Introduction to Software Development

Week 3 Day 3

Led by: Emily Crose

for

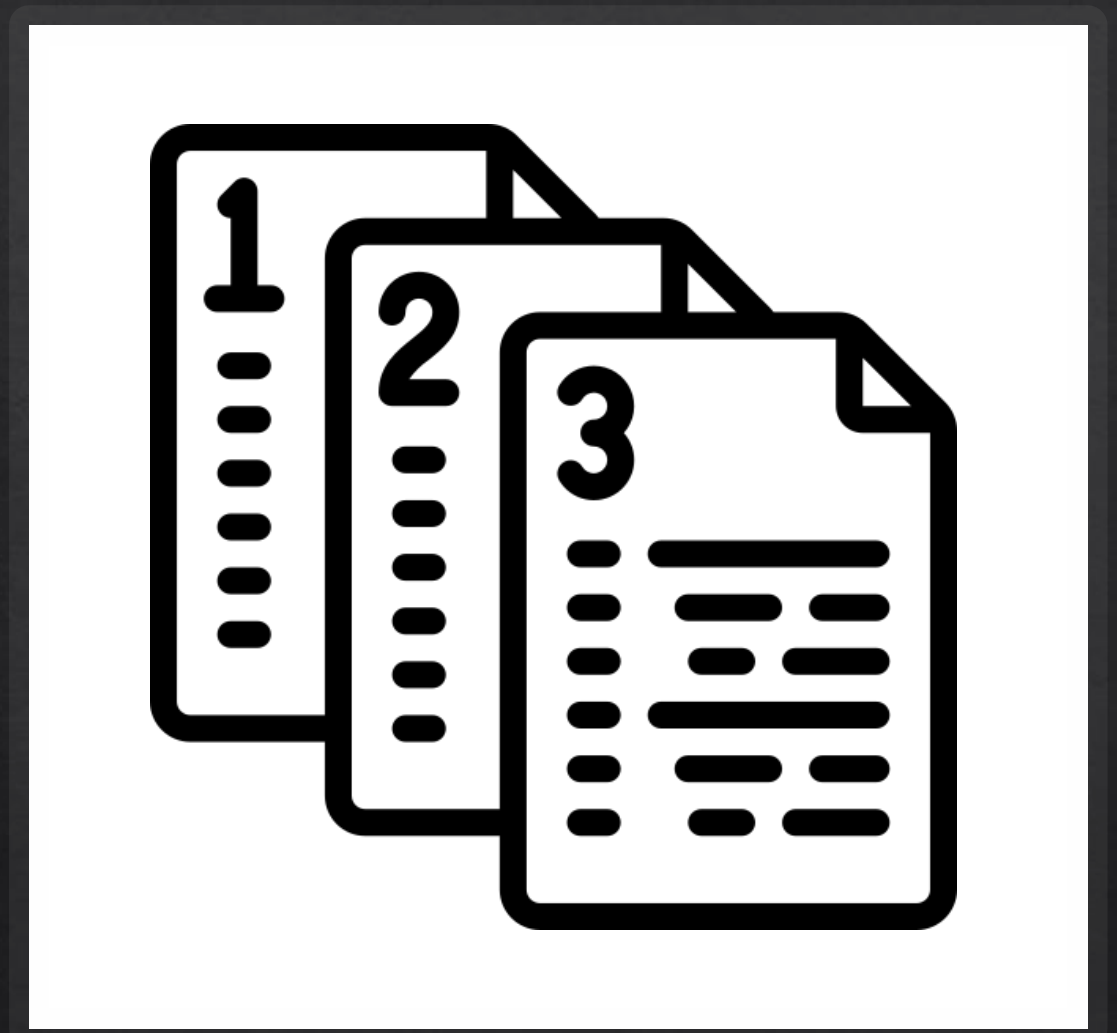
Oakland University

Last Session Recap

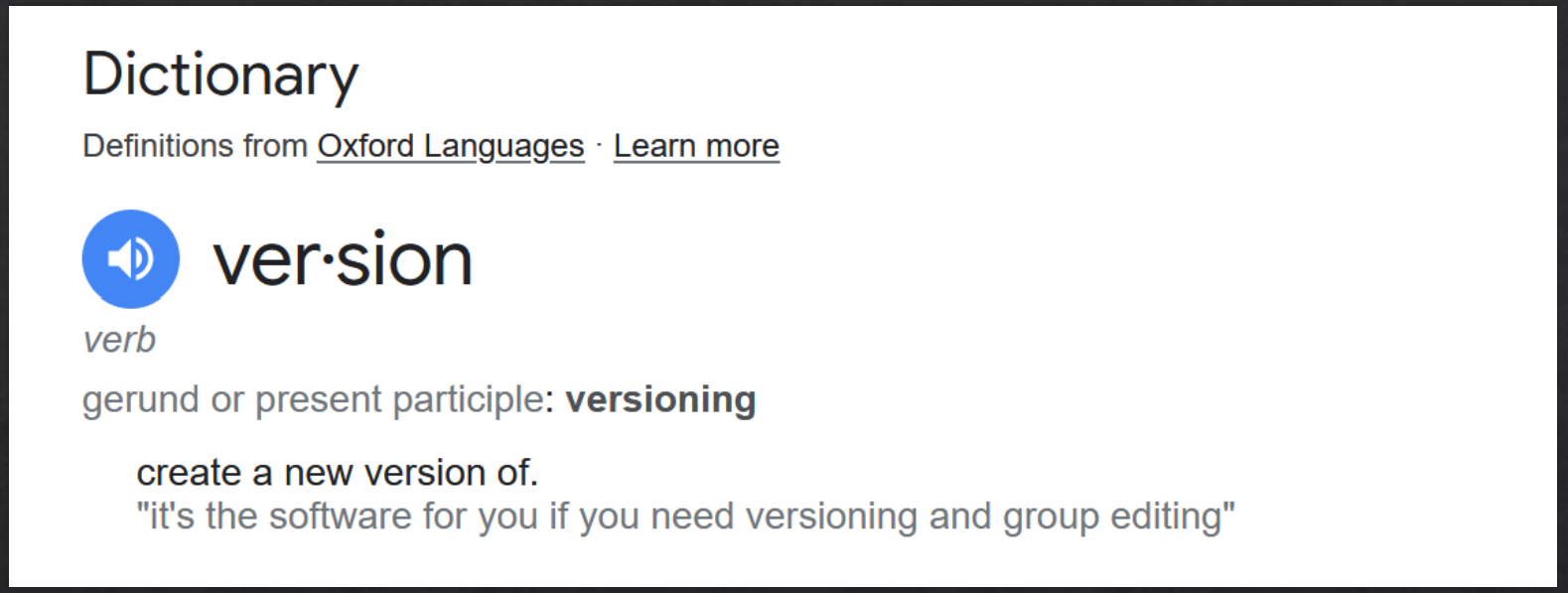

Questions From Last Session?

Terms To Listen For

- Versioning
  - When we make changes to our codebase
- Change Management
  - Our approach to making and documenting changes
- “Prod”
  - In production network
- “Dev”
  - Development network/branch



Versioning



Versioning: Definition

Dictionary

Definitions from Oxford Languages · Learn more

up·date

verb

gerund or present participle: **updating**

/ˌəpˈdāt/

make (something) more modern or up to date.
"security measures are continually updated and improved"

