Everyone Can Play!

Building CTFs for Non-Security Folks

Joe Kuemerle / joe@kuemerle.com / @jkuemerle

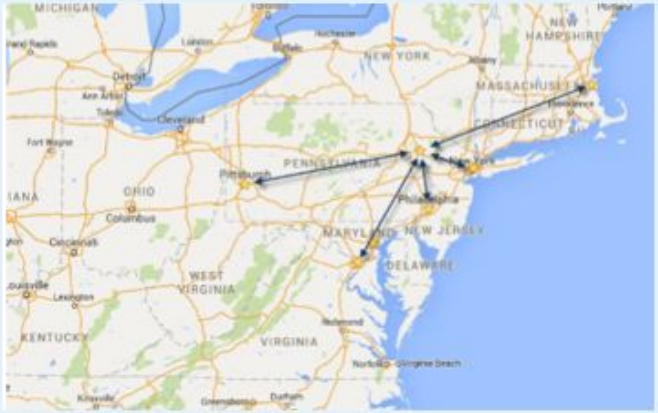
BLUE TEAM CON

https://upload.wikimedia.org/wikipedia/commons/5/5a/Muggle_Quidditch_Game_in_Vancouver_2.jpg

techbash

November 8-11, 2022 | Pocono Manor, PA

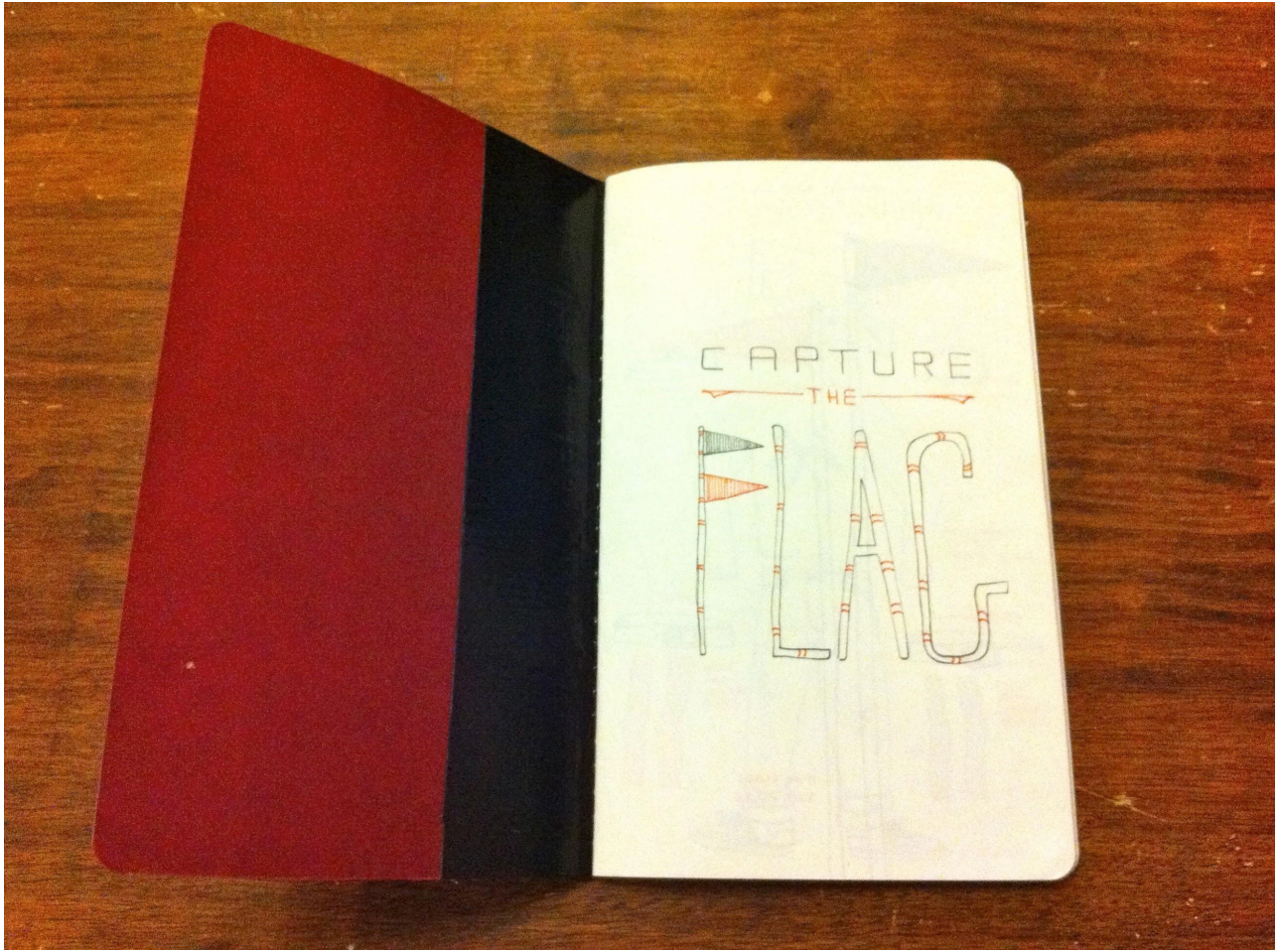
- Great speakers with top content
- A fraction of the cost of the more crowded conferences
  – 3-day conference plus lodging for less than $1000
- Full day deep dive preconference sessions available
- Easy to get to from almost anywhere
- In addition to the breakout sessions, you get a great hallway track, attendee reception, game night and more
- Full day of kids & family sessions on Friday, free for families of attendees
- Discounted Kalahari Waterpark room nights: stay, learn and play all in one place



https://techbash.com or **@techbash**

Agenda

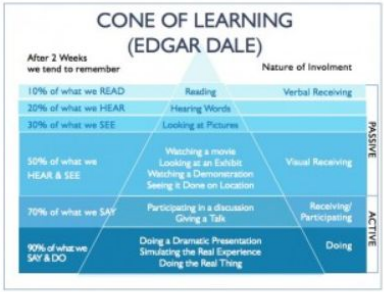
- **Why**
  - Learning studies
  - Proven success
- **What**
  - Building challenges
  - Easy to participate
  - Fun
- **How**
  - Easy to run
  - Measured



https://www.flickr.com/photos/14941806@N06/5723253006

@jkuemerle

Source: National Training Laboratories, Bethel, Maine



Examples of what the Cone of Experience became. The links to the images above have been removed to protect the mistaken. They are just two examples of the hundreds found on a simple Web search.

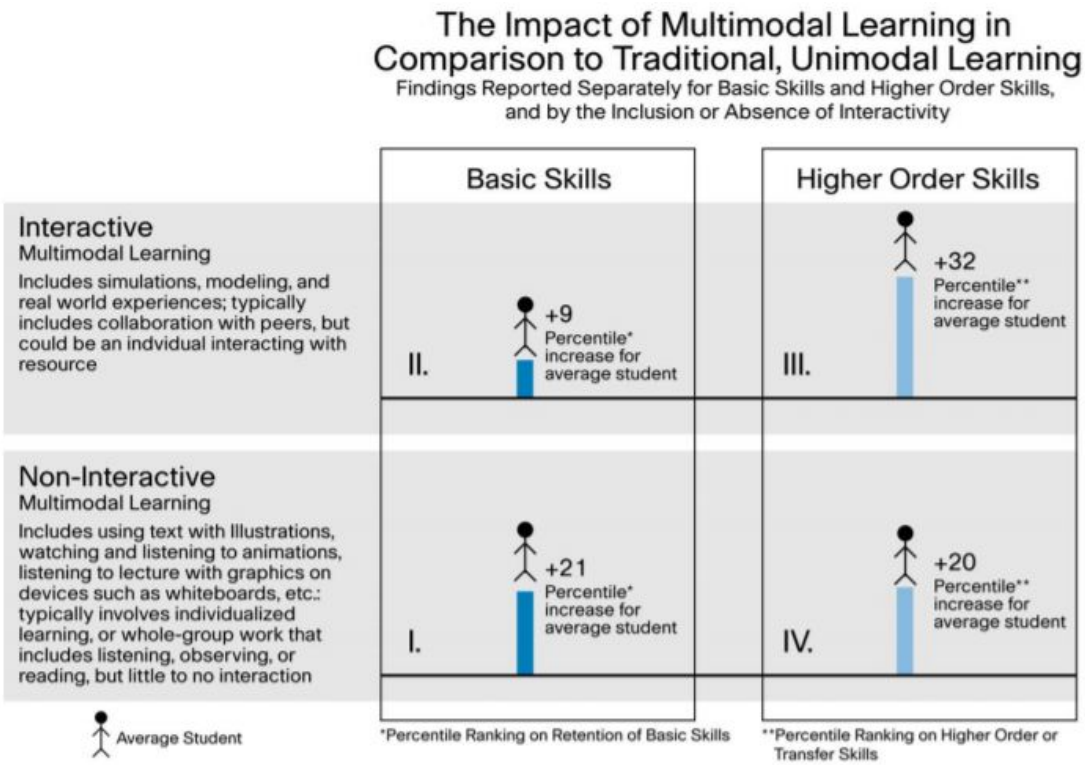
https://acrlog.org/2014/01/13/tales-of-the-undead-learning-theories-the-learning-pyramid

