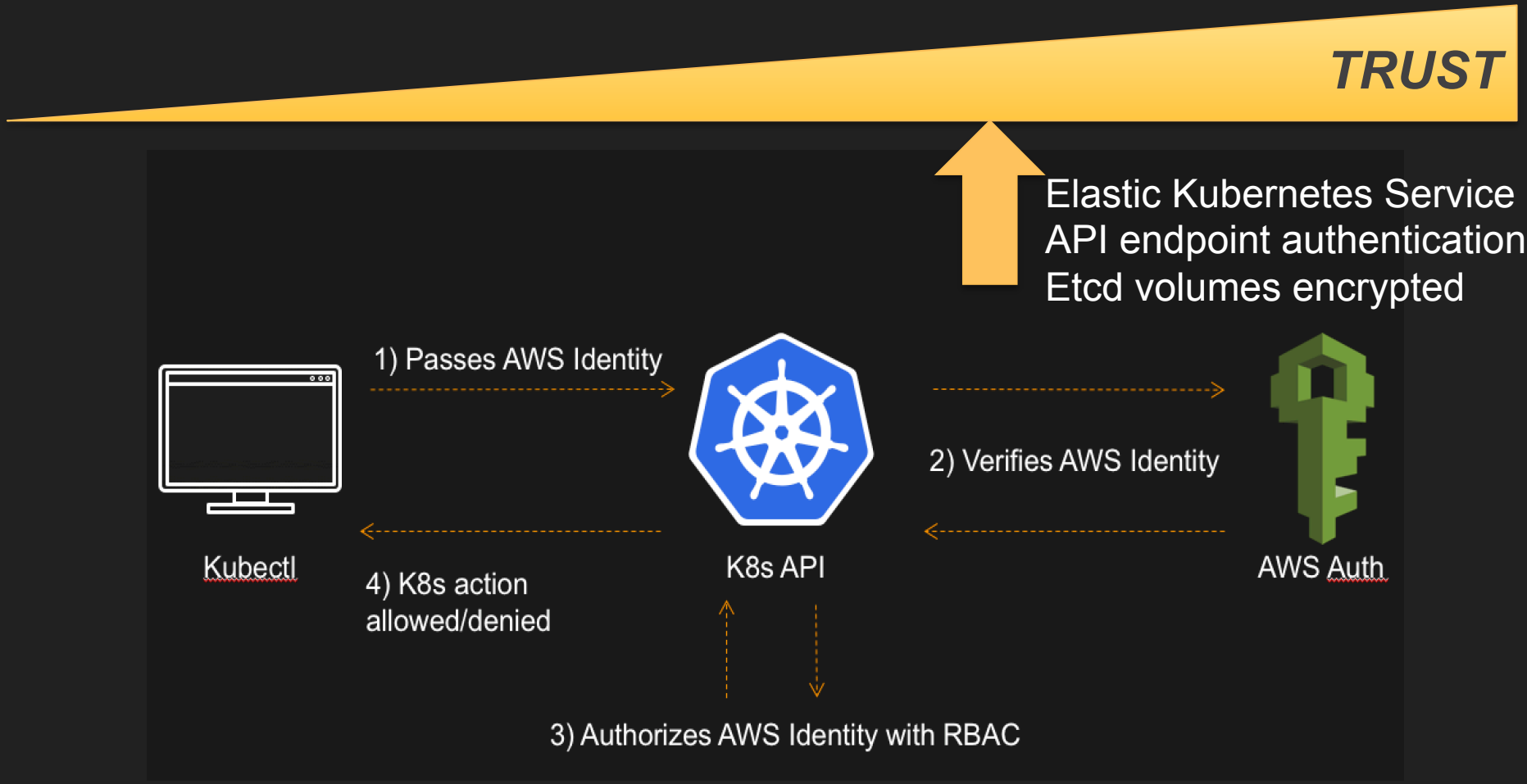


TRUST



Elastic Kubernetes Service
- Kubernetes endpoint
- Managed master nodes
- Native integration with AWS

aws


TRUST
Elastic Kubernetes Service
API endpoint authentication
Etcd volumes encrypted
1) Passes AWS Identity
2) Verifies AWS Identity
Kubectl
K8s API
AWS Auth
4) K8s action
allowed/denied
3) Authorizes AWS Identity with RBAC

