Arcades and Audits 

Miranda Fullerton
BSidesSF 2019

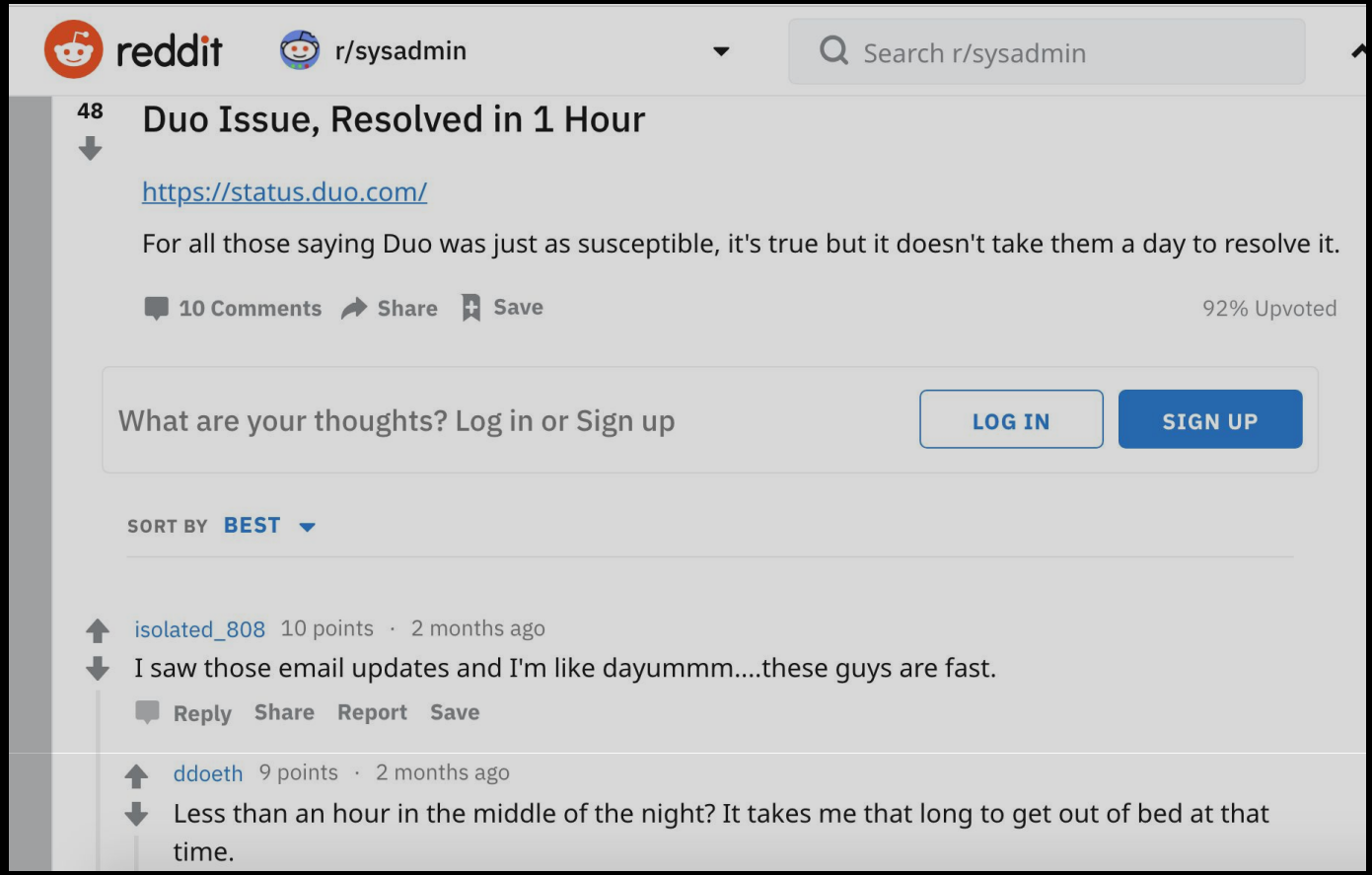
Miranda Fullerton

SE, CloudSecOps @duosec

@0hh1miranda

#arcades-and-audits


Search for users, groups, applications, or devices
ACME Corporation
John User
Dashboard
Device Insight
Policies
Applications
Dashboard
Add New...
20k
Out of Date
47k
Up to Date
68,013 total endpoints
97.3%
Authentication Success
2.7% denied authentications
4k
Total Users
1,336 licenses remaining
1
Bypass User
2
Locked Out
83k Authentications
In the last 48 hours, shown at every 30 minutes.
1.5k
1.0k
500
0
6PM
12AM
JAN 22
6AM
12PM
6PM
12AM
JAN 25
6AM
12PM
Authentication Log
Last 10 attempts
Full authentication log
Timestamp
Result
User
Application
Access Device
Second Factor
What's New?
APRIL 30, 2018
Admin SSO
AT&T
11:07 AM
84%
Login Request
Powered by Duo Security
ACME
Acme, Inc.
Development Server
johnquser
192.0.2.24
Kalamazoo, MI
11:07am EST
June 15, 2018
Approve
Deny