Multimodal Learning Through Media: What the Research Says

By Metiri Group – Commissioned by Cisco

Contacts:
Charles Fadel, Global Lead, Education; Cisco Systems, Inc.: cfadel@cisco.com
Cheryl Lemke, CEO, Metiri Group: clemke@metiri.com

Multimodal Learning Through Media: What the Research Says



https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/Multimodal-Learning-Through-Media.pdf

1. Multimedia Principle: Retention is improved through words and pictures rather than through words alone.

2. Spatial Contiguity Principle: Students learn better when corresponding words and pictures are presented near each other rather than far from each other on the page or screen.

3. Temporal Contiguity Principle: Students learn better when corresponding words and pictures are presented simultaneously rather than successively.

4. Coherence Principle: Students learn better when extraneous words, pictures, and sounds are excluded rather than included.

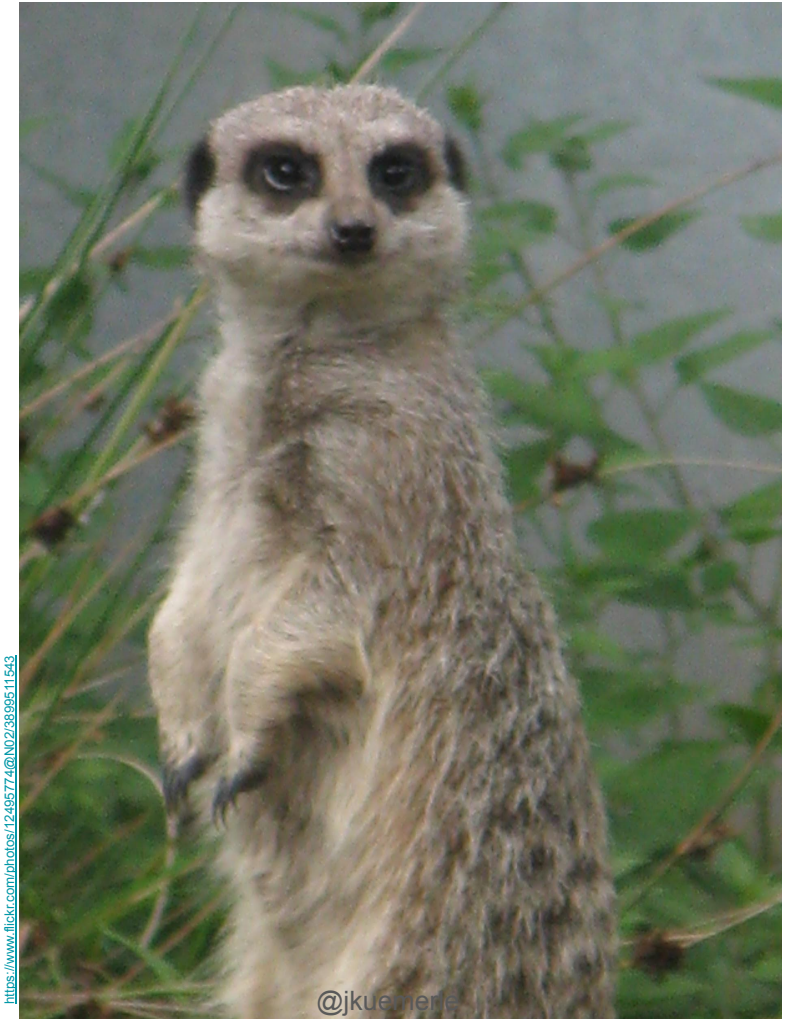
5. Modality Principle: Students learn better from animation and narration than from animation and on-screen text.

6. Redundancy Principle: Students learn better when information is not represented in more than one modality – redundancy interferes with learning.

7a. Individual Differences Principle: Design effects are higher for low-knowledge learners than for high-knowledge learners.

7b. Individual Differences Principle: Design effects are higher for high-spatial learners rather than for low-spatial learners.

8. Direct Manipulation Principle: As the complexity of the materials increase, the impact of direct manipulation of the learning materials (animation, pacing) on transfer also increases



https://www.flickr.com/photos/12495774@N02/3899511543

@jkuemerle

https://trailhead.salesforce.com/pt-BR/content/learn/modules/get_ready_for_dreamforce_onsite/get_ready_for_dreamforce_onsite_get_to_know_the_campus

https://www.flickr.com/photos/37984062@N03/3495248498

1. Multimedia Principle: Retention is improved through words and pictures rather than through words alone.

2. Spatial Contiguity Principle: Students learn better when corresponding words and pictures are presented near each other rather than far from each other on the page or screen.

3. Temporal Contiguity Principle: Students learn better when corresponding words and pictures are presented simultaneously rather than successively.

4. Coherence Principle: Students learn better when extraneous words, pictures, and sounds are excluded rather than included.

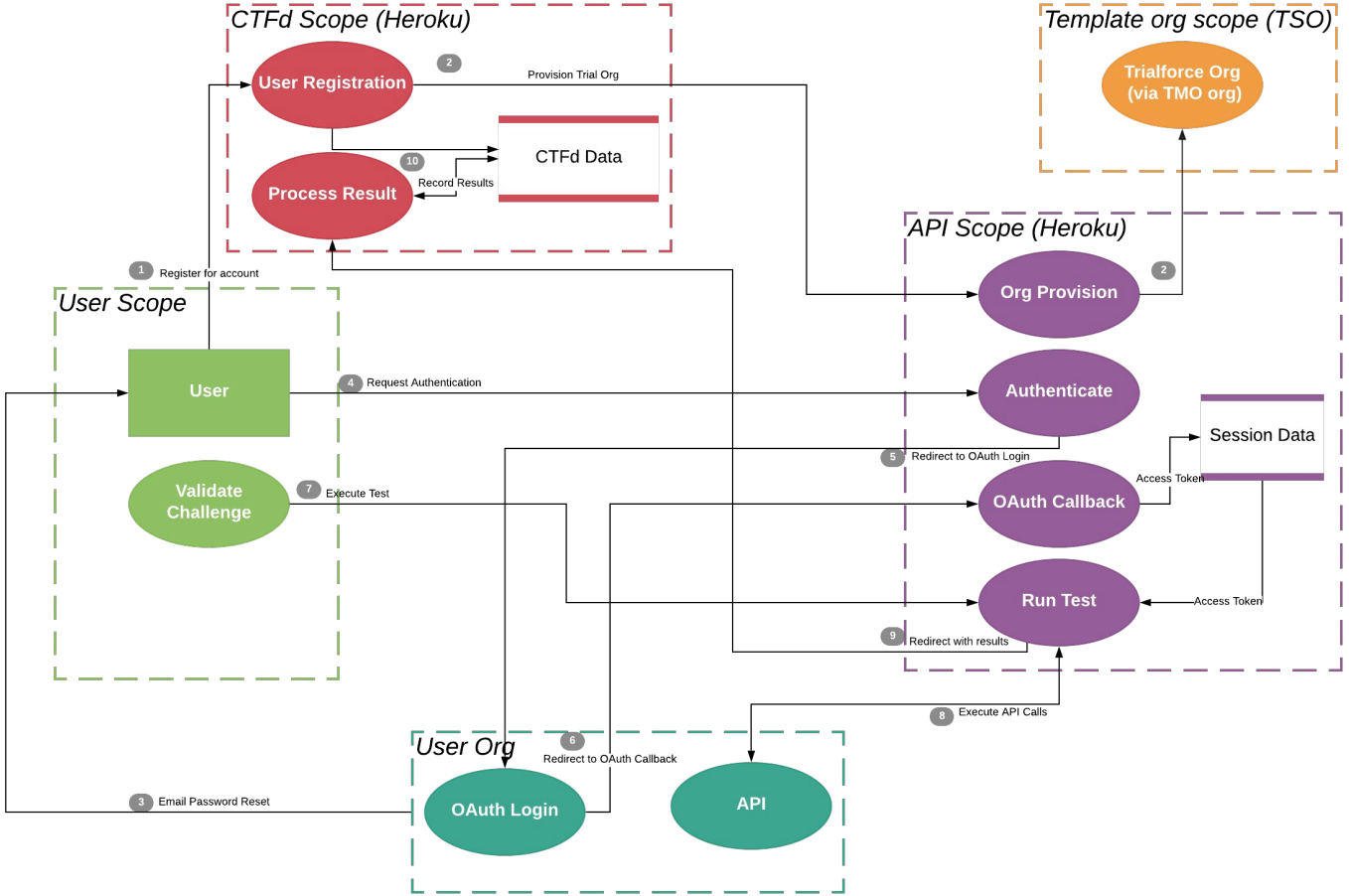
5. Modality Principle: Students learn better from animation and narration than from animation and on-screen text.