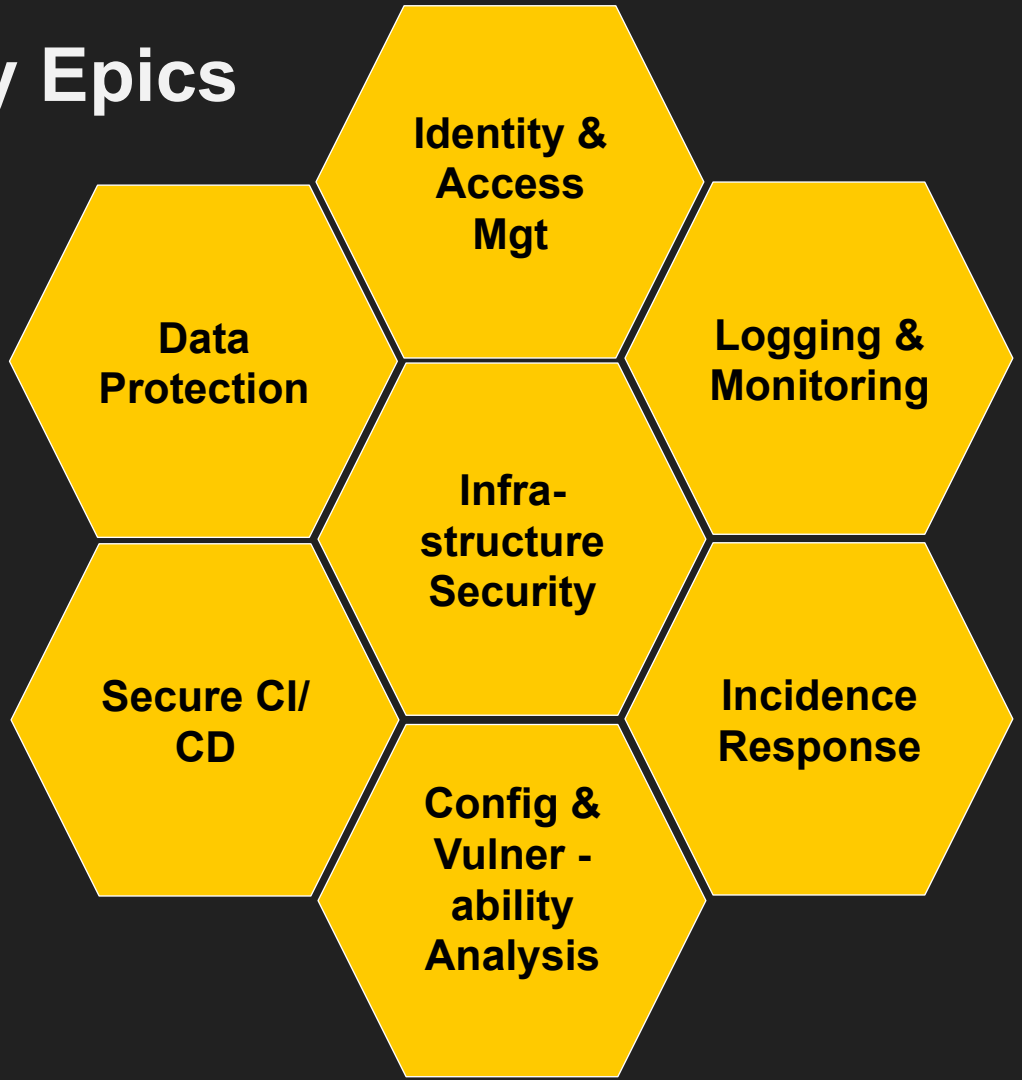
But no matter where you are on the trust scale, plan to integrate security automation