reddit
r/sysadmin
Search r/sysadmin
48
Duo Issue, Resolved in 1 Hour
https://status.duo.com/
For all those saying Duo was just as susceptible, it's true but it doesn't take them a day to resolve it.
10 Comments
Share
Save
92% Upvoted
What are your thoughts? Log in or Sign up
LOG IN
SIGN UP
SORT BY BEST
isolated_808 10 points · 2 months ago
I saw those email updates and I'm like dayummm....these guys are fast.
Reply
Share
Report
Save
ddoeth 9 points · 2 months ago
Less than an hour in the middle of the night? It takes me that long to get out of bed at that time.

firefighter.png

Story time...

The Washington Post
Democracy Dies in Darkness

Technology

Fire causes $company customers to lose access to accounts

By **Ken Sweet | AP**
February 7

NEW YORK — [redacted] customers experienced issues with accessing online or mobile banking as well as other banking services nationwide, after a fire happened at one of the bank's data centers.

[redacted] on Thursday blamed the technical issues on smoke, which was "detected following routine maintenance."

It is unknown how many [redacted] customers have been impacted, but the fire at the unspecified location has caused reported outages to [redacted]'s mobile banking app as well as its online banking portal.

That’s why we plan for this!

- You don’t need to implement chaos engineering to come back after a disaster.
- You just need a solid plan!

INSERT COIN

TO CONTINUE!

BCDR???

Business Continuity / Disaster Recovery

Business Continuity

- Company continues to operate with minimal or no downtime
- Policy can be for business unit or entire organization
- Example: Payroll unaffected by earthquake so employees continue to get paid

Disaster Recovery

- Major, usually physical disruptions to service
- Restore data or operability of the target system or infrastructure
- Example: California falls into the sea, DC there unavailable

RTO

Recovery Time Objective

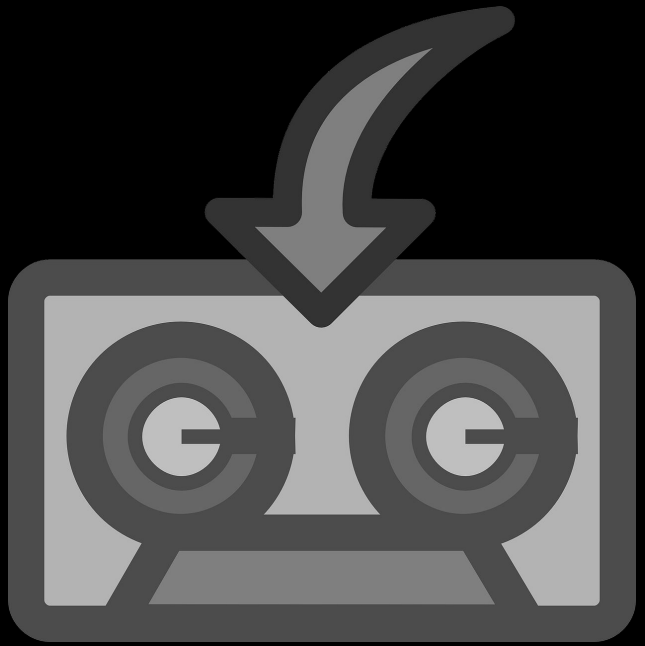
RPO

Recovery Point Objective

TTR

Time To Resolution

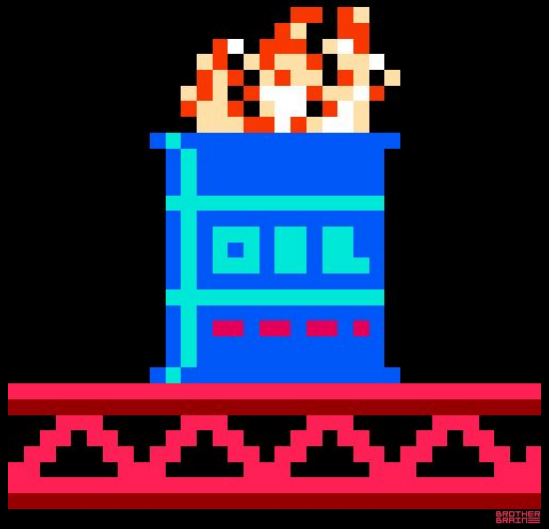
RTO, RPO, and TTR: A Simple Example



- Suppose you backup to tape
- Process takes 2 hours
- Happens at 0600 and 1800
- RTO is 2 hours
- RPO is 1 day (24 hours)