Similar: modernize | bring up to date | renovate | refurbish

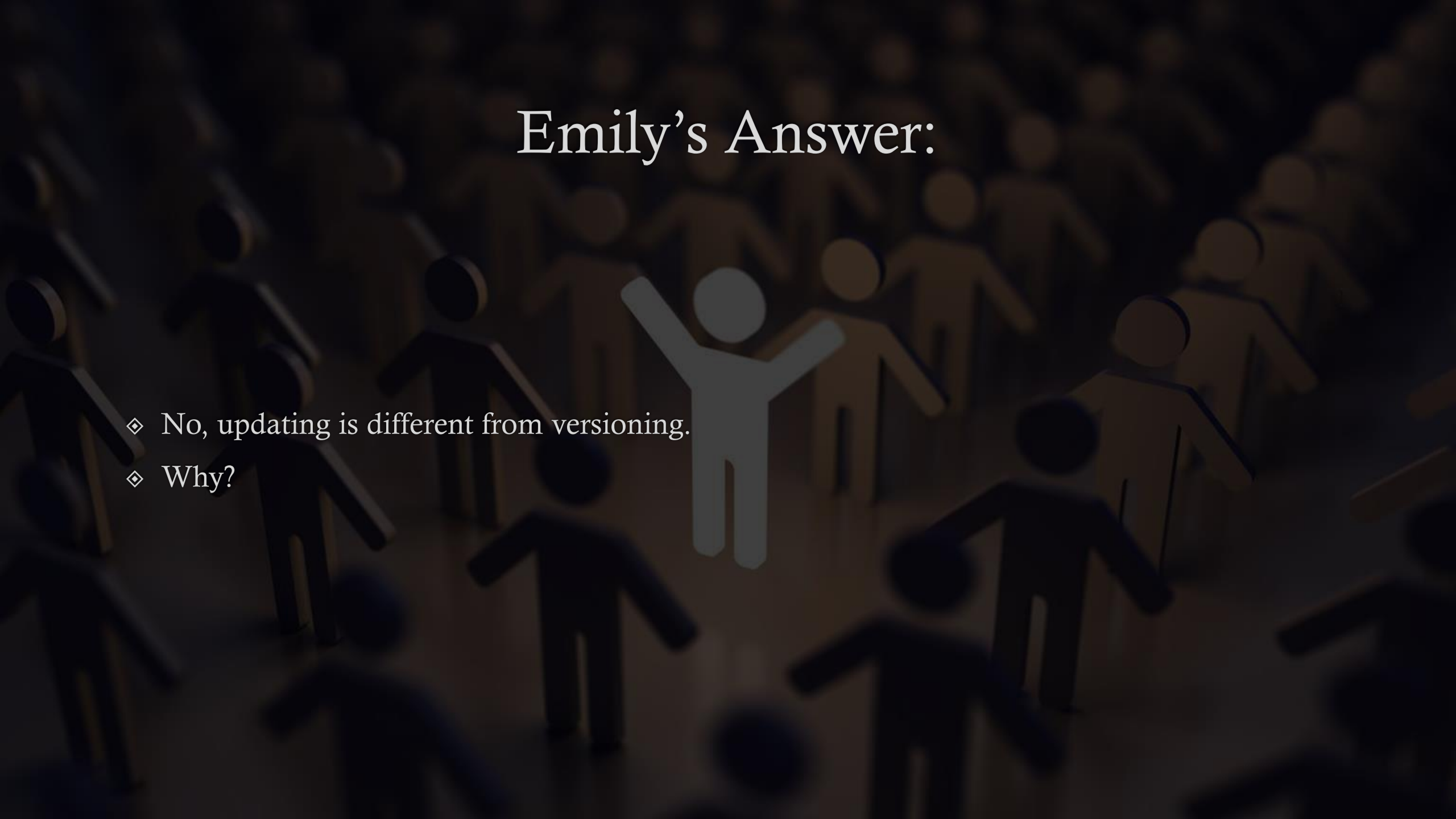
- give (someone) the latest information about something.
  "the reporter promised to keep the viewers updated"

  Similar: brief | bring up to date | inform | fill in | advise

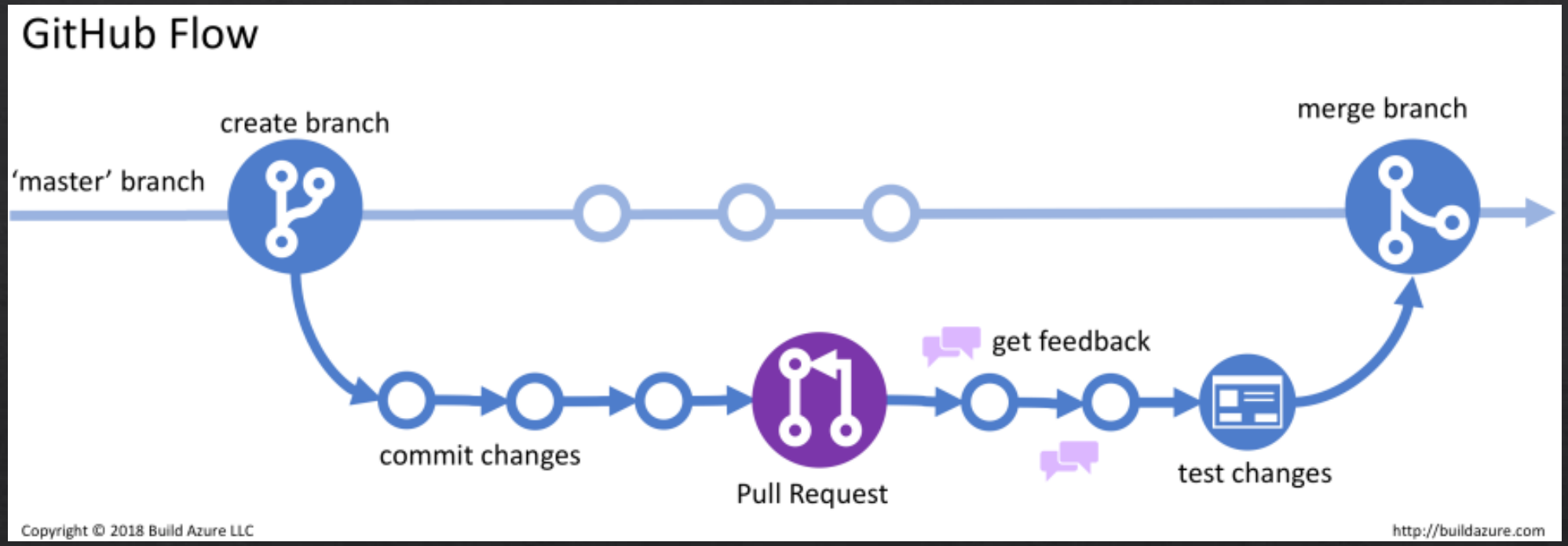
Updating Definition


Question:
Is Versioning The Same As
Updating?

Emily's Answer:



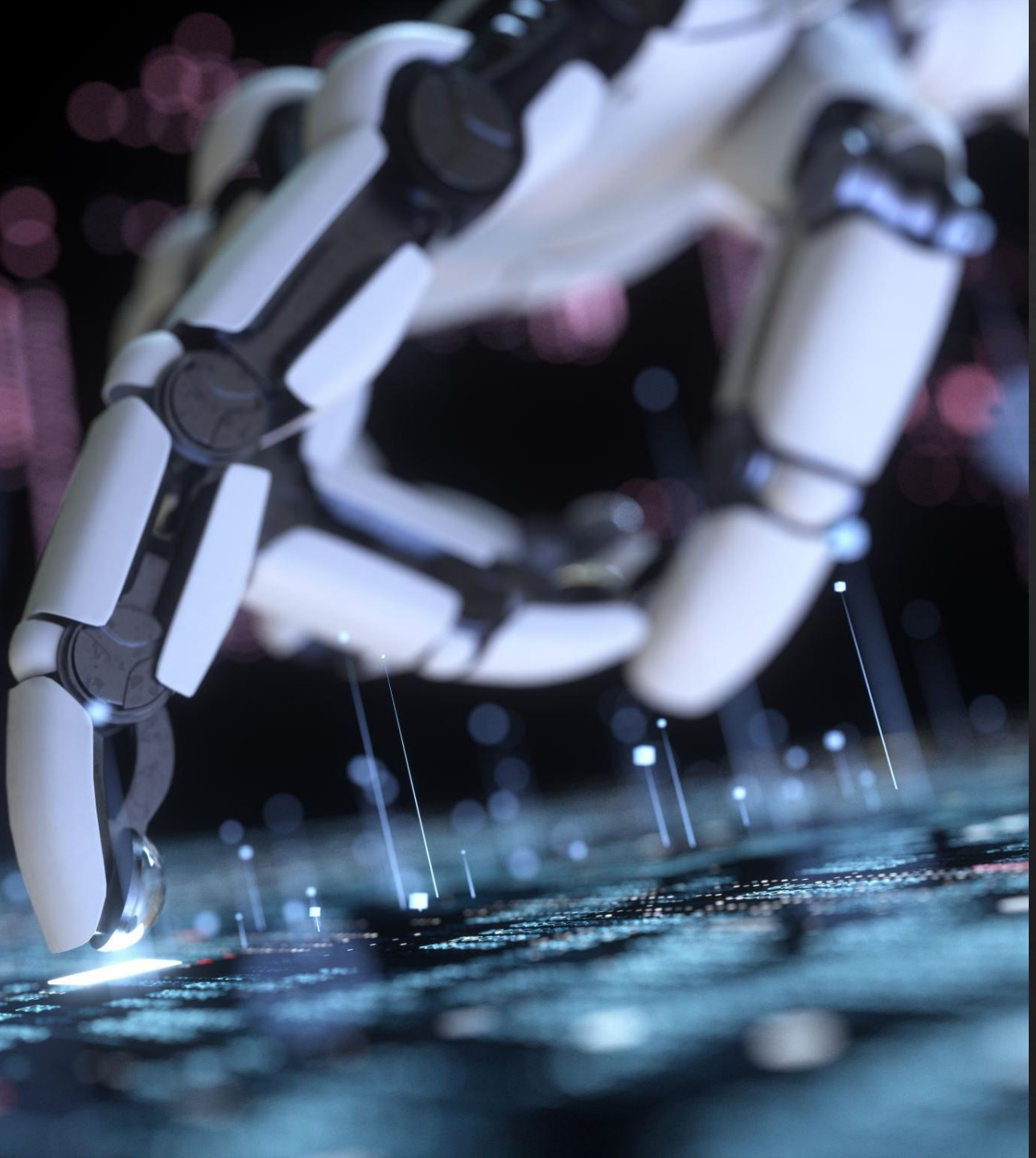
- No, updating is different from versioning.
- Why?