6. Redundancy Principle: Students learn better when information is not represented in more than one modality – redundancy interferes with learning.

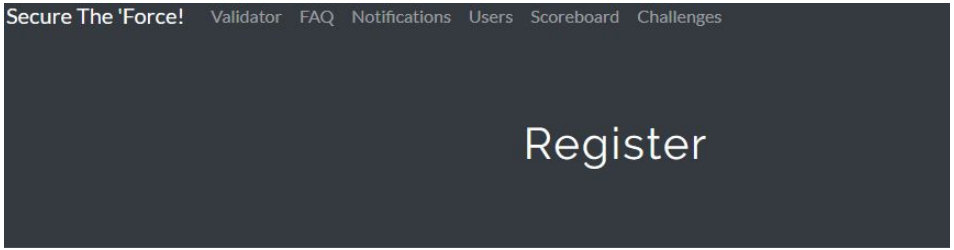
7a. Individual Differences Principle: Design effects are higher for low-knowledge learners than for high-knowledge learners.

7b. Individual Differences Principle: Design effects are higher for high-spatial learners rather than for low-spatial learners.

8. Direct Manipulation Principle: As the complexity of the materials increase, the impact of direct manipulation of the learning materials (animation, pacing) on transfer also increases



https://engineering.salesforce.com/capture-the-flag-secure-your-knowledge-37b43180e55a



First Name

Test

Last Name

User

User Name

TestUser

Email

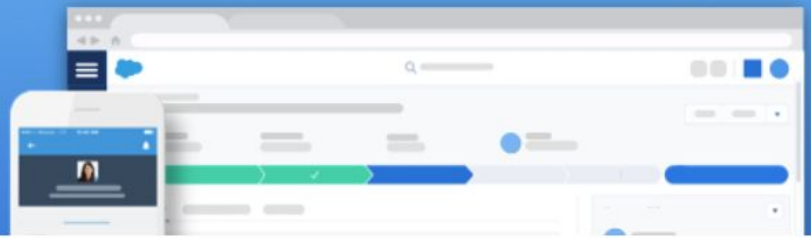
test_user@example.com

Password

Submit

@jkuemerle

Thanks for signing up with Salesforce!



Click below to verify your account.

Verify Account

To easily log in later, save this URL:
https://[redacted].my.salesforce.com

Username:
[redacted]@[redacted].com.399495

Again, welcome to Salesforce!

@jkuemerle

Challenges

Initialization

Initialize
50

Trivia

Trivia012 100	Trivia013 100	Trivia014 100	Trivia015 100
Trivia016 100	Trivia017 100	Trivia018 100	Trivia019 100
Trivia020 100	Trivia021 100	Trivia028 100	Trivia029 100
Trivia030 100	Trivia031 100	Trivia032 100	Trivia033 100
Trivia034 100	Trivia035 100	Trivia036 100	Trivia037 100

Challenge | 0 Solves

Cross Site Scripting Protection

500

Astro read the following snippet and wanted to secure their org in the same way: If a reflected cross-site scripting attack is detected, the browser renders a blank page with no content.

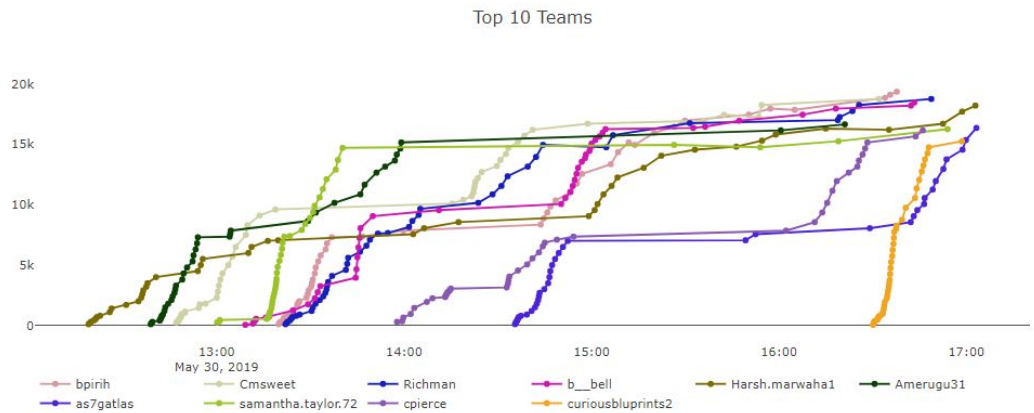
Help Astro secure their org so that if a reflected cross-site scripting (XSS) attack is detected, the browser renders a blank page with no content.

Validate


SETUP
Session Settings
Enable Stricter Content Security Policy
Lightning Locker API Version
Use security enhancements in API version
47.0
Freeze JavaScript Prototypes
Freeze JavaScript Prototypes
XSS protection
Enable XSS protection
Content Sniffing protection
Enable Content Sniffing protection


Challenge
0 Solves
Cross Site Scripting Protection
500
Congratulations! Your flag value is: JhdHVs
Submit Flag