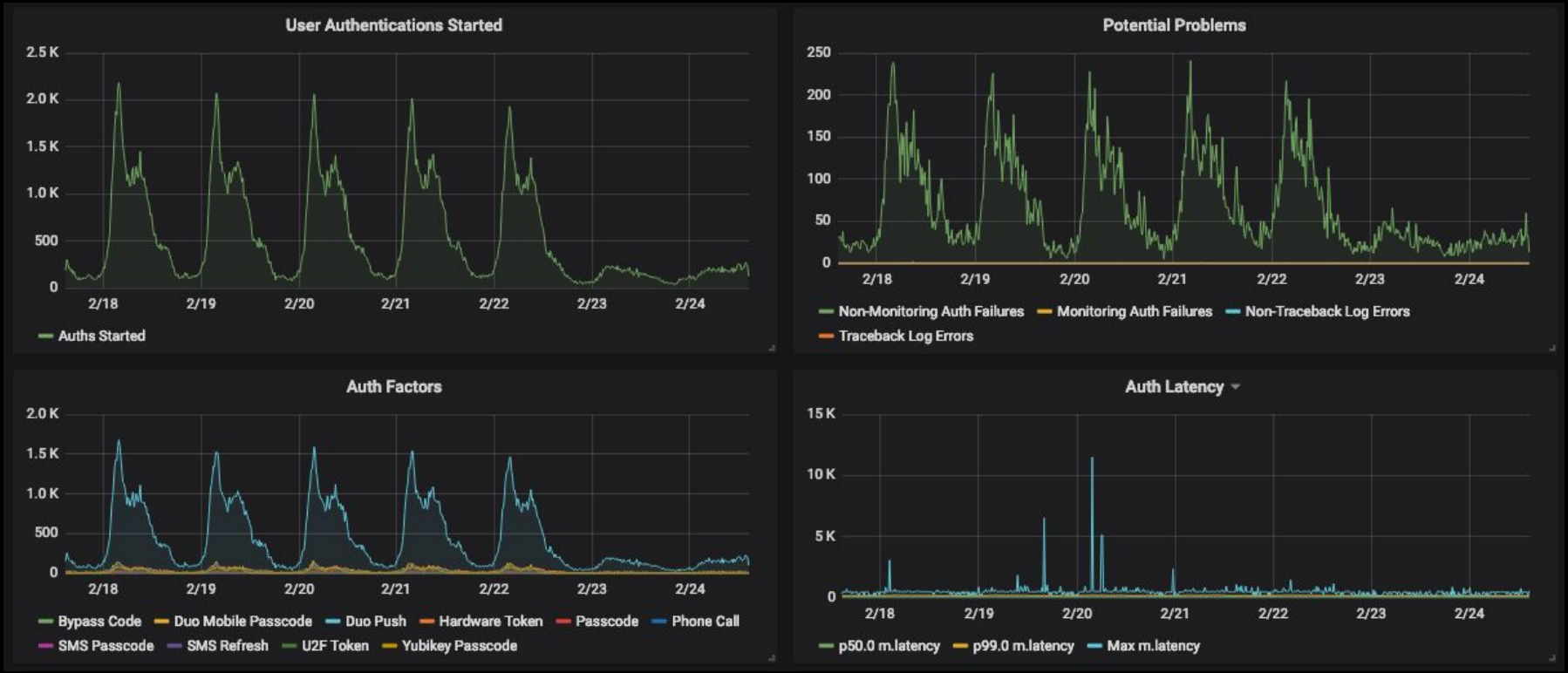
DB failure at 1400 - use
the most recent tape...

BCDR Planning: Prioritization



- What are you relied on for?
- Establish P0, P1, P2, etc.
- Establish RTO and RPO
- How can you test these areas with your Ops Team?