Step 2

Security by Design


Security
Ownership

Security Epics



Privacy by Design

- Every member of your team is a security owner
- Decompose Epics to functional stories
- Create security related acceptance criteria
- Same CI/CD pipeline to roll out security features

Step 3

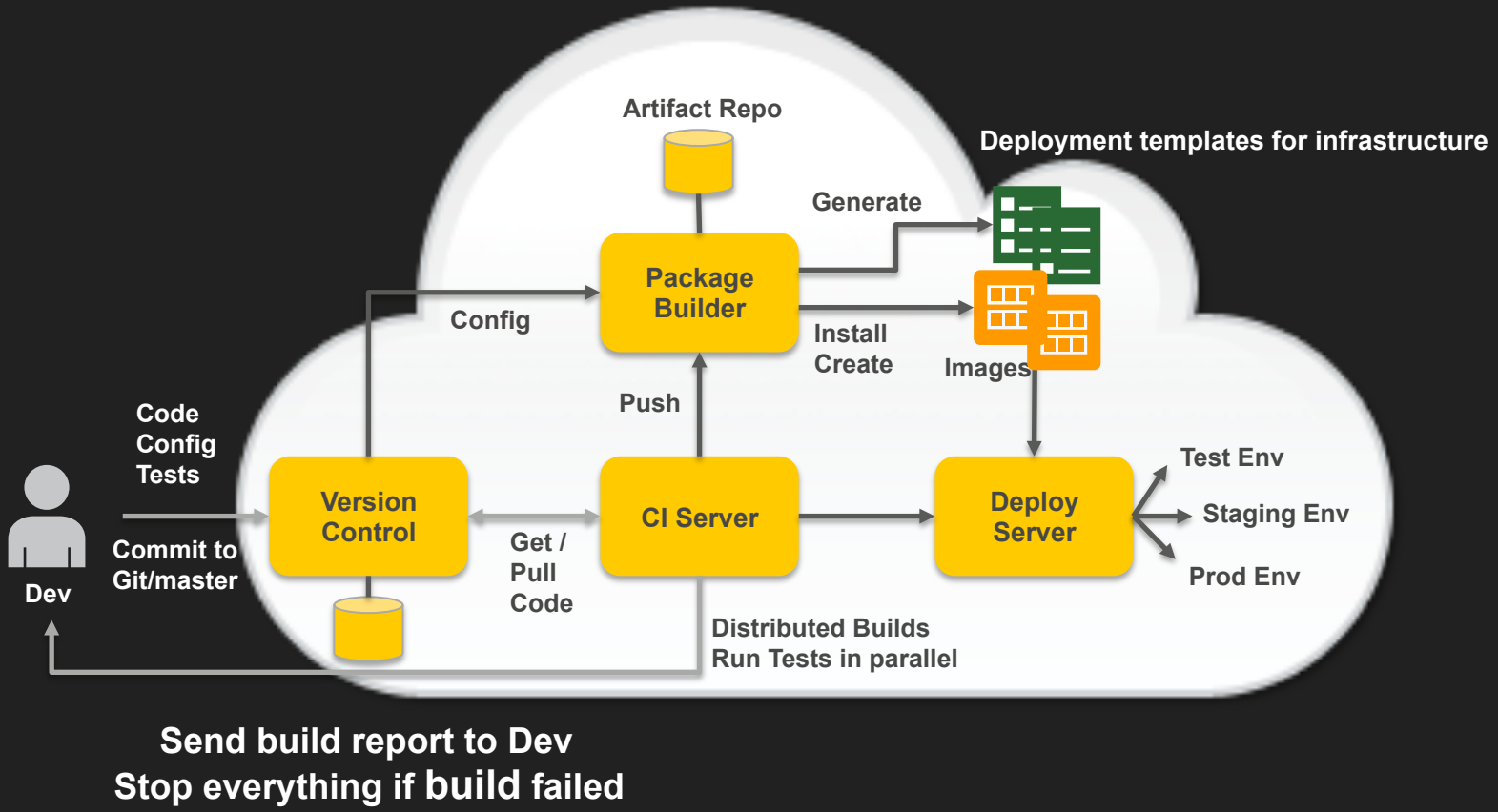
What are you securing?