Versioning At-A-Glance

Change Management

Virtualization & Sandboxing



Virtualization, what is it?

- Virtualization is an isolated Run Time Environment (RTE)
  - Easily replaceable
  - Highly customizable

Why Virtualize?

Create and deploy environments

Prepare for future attacks

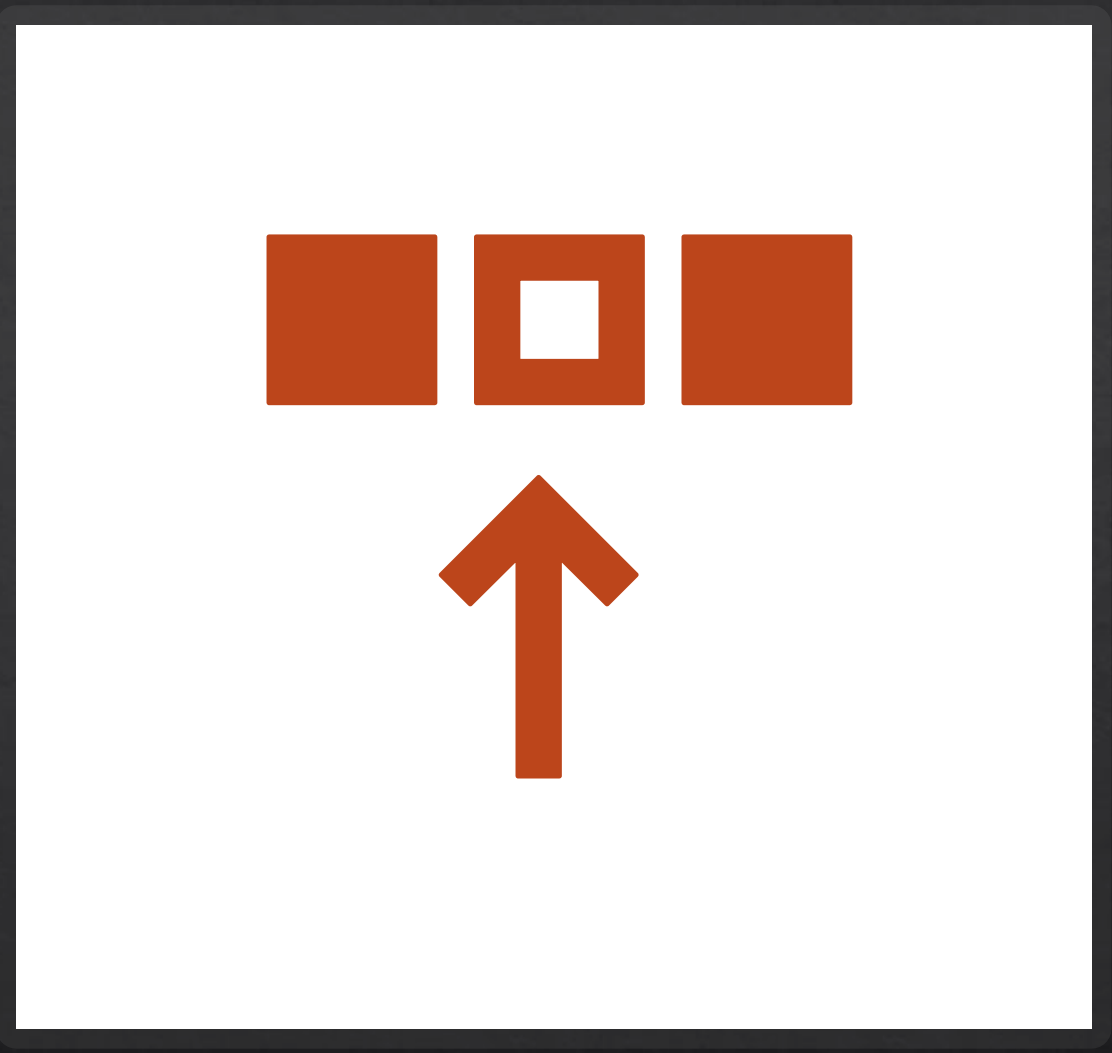
Gain access to advanced networking and support

Enhance collaboration

Save your company money

Where Can We Use Them?

- In programming:
  - Virtual ENV
- In Testing
  - Vagrant
- In Deployment
  - Docker
  - Kubernetes

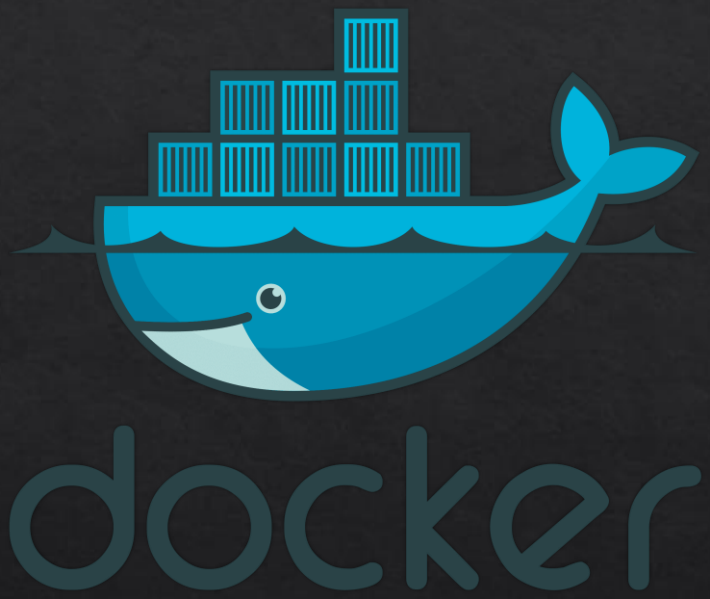


Vagrant

- Ideally Used:
  - As endpoint development hosts (vs. server-based)
- Benefits:
  - Can be used to distribute copies of the same environment
  - Somewhat easy to automate deployment/setup