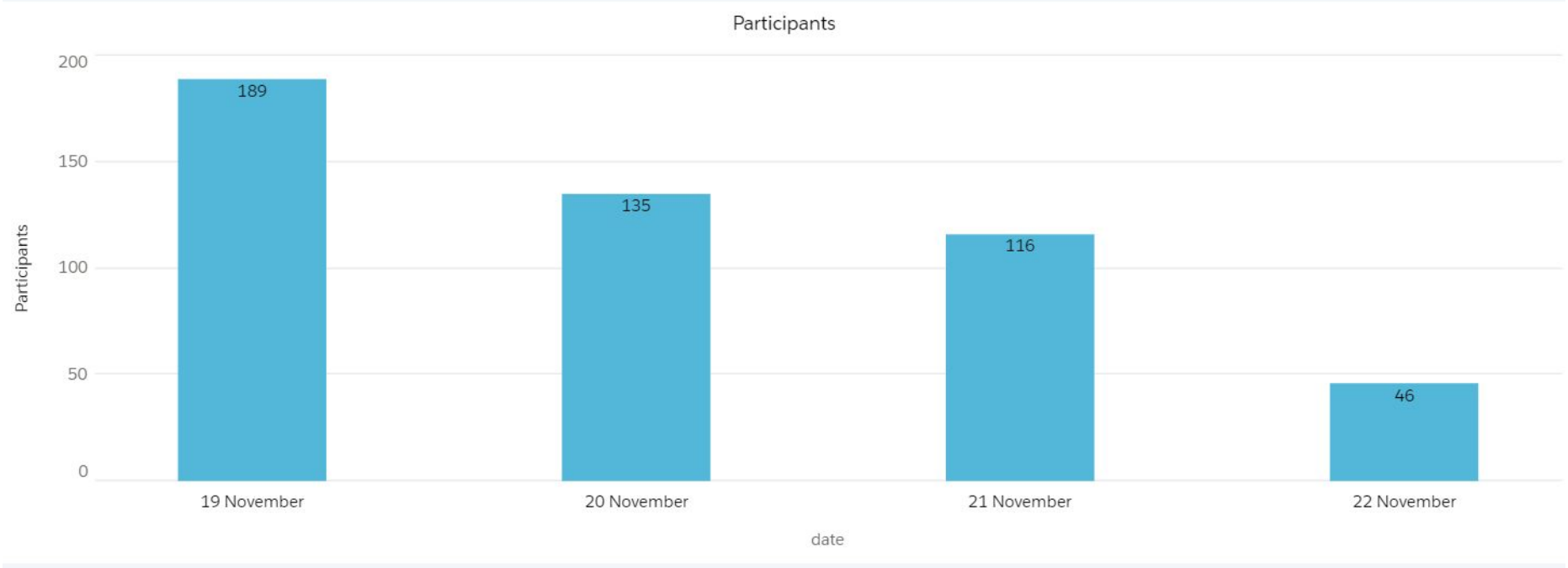
Scoreboard



Place	Team	Score
1	bpirih	19350
2	Cmsweet	18750
3	Richman	18750
4	b__bell	18450

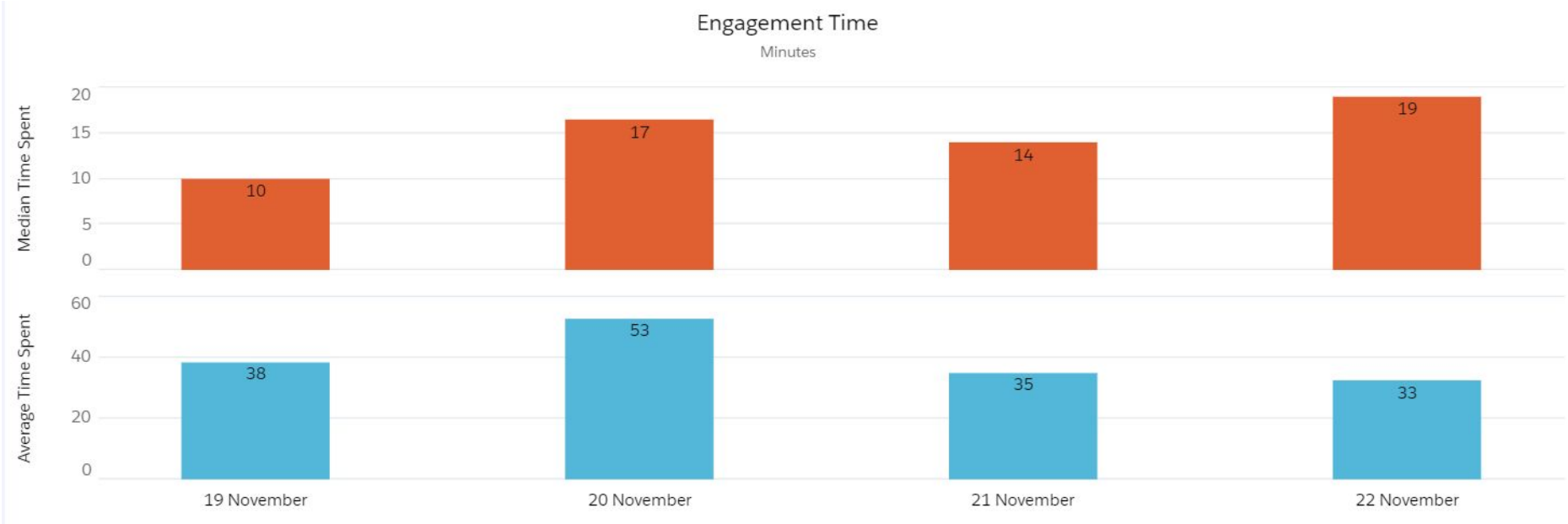
https://engineering.salesforce.com/play-games-learn-better-fc782757c884