Step 3 What are you securing

1. Security of the CI/CD Pipeline
   - Access roles
   - Hardening build servers/nodes

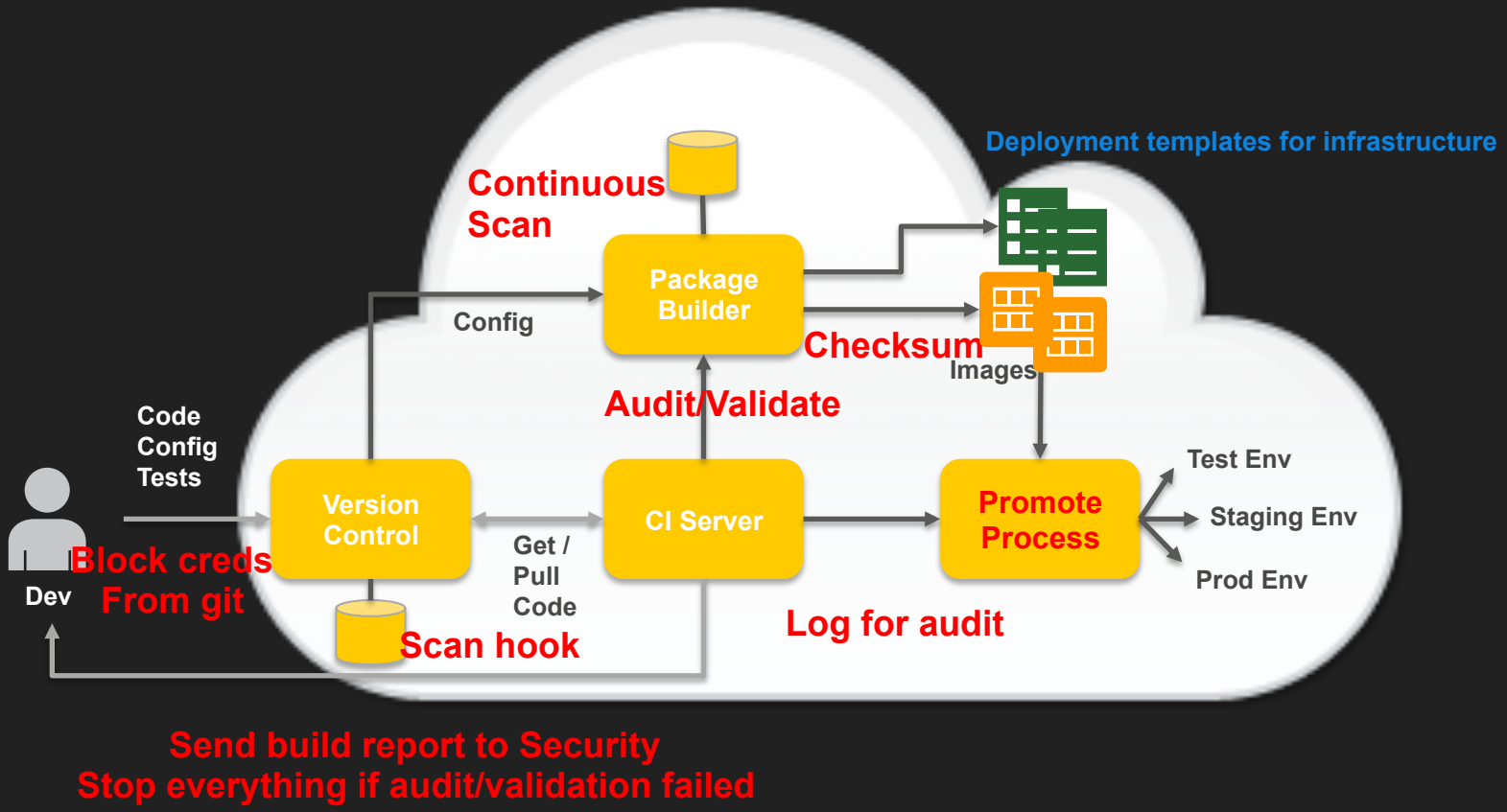
3. Security in the CI/CD Pipeline
   - Artifact validation
   - Static code analysis