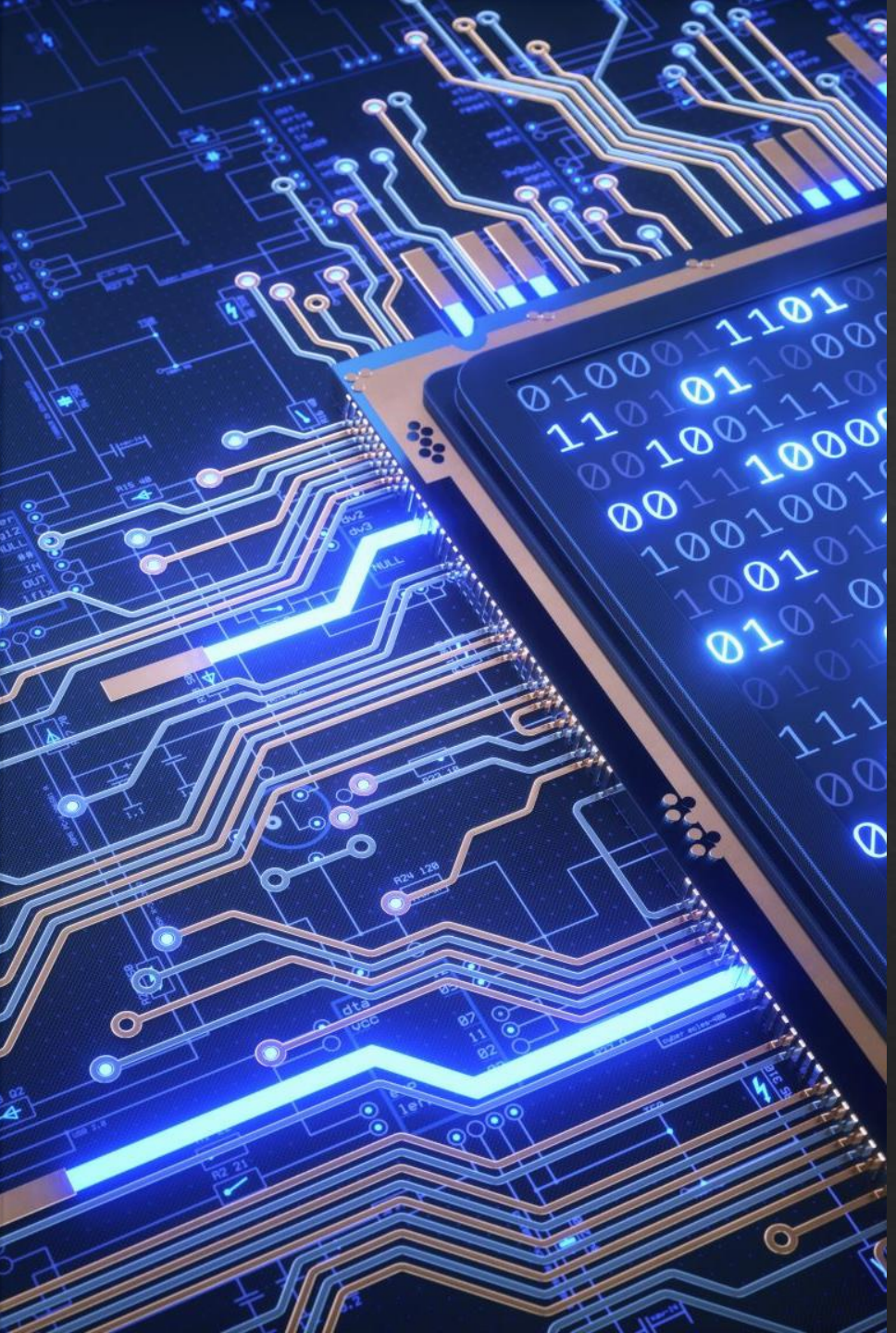
Docker

- Ideal use:
  - Isolated services
- Benefits:
  - Highly customizable/configurable
  - Can be deployed either persistent or as a single instance



Kubernetes

- Ideal use:
  - Server images/clusters
- Benefits:
  - Operates as an appliance
  - Alternative to Docker
  - Better for scaling

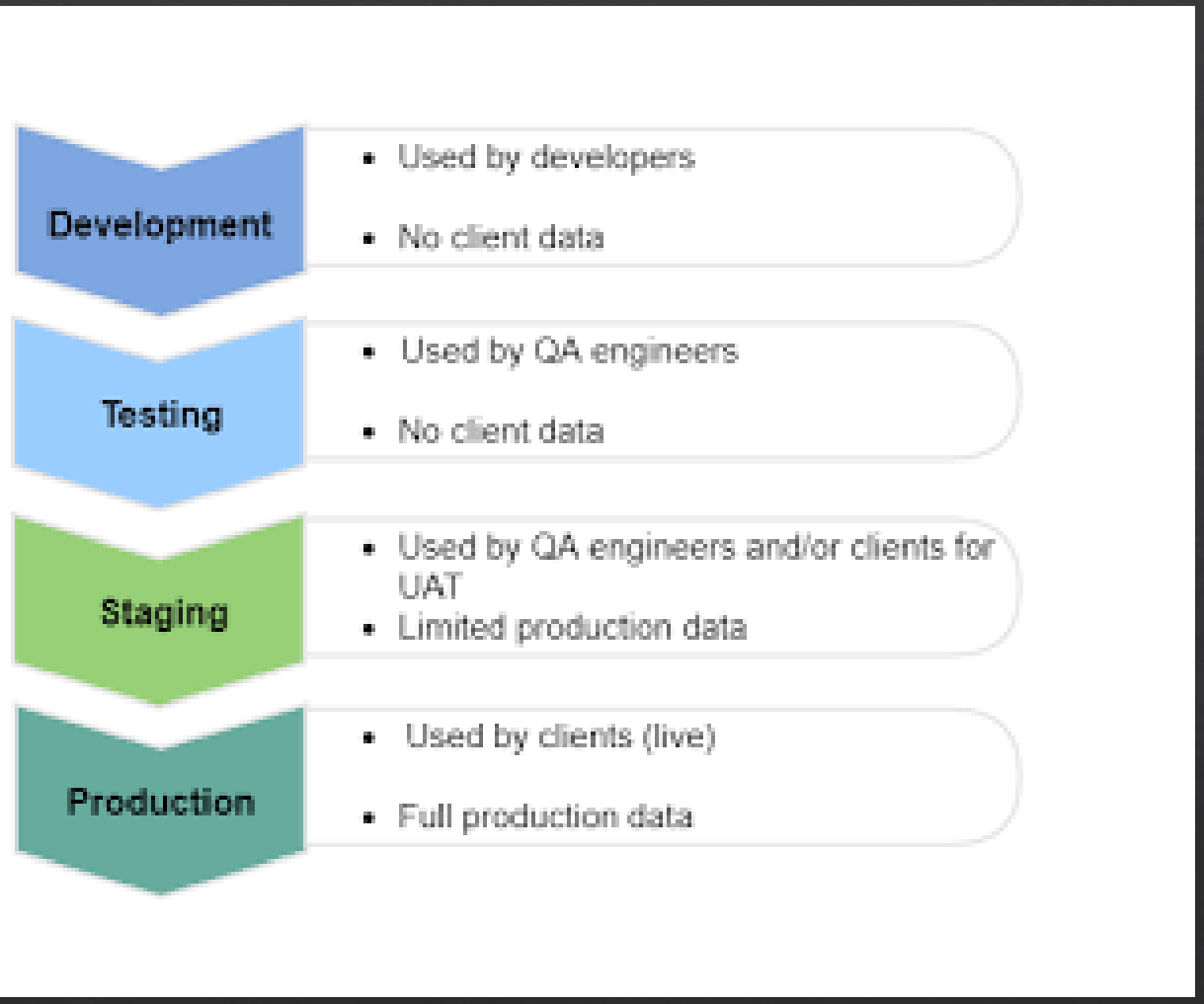


Tips For Virtualizing

- Take the time to carefully plan virtualization environments
  - Apply SDLC elements to building these environments?
  - These may be deployed in production!

Understanding Environments

- Environments:
  - Production
  - Redundant Production
  - Testing

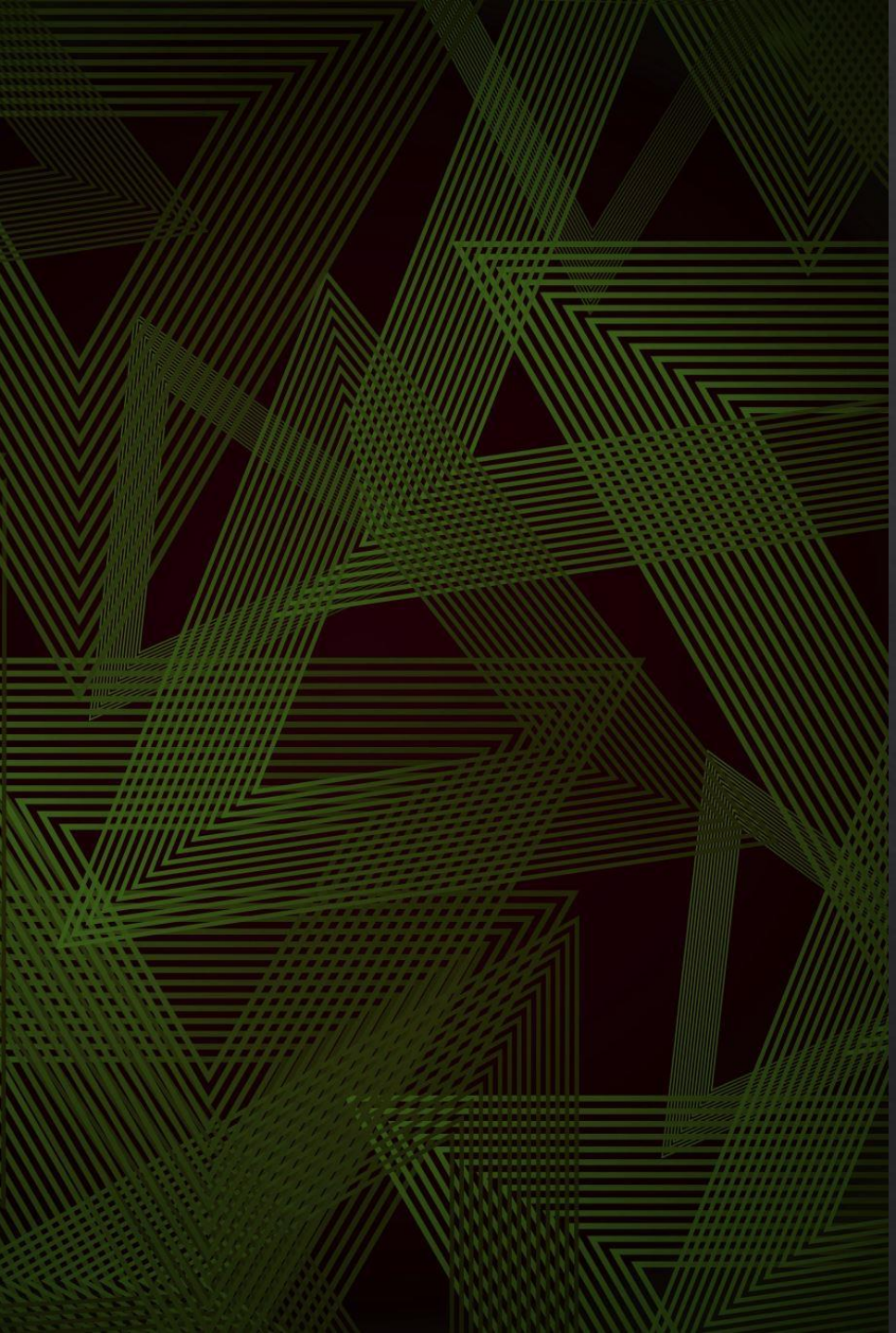


Environments Cont'

What Is Prod?