Total Participants	486

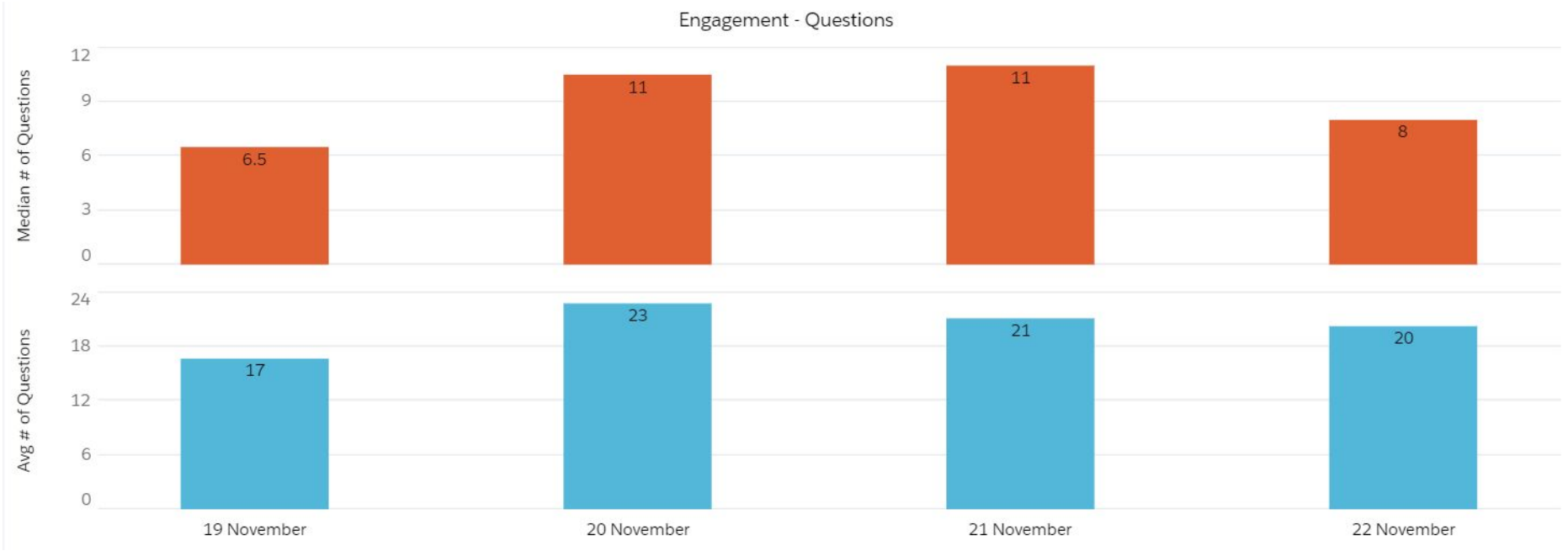


@jkuemerle

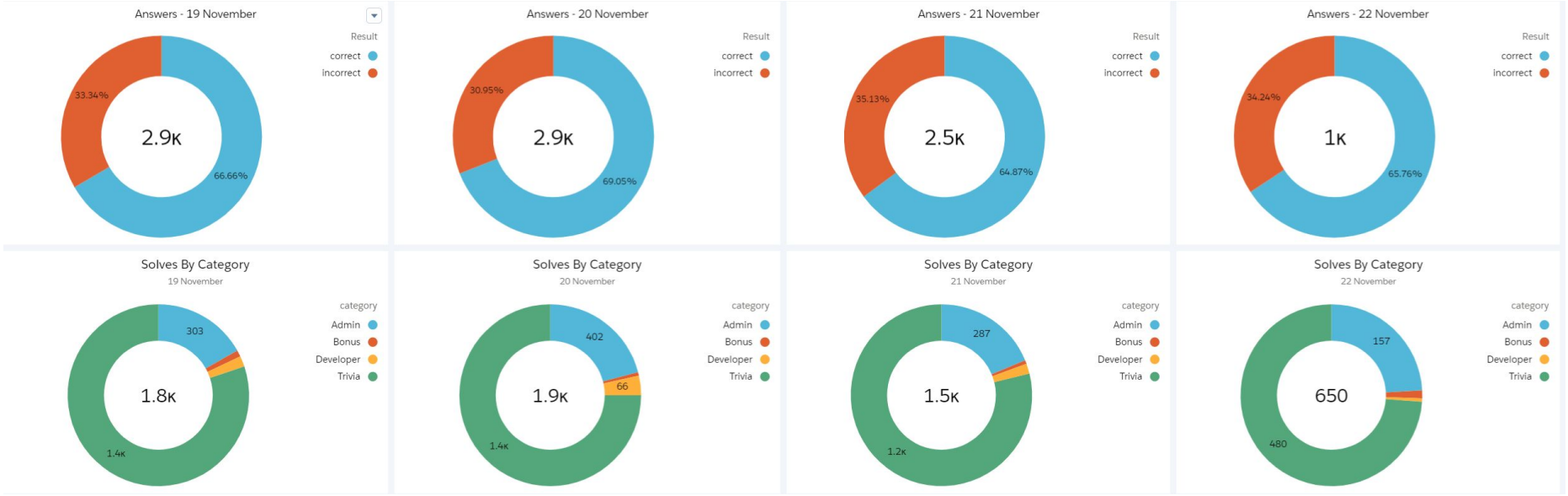
https://engineering.salesforce.com/play-games-learn-better-fc782757c884

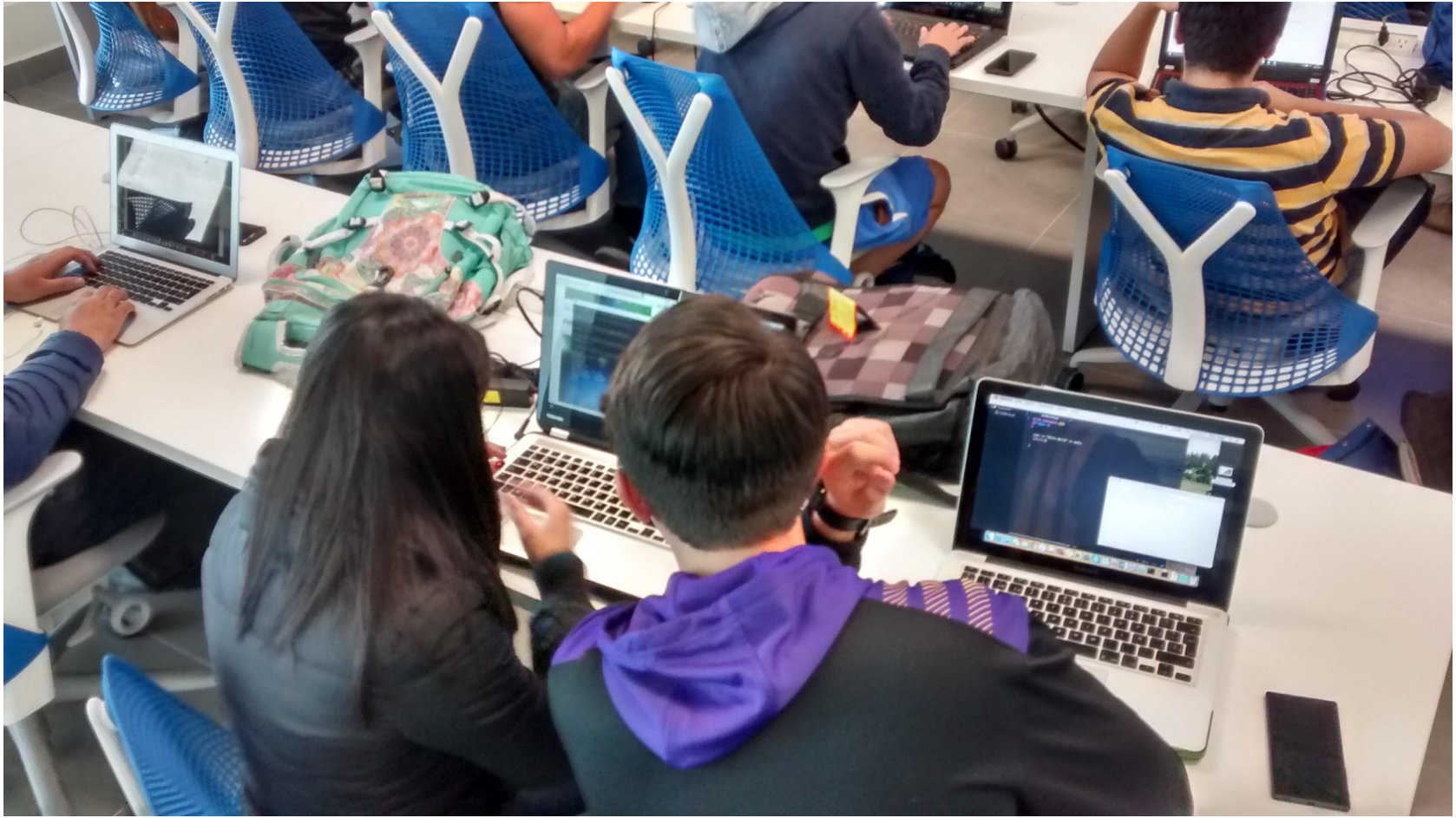


https://engineering.salesforce.com/play-games-learn-better-fc782757c884



https://engineering.salesforce.com/play-games-learn-better-fc782757c884





https://www.flickr.com/photos/35509232@N06/24271690249

https://www.flickr.com/photos/79673928@N08/10519784515

@jkuemerle

https://www.flickr.com/photos/78814955@N00/46868044302

@jkuemerle

- **Relevancy -** challenges should use the same technologies and platforms that the participants work in

- **Appropriateness** - challenges should cover vulnerability categories that are known to exist in the participants codebases

- **Interesting/Engaging** - challenges should draw the participants attention and encourage them to find solutions