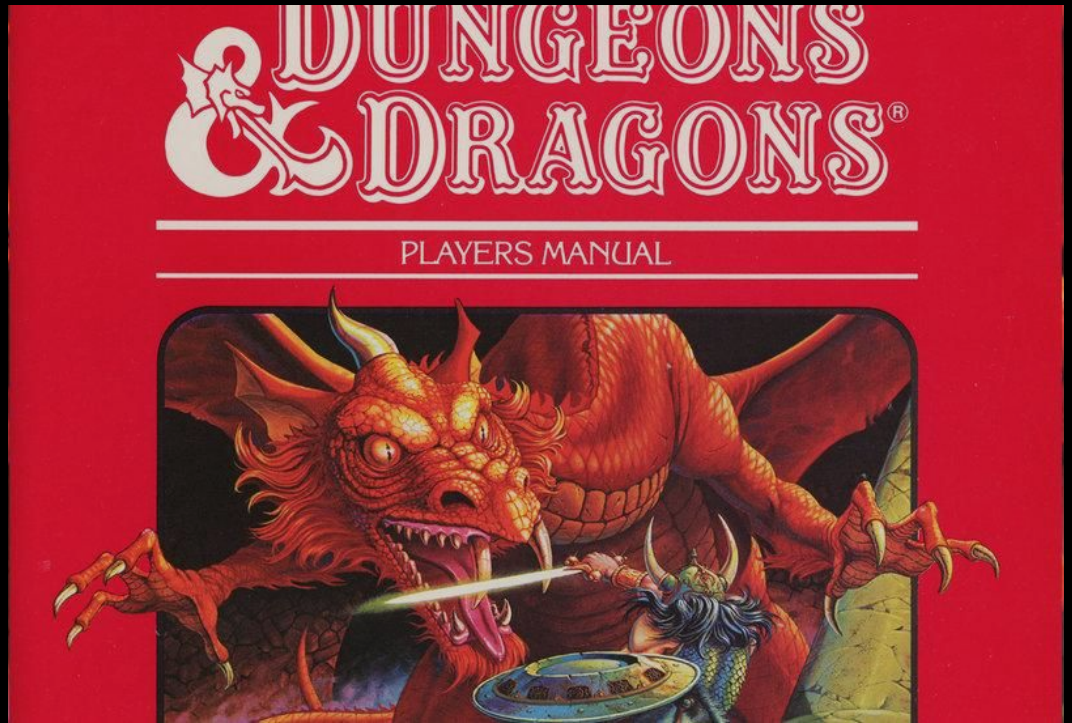
Example: PO at Duo (Authentication)



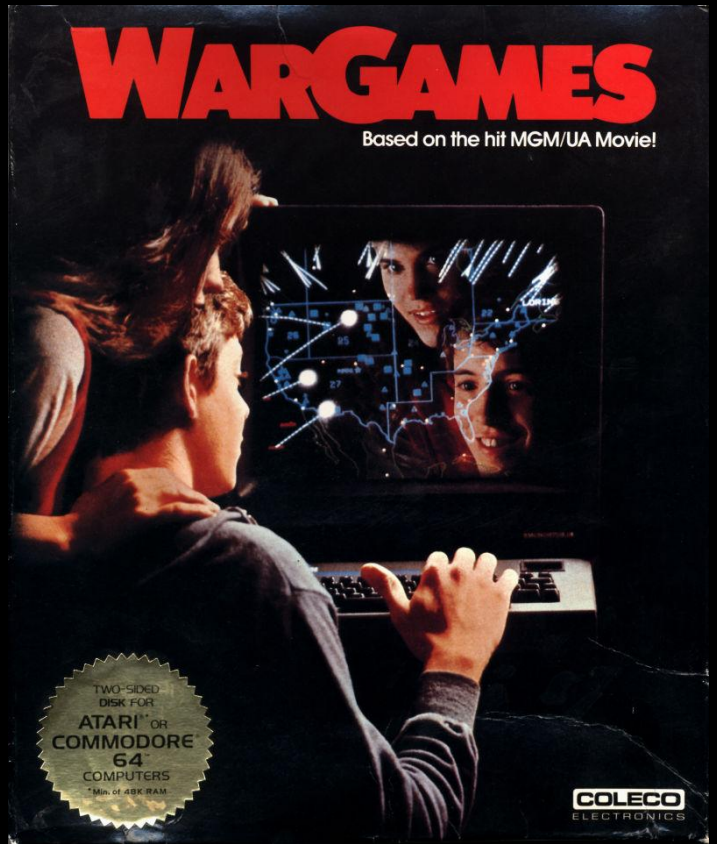
NIST Special Publication 800-34, Rev 1, Sec 3.5

- Contingency Planning Guide for Federal Information Systems
- 2 types:
  - Tabletop exercise
  - Functional exercise

NIST Exercise: Tabletop



NIST Exercise: Functional



Argument for Gamifying BCDRs

FedRAMP

EPCS

?