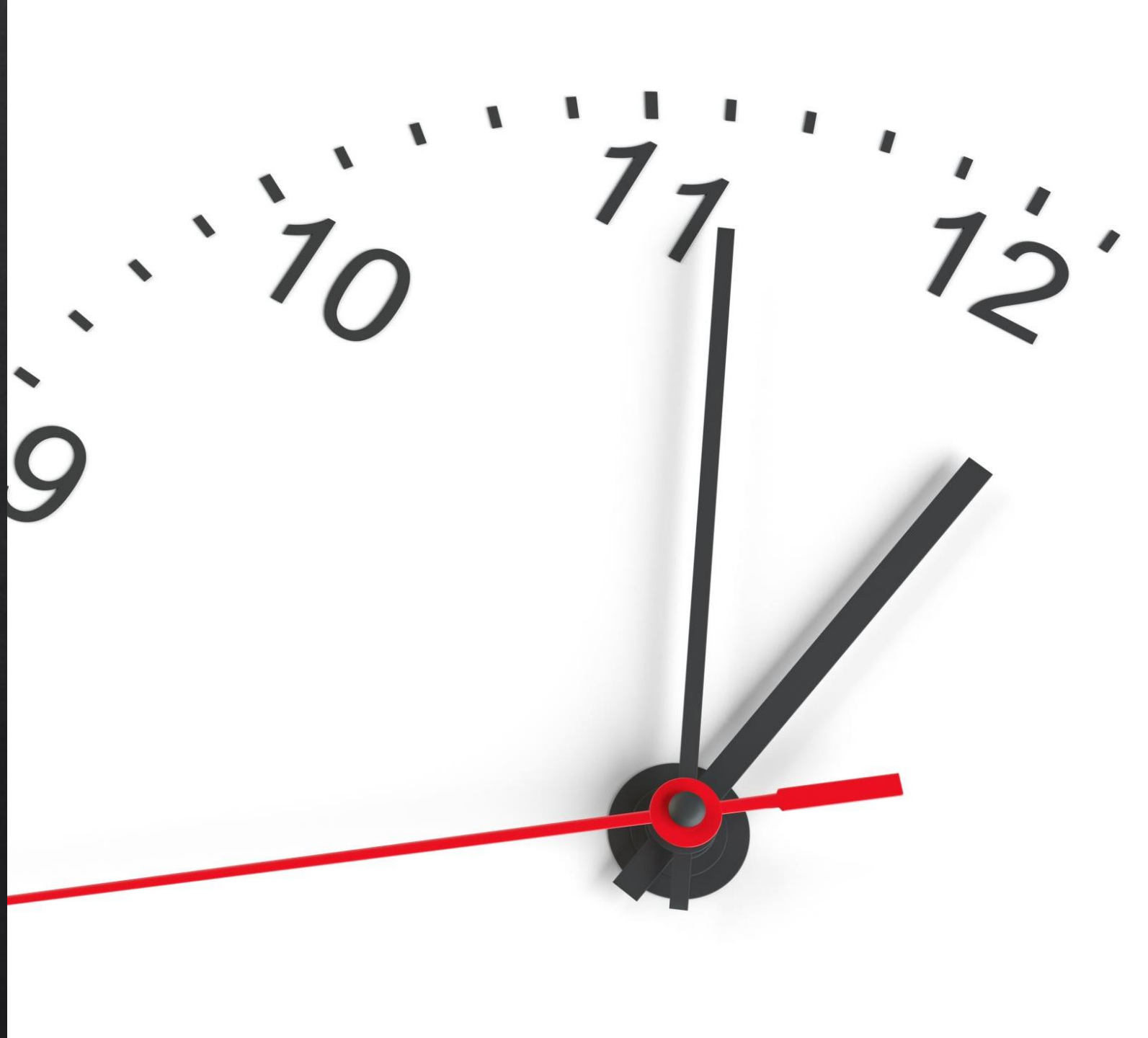
Why Not Just Push To Prod?

This Is An Option Of Last Resort

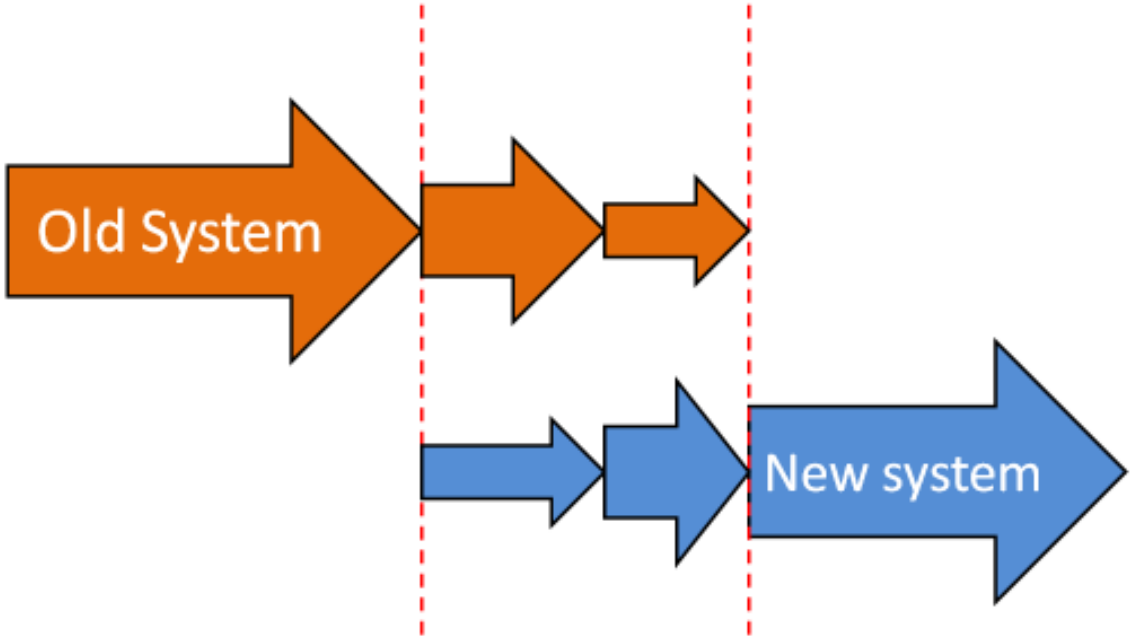


Testing & Deployment

10 minute break



Launch & Revert



Phased Deployment

Example


Internal group A
Internal group B
External group A
External group B
External group C

Pilot Testing

Phase 1: Early stages of questionnaire development	Phase 2: Structured field piloting	Phase 3: Field implementation practice
• Understand the purpose of the questionnaire • Test and develop new questions • Adapt questions to context • Build familiarity, get a sense of time • Find best way to ask questions through focus group discussions • **Re-work, share, and re-test**	• Questionnaire is close to being finalized • Test for question options, skips, and translation • Test whether respondents interpret the questions properly • **Simulate the environment of the actual survey**	• Final questionnaire is ready • Implementation practice to focus on surveyors • Test to see time taken, improving efficiency in coordination • Feedback and continued practice to improve implementation

Building A Good Pilot Group

Eating Our Own Dogfood

Deployment Monitoring

What Do We Want To Monitor?