- **Solvable** - challenges should have a clear and accurate solution

- **Reflective** - challenges should reinforce targeted concepts

https://www.flickr.com/photos/93416311@N00/2195946360

@jkuemerle

Red Flags - Avoid

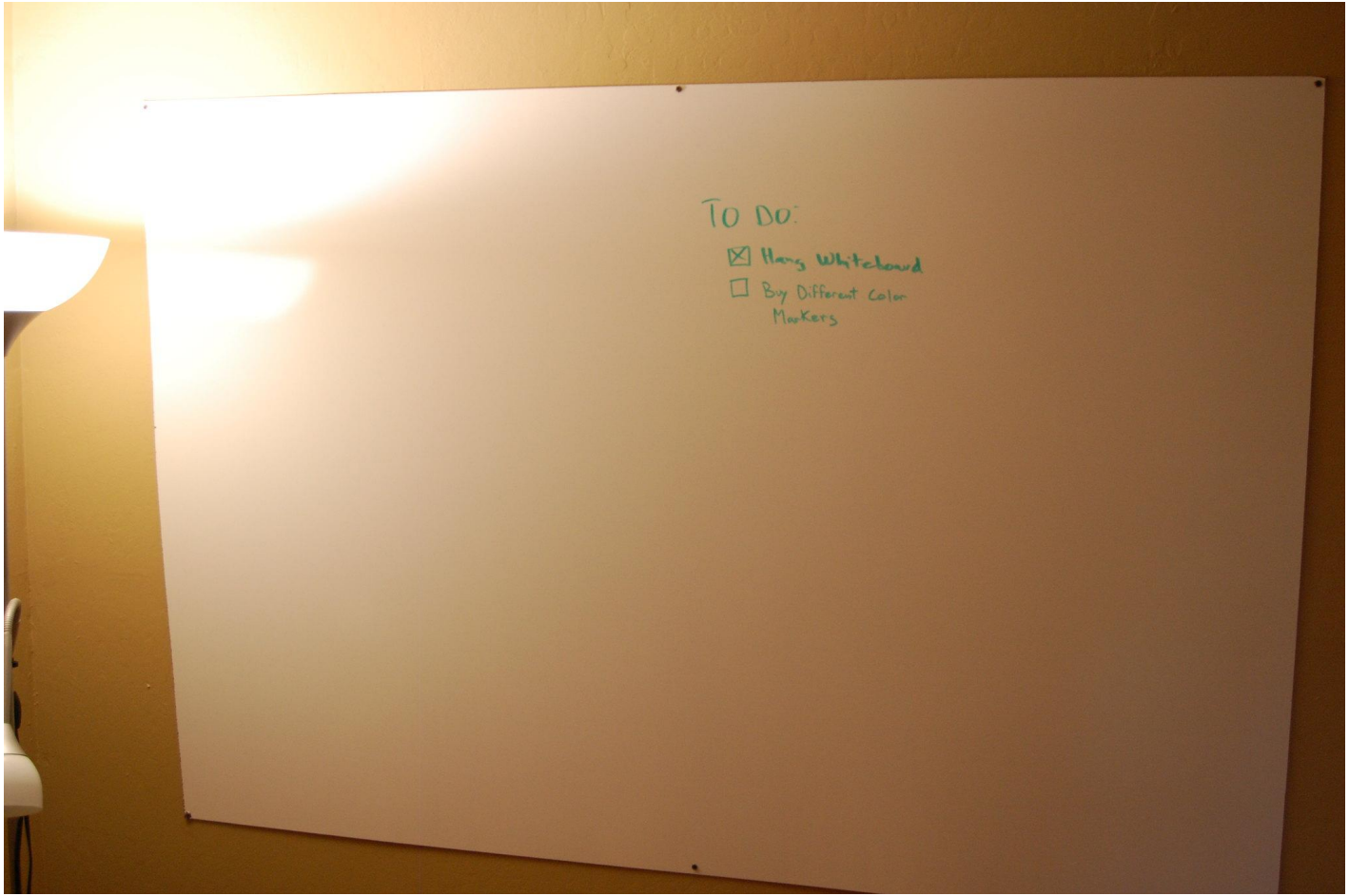
- **Excessive Obscurity** - solutions should be discoverable (with a reasonable amount of effort)

- **Non-Relevant** - work to solve challenges should not be far outside of the participants skill set and work requirements

- **Open Ended** - challenges should have enough guidance to allow the participant to find an agreed upon “good” solution

https://www.flickr.com/photos/21597369@N06/2091577071

@jkuemerle



https://www.flickr.com/photos/32184125@N00/4310830876

- **Relevancy -** challenges should use the same technologies and platforms that the participants work in
- **Appropriateness** - challenges should cover vulnerability categories that are known to exist in the participants codebases
- **Interesting/Engaging** - challenges should draw the participants attention and encourage them to find solutions
- **Solvable** - challenges should have a clear and accurate solution
- **Reflective** - challenges should reinforce targeted concepts

Red Flags - Avoid

- **Excessive Obscurity** - solutions should be discoverable (with a reasonable amount of effort)
- **Non-Relevant** - work to solve challenges should not be far outside of the participants skill set and work requirements
- **Open Ended** - challenges should be have enough guidance to allow the participant to find an agreed upon “good” solution

https://www.flickr.com/photos/95380334@N04/8704970501

https://github.com/salesforce/integrated_challenge

https://www.flickr.com/photos/50318388@N00/304687602

https://commons.wikimedia.org/wiki/File:Judges_hold_up_their_respective_scores.jpg

https://www.flickr.com/photos/144008357@N08/32943365784

https://commons.wikimedia.org/wiki/File:JBER_telephone_operators_connect_calls,_people_120124-A-ZY202-001.jp

https://www.flickr.com/photos/23299838@N08/3350934724

@jkuemerle

http://www.bertiesinn.com/beltsander_races/2017_beltsander_race.html

https://pixabay.com/photos/climbing-rock-climbing-overhang-2264698/

@jkuemerle

Confidential Document - Sens 100	Zero Stars 100	Login Admin 250	Weird Crypto 250
Bjoern's Favorite Pet - Broker 450	Forged Review 450	Login Amy 450	Login Jim 450
Payback Time 450	Product Tampering 450	Access Log - Sensitive Data E 700	Misplaced Signature File 700
Server-side XSS Protection 700	User Credentials 700	Change Bender's Password - E 1000	Email Leak - Sensitive Data E 1000
Extra Language - Broken Anti 1000	Frontend Typosquatting 1000	NoSQL Exfiltration 1000	Reset Bjoern's Password 1000
Two Factor Authentication 1000	Imaginary Challenge 1350	SSRF 1350	

https://pxhere.com/en/photo/1451207

https://www.flickr.com/photos/pheezy/3769080979/

@jkuemerle

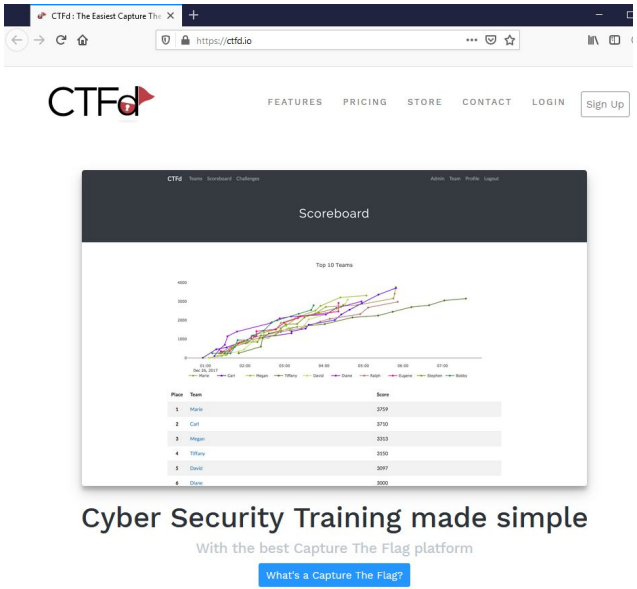
https://www.picpedia.org/highway-signs/i/integration.html