CI/CD for DevOps

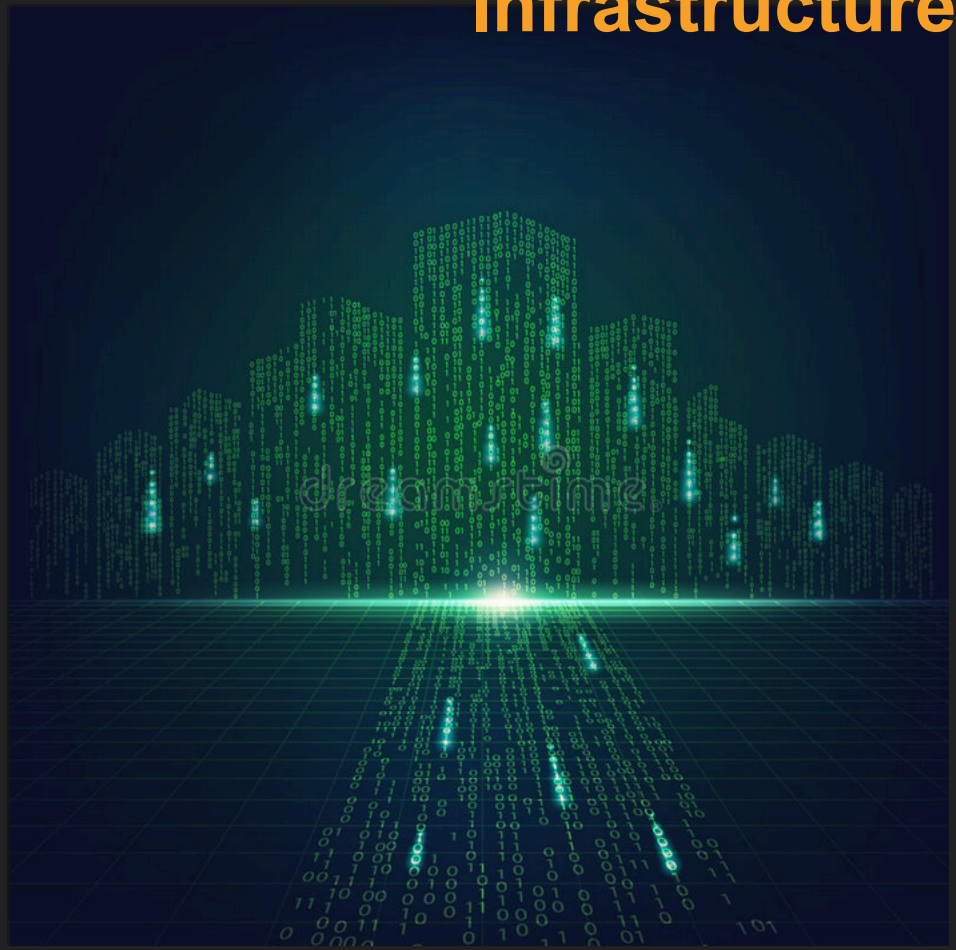


Send build report to Dev
Stop everything if build failed

CI/CD for DevSecOps



Infrastructure as Code



Write, Version, Store, Deploy your Infrastructure as Code

- AWS CloudFormation