Positive Effects of Gaming

“Video Games: Play That Can Do Serious Good”

Eichenbaum, Bavelier, & Green

- Retention
- Decision-Making
- Perception
- Attention

Positive Effects of Gaming, cont'd

"Debiasing Decisions: Improved Decision Making With a Single Training Intervention"

Morewedge, et al.

- Compared effects of removing six cognitive biases
- Participants either watched a video or played a video game
- Game: 39% short-term, 30% long-term
- Video: 22% short-term, 20% long-term

It’s Only a Game - Don’t Get Overwhelmed

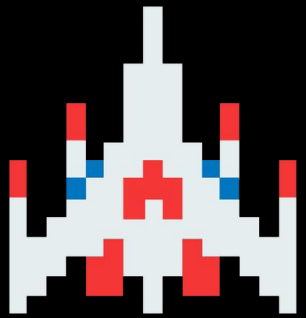
Best Practices

Care

Care

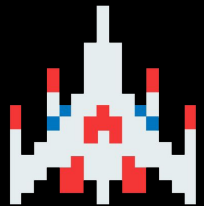
- Context: What is in- and out-of-scope?
- >1 facilitator to 3 participants
  - More if higher level of complexity
- Participants are HUMAN
  - Need sustenance and might forget
  - No blame - learning opportunities only
  - Put good in, get good out (action item ownership)

Make It Remote



Make It Remote

- Build for remote, whether you have a distributed team or not
  - In a live event, you'd have to relocate anyway
  - Allows team mates participate if they had their own "disaster"
- Clearly mark resources and communicate how to access them
  - Shared folder, directory
  - Safe branch, "`git checkout -b 2019bcdr-drill`"
- I said it before, I'll say it again: FOOOOOOOD

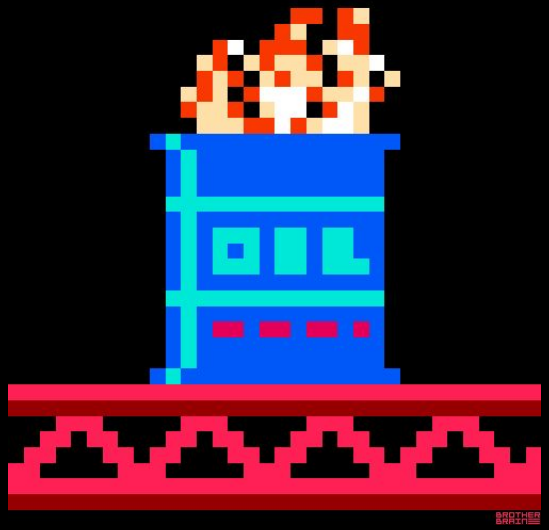


Timebox It

Timebox It

- Day-long BCDR drills are inhumane
- No more than 4 hours
  - Enough time to hit TTR
- Debrief can happen same-day or soon thereafter
  - Give participants time to compile
  - Keep it soon enough after the drill that feedback is relevant

In Summary: BCDR Basics

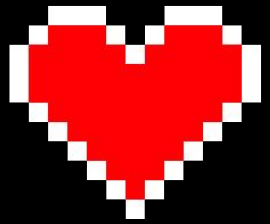


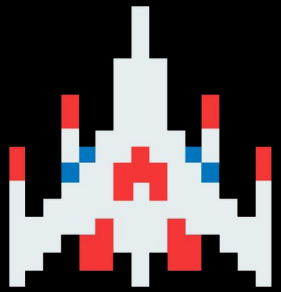
- RTO, RPO, TTR
- BCDR Planning: Prioritize P0, P1, P2

In Summary: NIST Exercises

- Tabletop
- Functional

In Summary: Best Practices





- Care
- Make It Remote
- Timebox It

Video Games Referenced and Their Initial Release Dates

- Crystal Castles, 1983
- Donkey Kong, 1986
- The Legend of Zelda, 1986
- Pac-Man, 1980
- Galaga, 1981
- Super Mario Bros, 1983

Thank you BSidesSF!

Questions?

https://sli.do

#BSidesSF2019