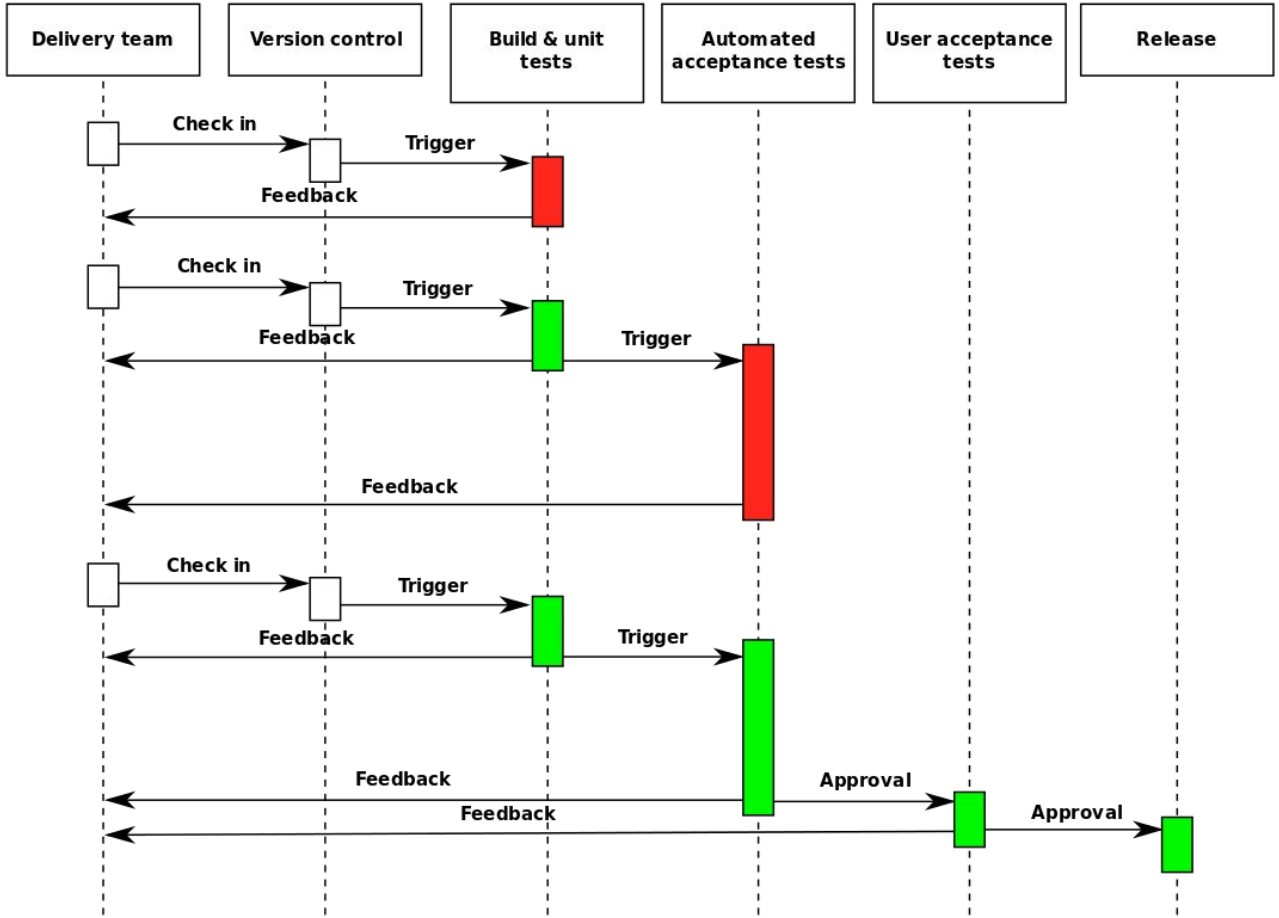
Platforms

Projects that can be used to host a CTF

- CTFd - Platform to host jeopardy style CTFs from ISISLab, NYU Tandon.
- FBCTF - Platform to host Capture the Flag competitions from Facebook.
- Haaukins- A Highly Accessible and Automated Virtualization Platform for Security Education.
- HackTheArch - CTF scoring platform.
- Mellivora - A CTF engine written in PHP.
- NightShade - A simple security CTF framework.
- OpenCTF - CTF in a box. Minimal setup required.
- PicoCTF - The platform used to run picoCTF. A great framework to host any CTF.
- PyChallFactory - Small framework to create/manage/package jeopardy CTF challenges.
- RootTheBox - A Game of Hackers (CTF Scoreboard & Game Manager).
- Scorebot - Platform for CTFs by Legitbs (Defcon).
- SecGen - Security Scenario Generator. Creates randomly vulnerable virtual machines.

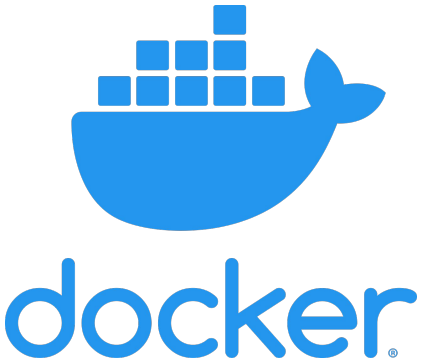
https://github.com/apsdehal/awesome-ctf





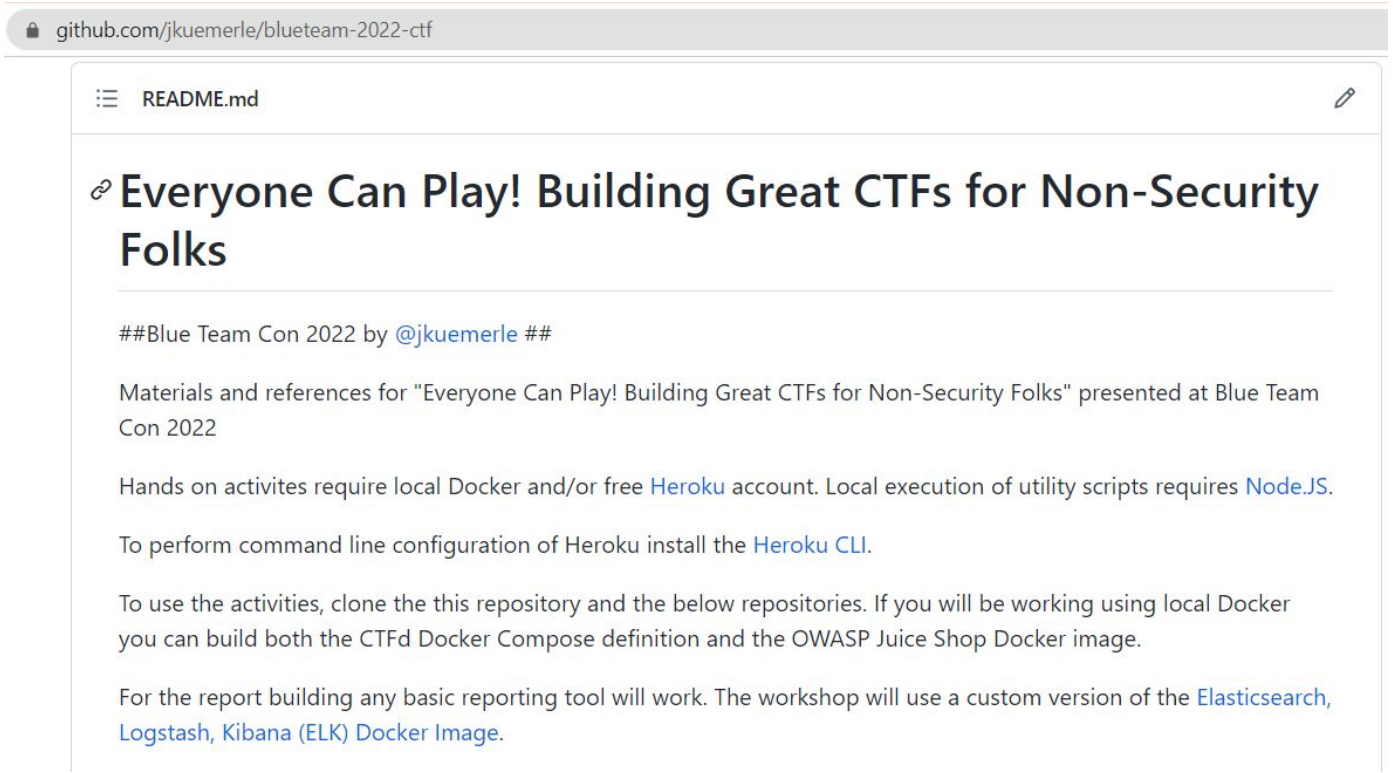
https://commons.wikimedia.org/wiki/File:Continuous_Delivery_process_diagram.svg