- Terraform

Mean Time To Recover

Immutable infrastructure

aws

Step 4

Automate Responses


Long Love


Log Love


Event Log
Love


Log Love

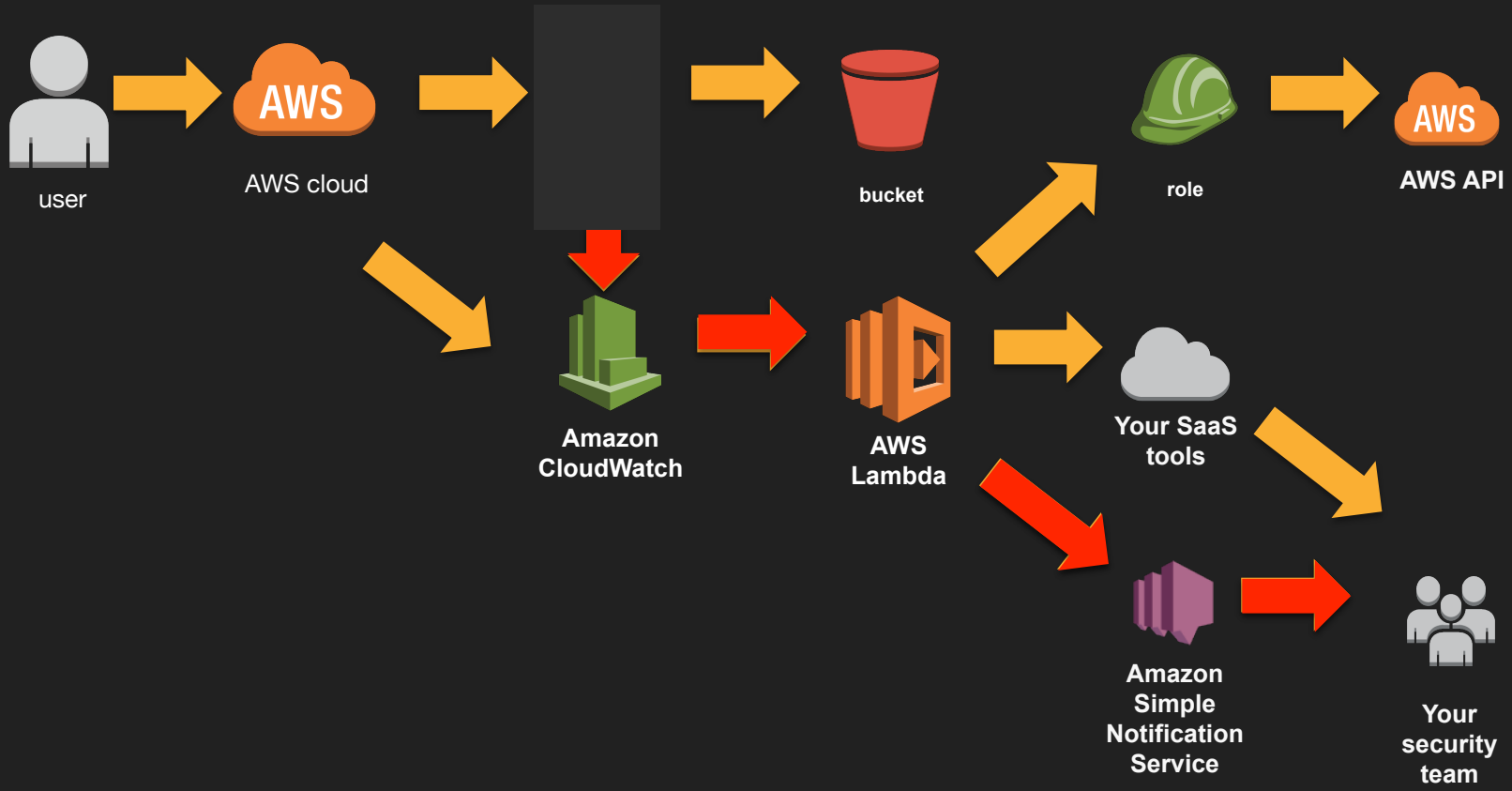
When are you collecting logs?

Why are you collecting logs?