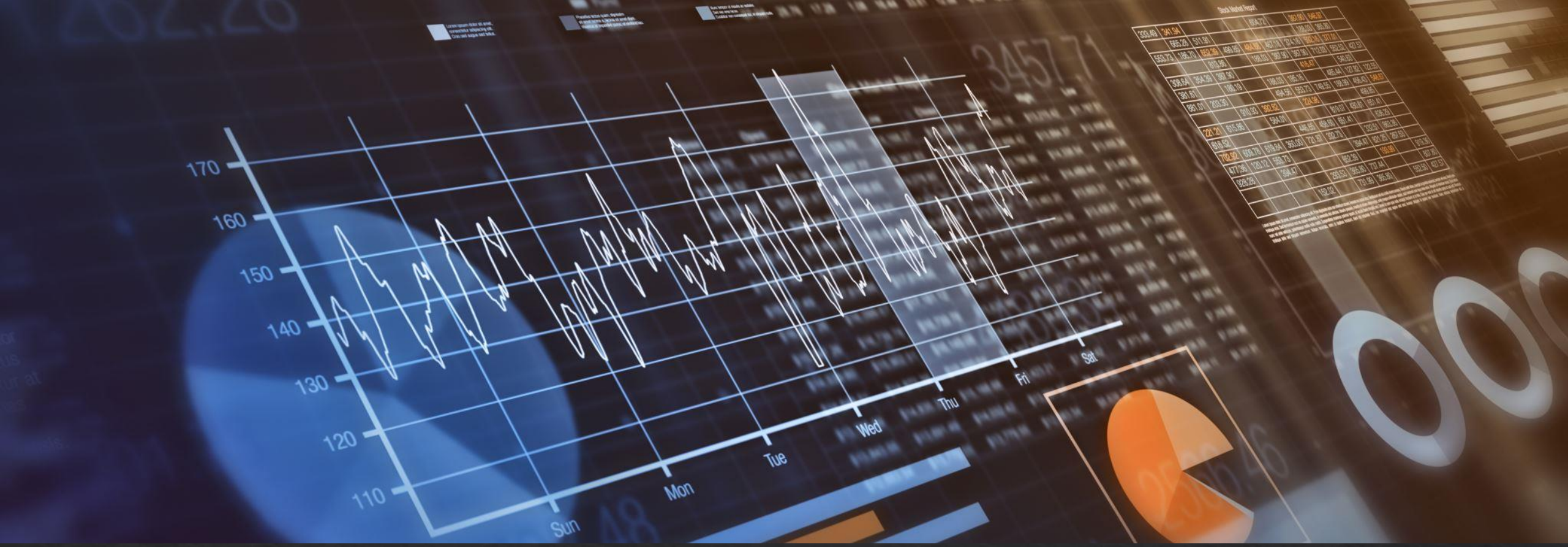
Logs

System stability

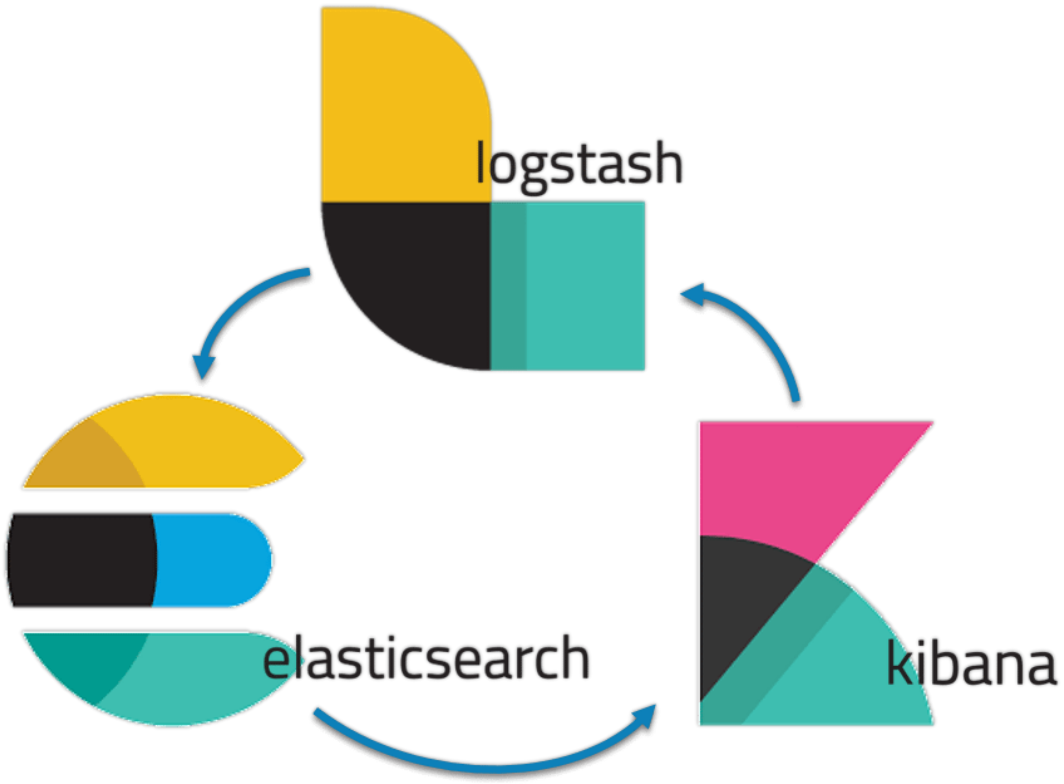
Endpoint stability

Telemetry

Has there been an interruption in expected incoming data?



