Carnegie Mellon

institute for SOFTWARE RESEARCH

DevOps-Continuous Integration

Incident Handling

1

Carnegie Mellon University

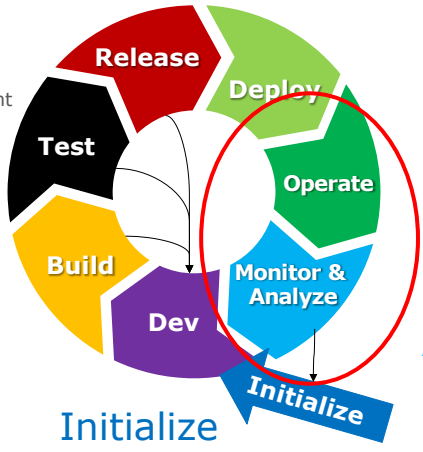
DEVOPS PROCESSES

Release
Approve for deployment

Test
Automate tests as much as possible

Build
Create an executable artifact

Dev
Perform normal development activities



Deploy
Move into production environment

Operate
Execute system and gather measurements about its operation

Monitor & Analyze
Display measurements taken during operation & analyze the data

Initialize
Select architecture to support other activities
Create scripts for other activities

© Len Bass 2021

institute for SOFTWARE RESEARCH

2

Carnegie Mellon University

Overview

- **Incident life cycle**
- Who performs incident response?
- What do responders look for?
- Post incident activities

© Len Bass 2021

Carnegie Mellon University

An incident occurs

- Incident - an event that could lead to loss of, or disruption to, an organization's operations, services or functions.
- In software terms – two different types of incidents:
  - Performance or availability problem with running system – topic of this lecture.
  - Security problem with network – handled separately.

© Len Bass 2021

Carnegie Mellon University

The incident is detected

- The incident is detected by a monitoring system. See https://youtu.be/h8YmtkZlspw if you don't remember
- The monitoring system has a collection of rules that determine when an incident has occurred.
- The monitoring system
  - sends out a page
  - Enters the incident in an incident repository

© Len Bass 2021

Carnegie Mellon University

Page is received

- The recipient:
  - Determines the immediate cause of the incident
  - Fixes the immediate cause so the system is operational again. This may involve assistance from others.
  - Records the immediate cause in the incident repository
  - Closes the incident.
  - Participates in post incident activities.

© Len Bass 2021

Carnegie Mellon University

Overview

- Incident life cycle
- **Who performs incident response?**
- What do responders look for?
- Post incident activities

© Len Bass 2021

Carnegie Mellon University

Two organizational models for incident response

- You Build it, You Run it. (Amazon)
- Site Reliability Engineering (SRE) model (from Google)

© Len Bass 2021

Carnegie Mellon University

You build it, you run it

"There is another lesson here: Giving developers operational responsibilities has greatly enhanced the quality of the services, both from a customer and a technology point of view. The traditional model is that you take your software to the wall that separates development and operations and throw it over and then forget about it. Not at Amazon. You build it, you run it. This brings developers into contact with the day-to-day operation of their software. It also brings them into day-to-day contact with the customer. This customer feedback loop is essential for improving the quality of the service."

-Wener Vogels

https://queue.acm.org/detail.cfm?id=1142065

Carnegie Mellon University

First responders

- In the Amazon model, the developers of a service wear the pagers.
- Rotated among members of the team that developed the service
- Each development team has its first responder at any point in time.

Carnegie Mellon University

Assumptions

- Members of the team developing the service understand the service best
- Problems with the service can be dealt with internally to the team
- The service that had the problem that caused the page is the cause of the problem.

Carnegie Mellon University

SRE

- Separate organizational unit to act as first responders
- Each application is assigned to a team within that unit.
- Teams can be responsible for multiple applications
- Teams have the option of refusing to support any particular application

Carnegie Mellon University

Assumptions

- SREs have an overall view of the application. This allows them to examine multiple services to determine problem.
- Development team listens and acts on SRE recommendations. This is the purpose of allowing an SRE team to refuse to support an application.
- SREs spend half of their time on call and half developing tools to support the SRE function.

© Len Bass 2021

Carnegie Mellon University

Overview

- Incident life cycle
- Who performs incident response?
- **What do responders look for?**
- Post incident activities

© Len Bass 2021

Carnegie Mellon University

Indicators

- Performance – latency and page load speed.
- Traffic – number of requests per unit time or number of users
- Availability – rate of failing requests or failing services
- Saturation – utilization of various resources

© Len Bass 2021

Carnegie Mellon University

SLxs

- SLA – Service Level Agreement. What is guaranteed to clients (internal or external) for each indcator
- SLO – Service Level Objective. A goal for the team for each agreement.
- SLI – Service Level Indicator. Measurement of the objective. For each indicator, define an SLI and alert when it is violated.

© Len Bass 2021

Carnegie Mellon University

Overview

- Incident life cycle
- Who performs incident response?
- What do responders look for?
- **Post incident activities**

© Len Bass 2021

Carnegie Mellon University

After system is operational

- Determine root cause of the incident and record it in incident repository.
- Fix or recommend fix for root cause.
- Examine incident repository for repeated or common incidents.
- Examine overall system performance data for bottlenecks. Fix or recommend fix to bottleneck.

© Len Bass 2021

Carnegie Mellon University

Summary

- Incidents occur when something is wrong with the system
- Monitoring systems trigger alerts based on performance, availability, traffic, and utilization measures
- First responders fix immediate problem
- Post incident activities help prevent future problems.

© Len Bass 2021