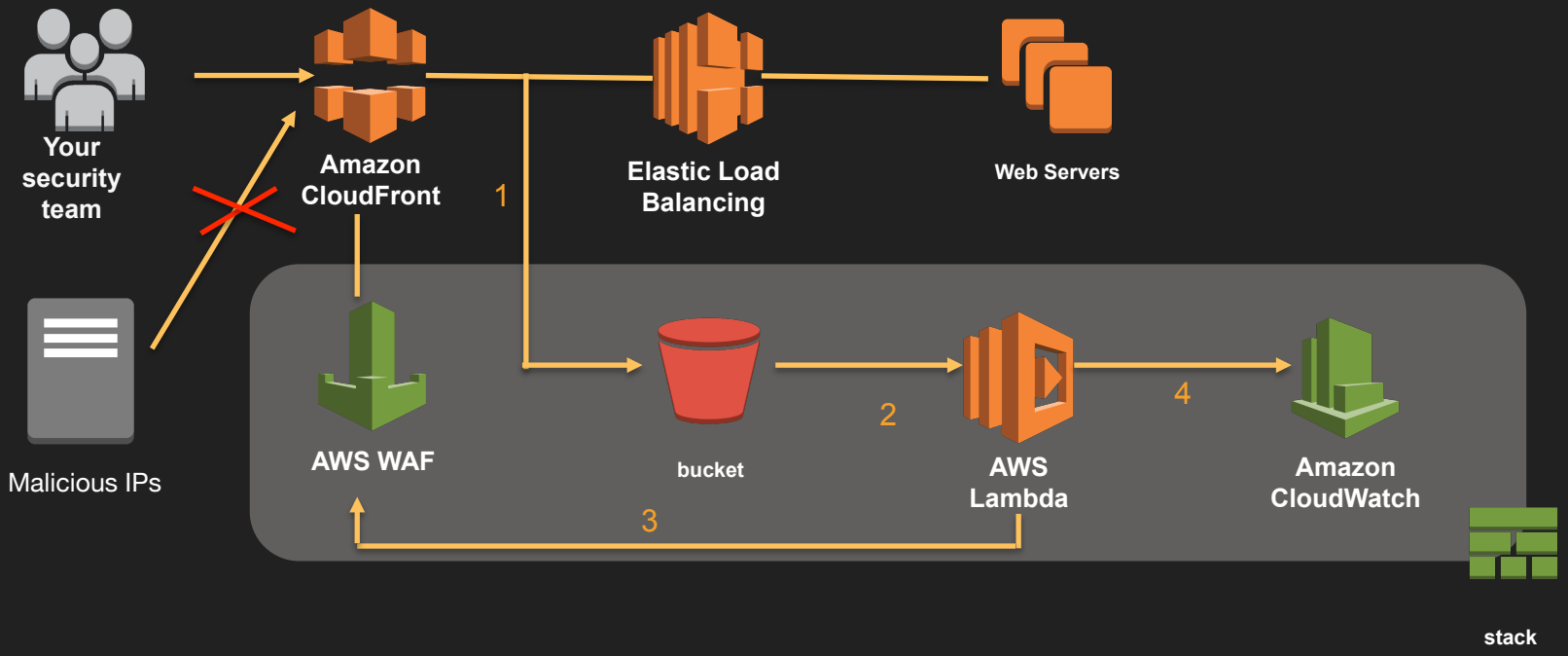
Where are you collecting logs?

What are you doing based on your logs?