Monitoring Software Options



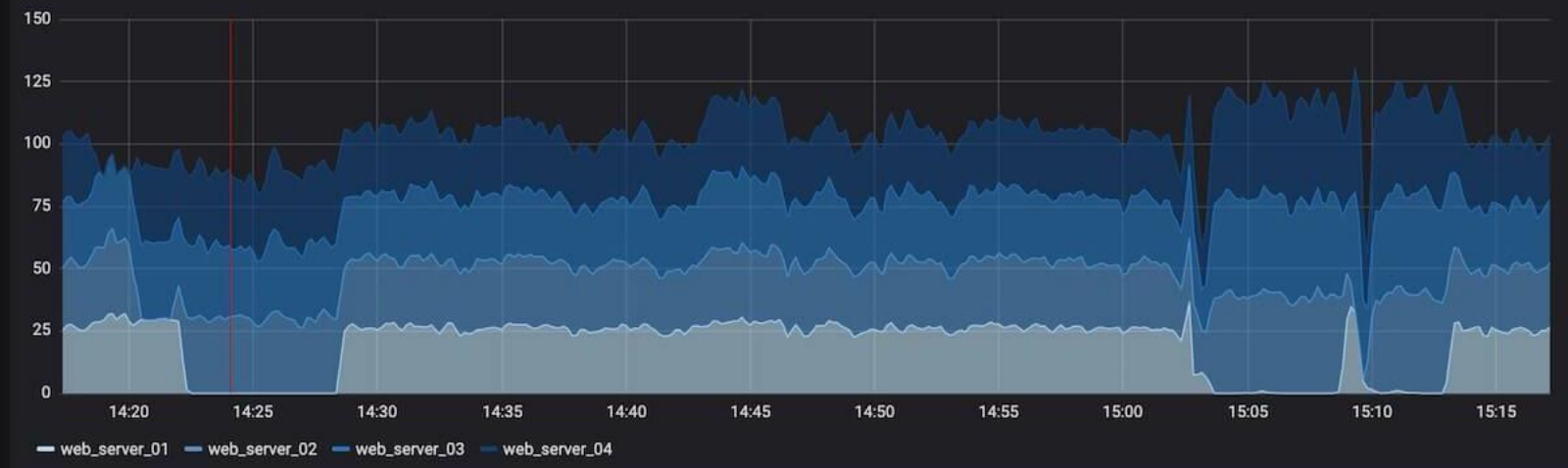
ELK

Grafana

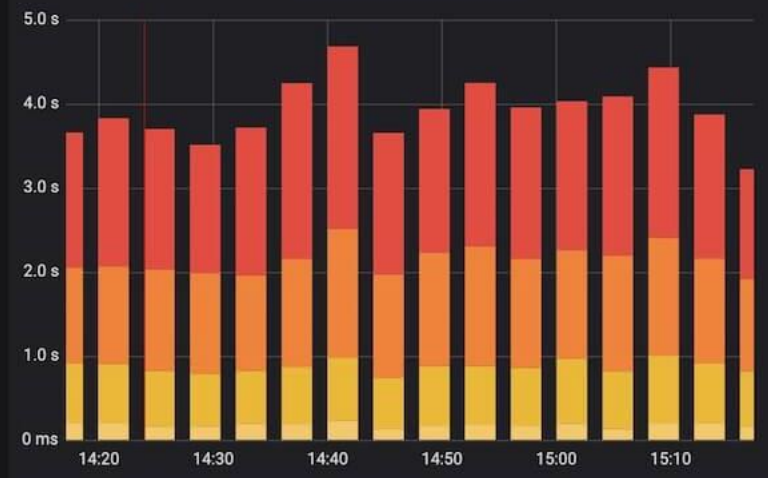
Logouts

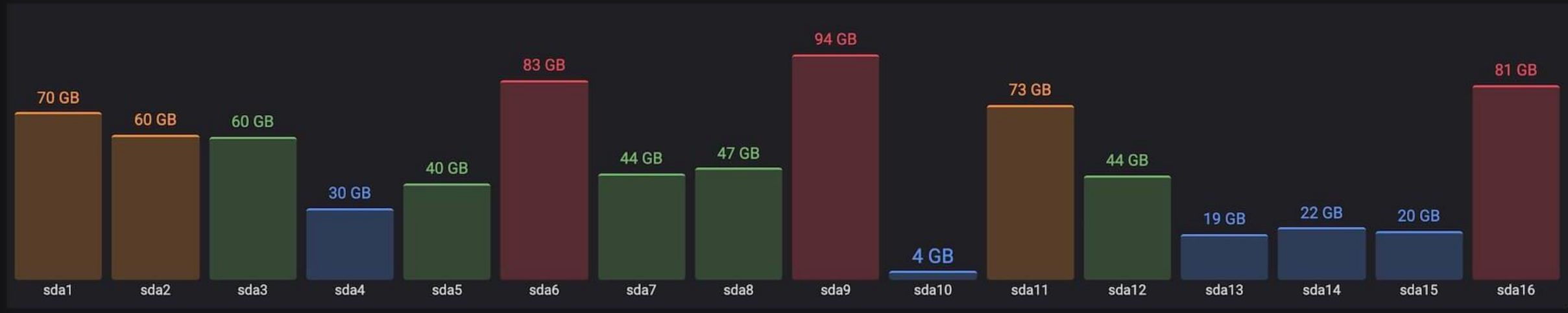
Sign outs

server requests



client side full page load

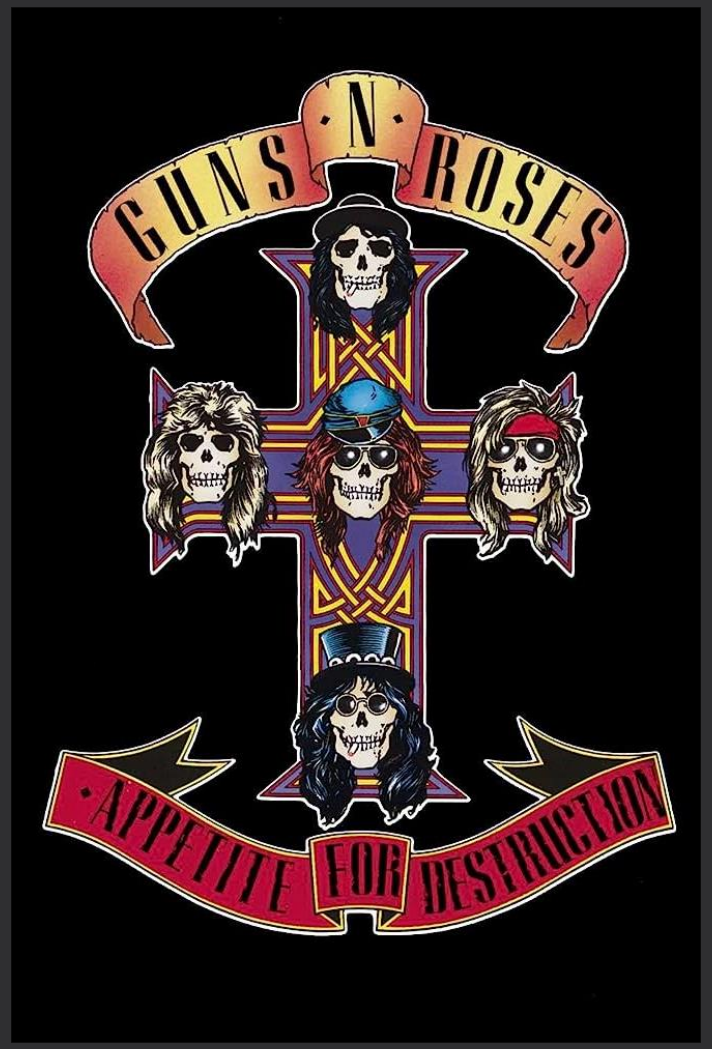





splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Investigations
Security Intelligence
Security Domains
Audit
Search
Configure
Enterprise Security
Incident Review
Search...
Hide Charts
Hide Filters
Urgency
Critical
High
Medium
Low
Informational
Unknown
Status
New
In Progress
Pending
Resolved
Closed
Owner
Administrator
esanalyst
unassigned
Domain
Access
Endpoint
Network
Threat
Identity
Audit
Saved filters
Tag
Add tags...
Urgency
Status
Owner
Type
Search Type
Correlatio...
Time or Associations
Time
Last 24 ...
Select...
Earliest: -24h@h
Latest: now
63 Notables
Edit Selected | Edit All Matching Events (63) | Add Selected to Investigation
Prev 1 2 3 4 Next
20 per page
Refresh
Title
Risk Object
Aggregated Risk Score
Risk Events
Type
Time
Disposition
Security Domain
Urgency
Status
ATT&CK tactic threshold exceeded over previous 7 days for user=wakanda
wakanda
80
4
Risk Notable
Today, 7:20 PM
Undetermined
Threat
Medium
New
Description:
ATT&CK tactic threshold exceeded for an object over the previous 7 days
Additional Fields
Value
Action
MITRE
T1059
T1098
T1176
T1189
MITRE Tactic
execution
persistence
persistence
initial-access
MITRE Tactic ID
TA0001
Related Investigations:
Currently not investigated.
Correlation Search:
Risk - 7 Day ATT&CK Tactic Threshold Exceeded - Rule
History:
View all review activity for this Notable Event
Contributing Events:
View the individual Risk Attributions
Adaptive Responses:
Response
Mode
Time
User
Status

Splunk

Knowing When To Revert


GUNS N ROSES
APPETITE FOR DESTRUCTION

Practical Deployment Tips

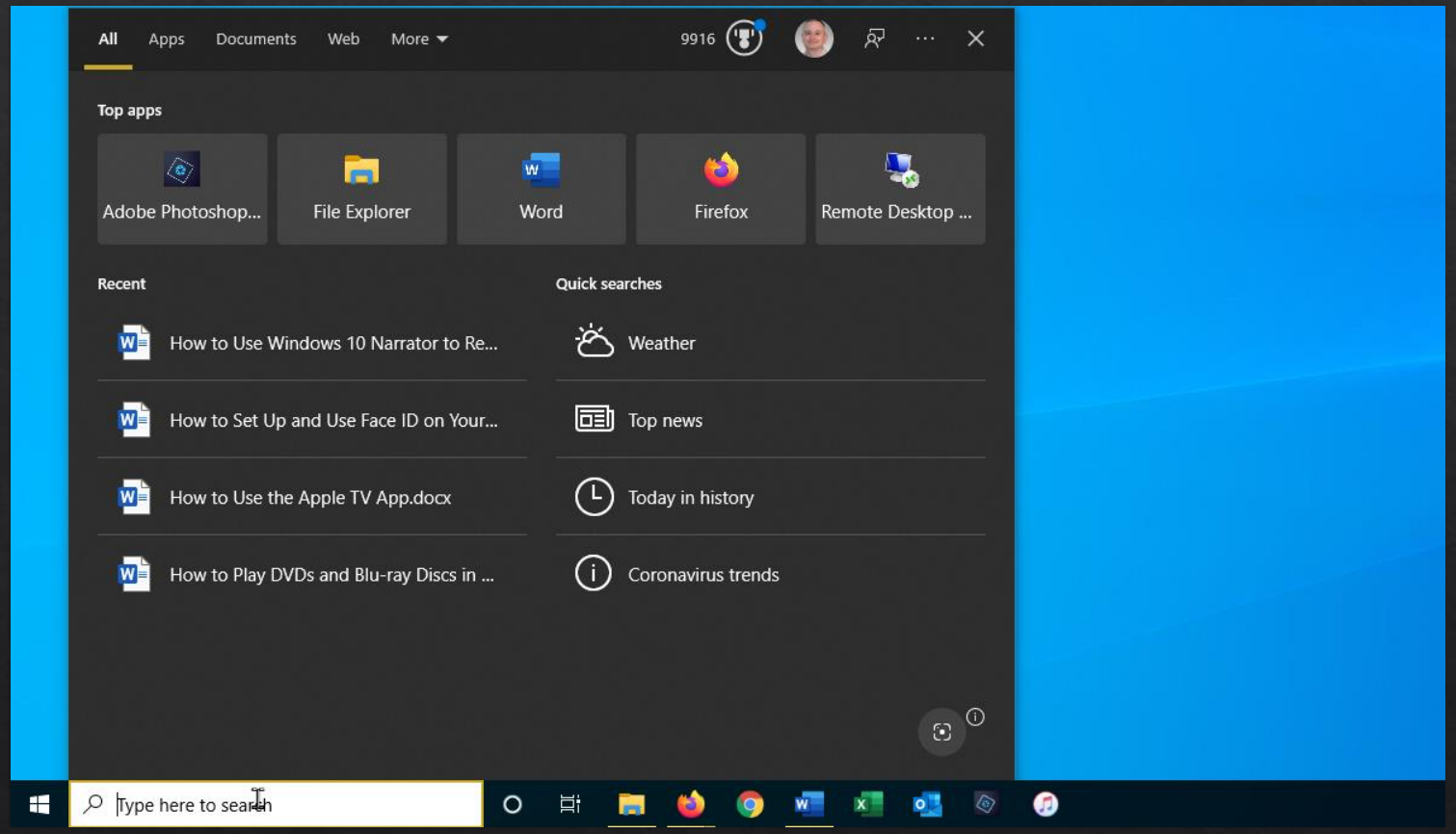
- Plan code deployment thoroughly!
- Avoid pushing updates on Fridays and at the end of the month
- Avoid pushing updates just before major holidays
- Assign a point-person for deployment
  - Diversify your point person from release-to-release

Regular Expressions

What Is Regex?

- Our way of parsing large volumes of data
- Strings-based method of searching
- Matches patterns rather than exact literal character strings

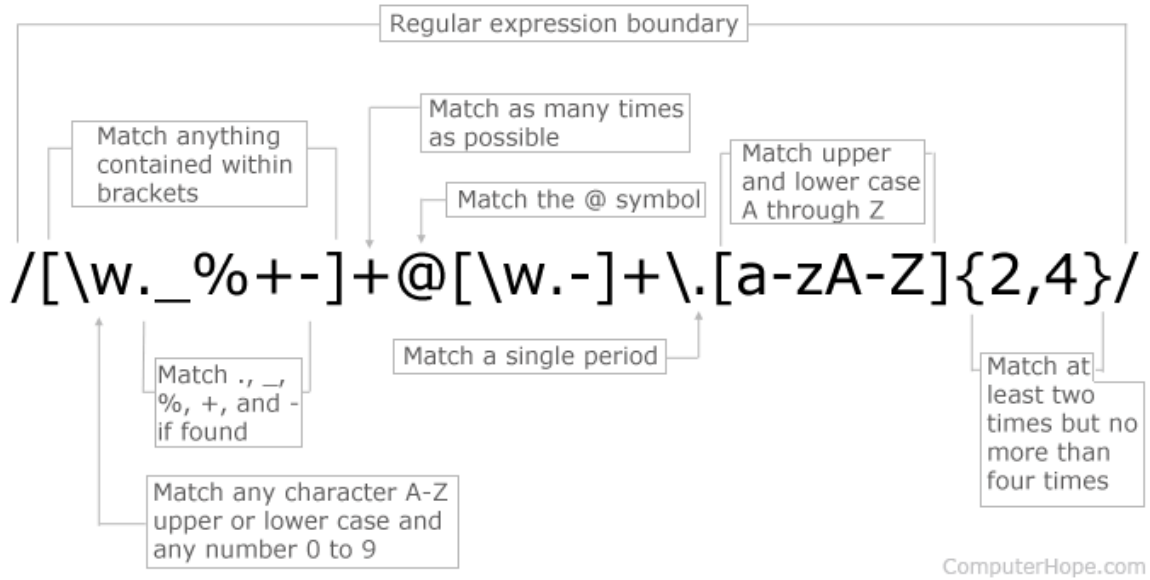
How We're Used To Searching



So What?

Problems Regex Solves

- What if we want to find information we don't know exists?
- What if we want to collect all of the information in a log with one specific feature?
  - Emails?
  - IP addresses?
  - Telephone numbers?
- What if we only have a pattern we recognize, but not a full list of filenames?

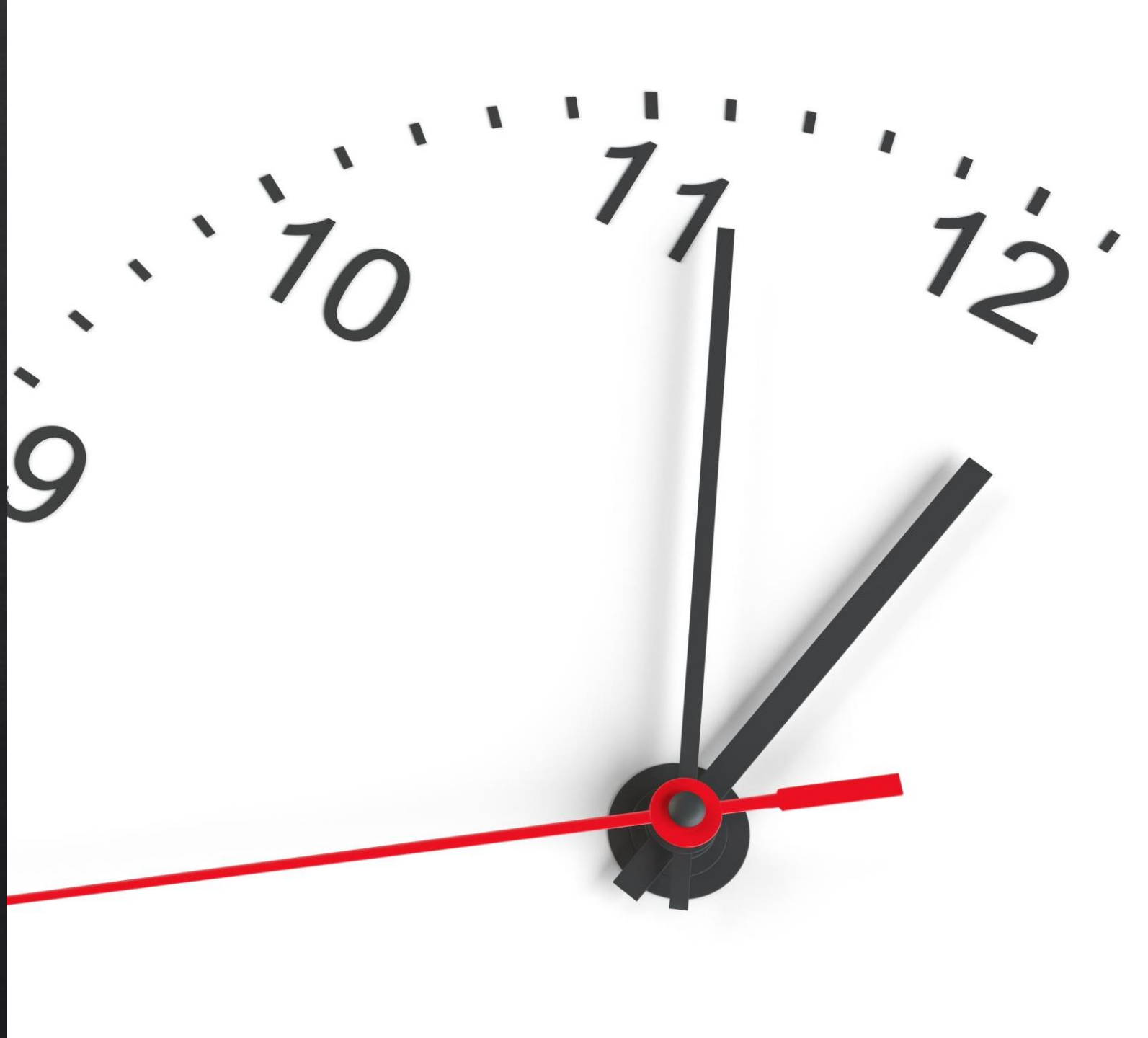


Regex Example

Try Regex Yourself!

- https://regexr.com/
- https://www.regextester.com
- https://regex101.com/

10 minute break



How Do We Apply The SDLC As Managers?

Finer Points of SDLC Application

Advice:
Be Flexible!


Use Our Tools

Here's A Secret:

The SDLC can be done out of order

(Within reason, of course)

AGILE

WATERFALL

LEAN

Emily's Opinion Moment

Reality

- Bug tickets
  - Urgent fixes
- Client requests
- MEETINGS
- Research
- Systems re-engineering
- MORE MEETINGS

Dealing With Customer Needs

Bug Prioritization


New Feature Development

Balancing Features With Fixes

Question or clarifications?

Review