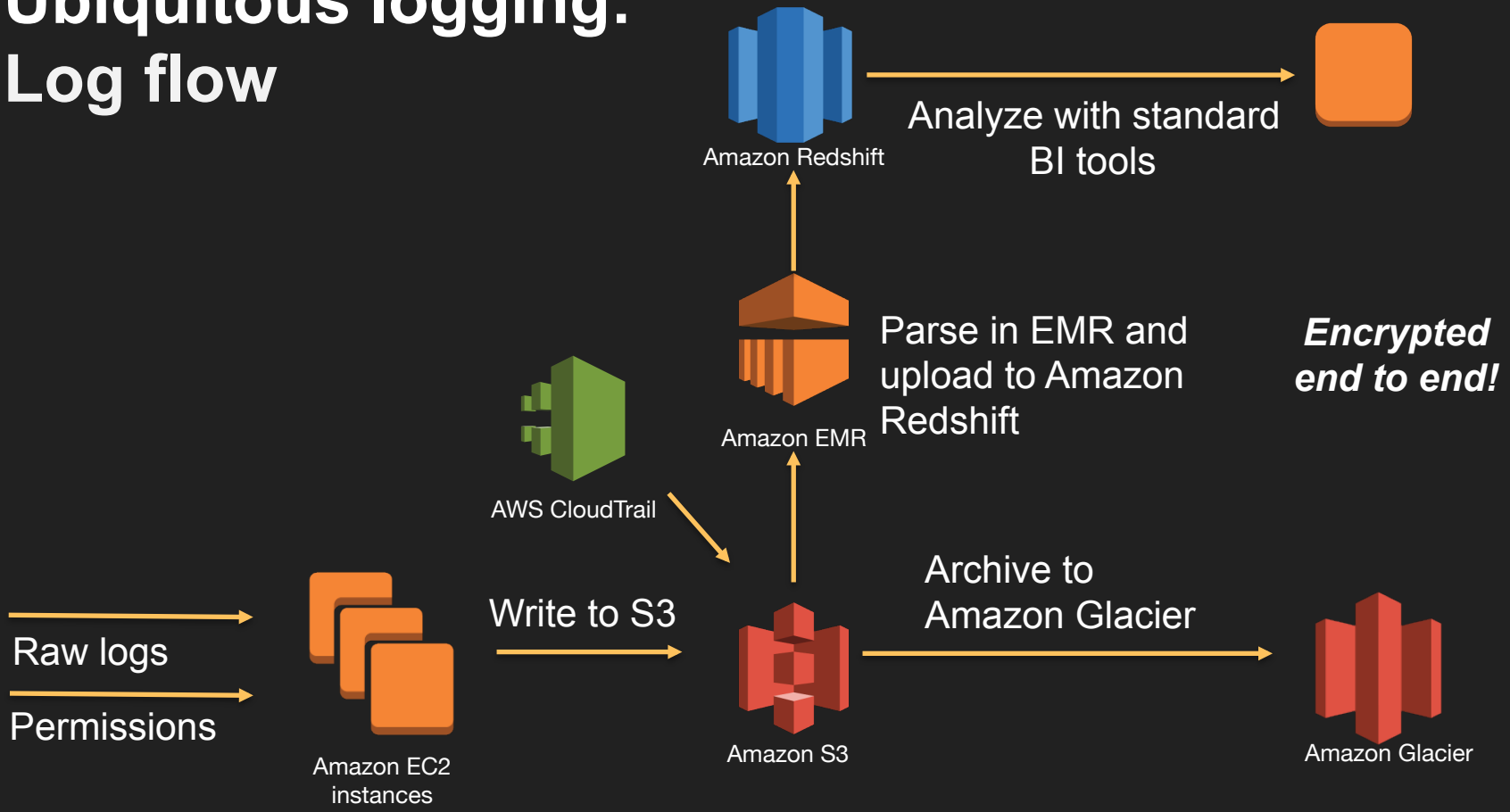
Putting it all together



Use logging services to prevent as well as protect



Ubiquitous logging: Log flow



Ubiquitous logging: What are we looking for?

- Unused permissions
- Overuse of privileged accounts
- Usage of keys
- Anomalous logins
- Policy violations
- System abuse

….

- Collect data once, many use cases

4 Steps to enable security automation at scale

- Establish your level of Trust
- Security by Design
- Security of and in the CI/CD pipeline
- Automated Responses

KEY TAKEAWAYS

Automation doesn’t sleep, eat, or need coffee in the morning

Ensure security in your DevOps practice by automating security at scale