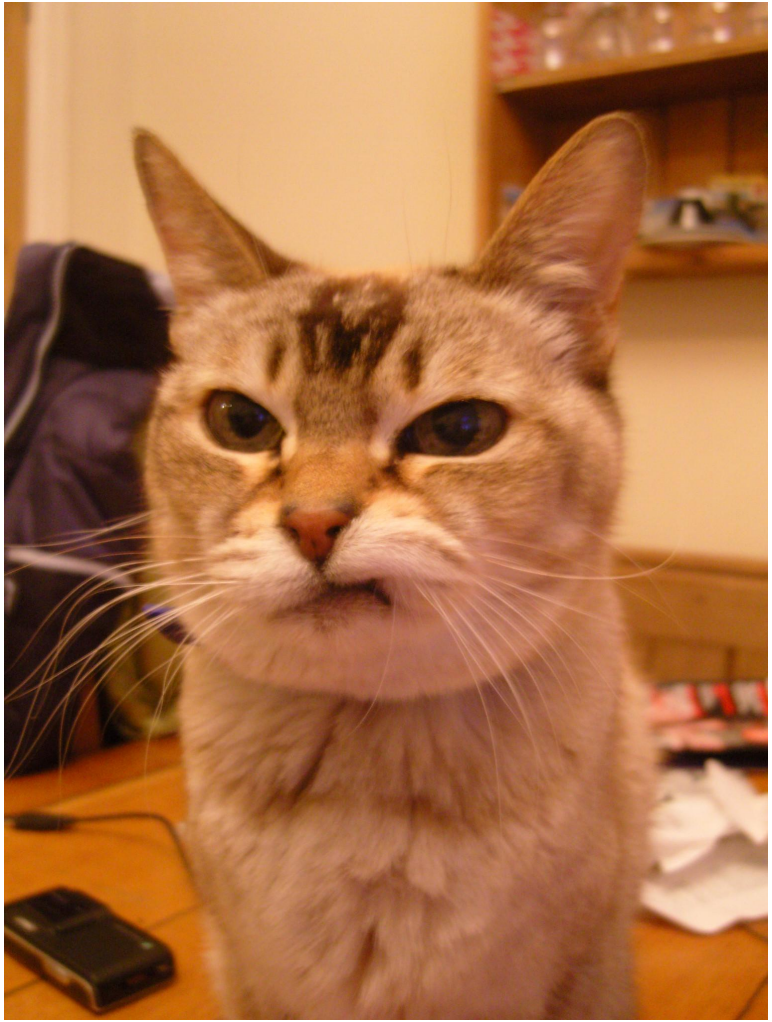
https://www.flickr.com/photos/mknowles/5358317992



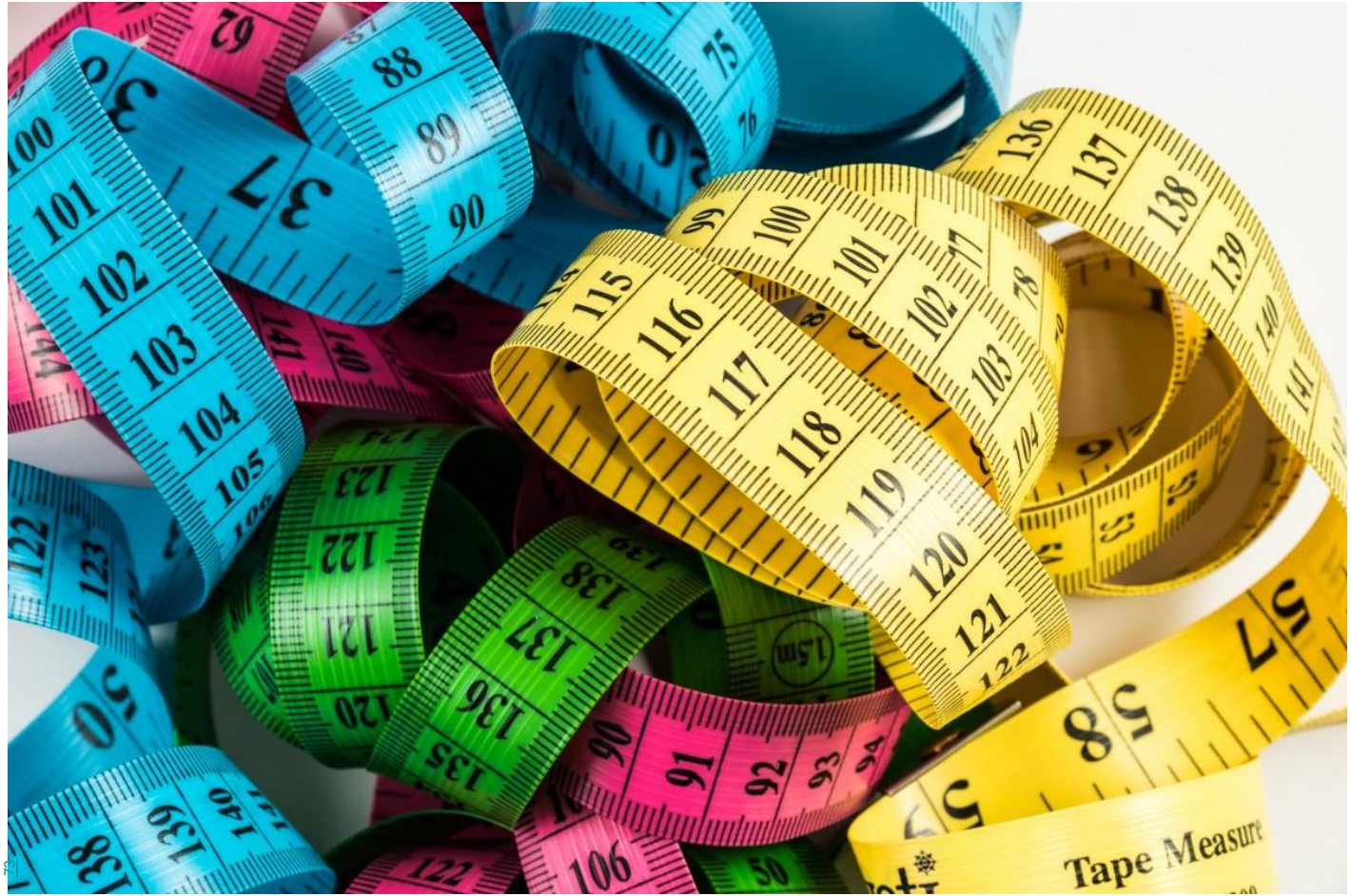
@jkuemerle

https://github.com/jkuemerle/blueteam-2022-ctf





https://www.flickr.com/photos/24886284@N00/3248529556

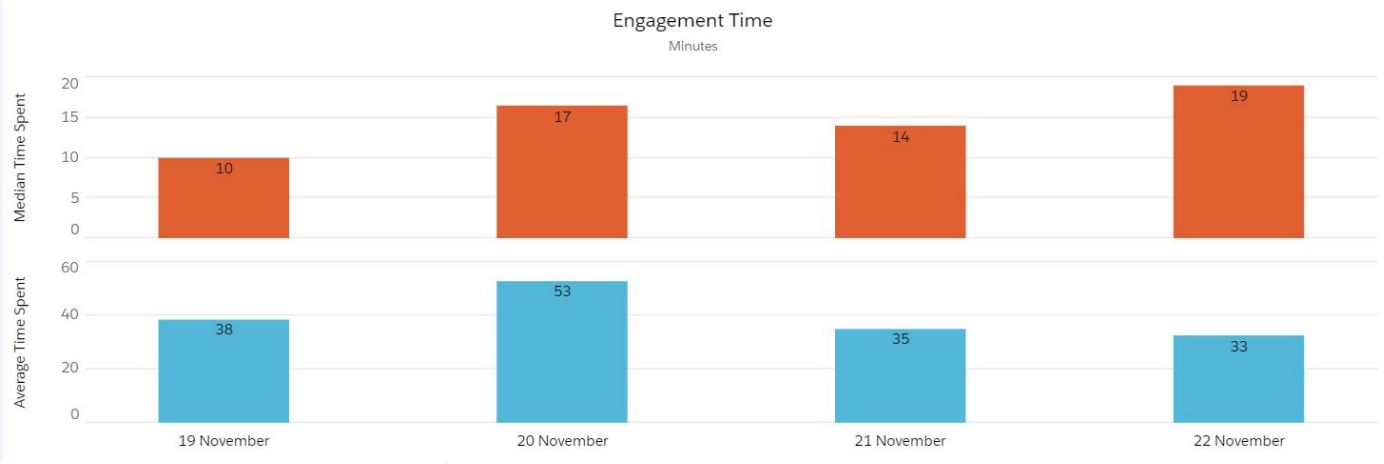


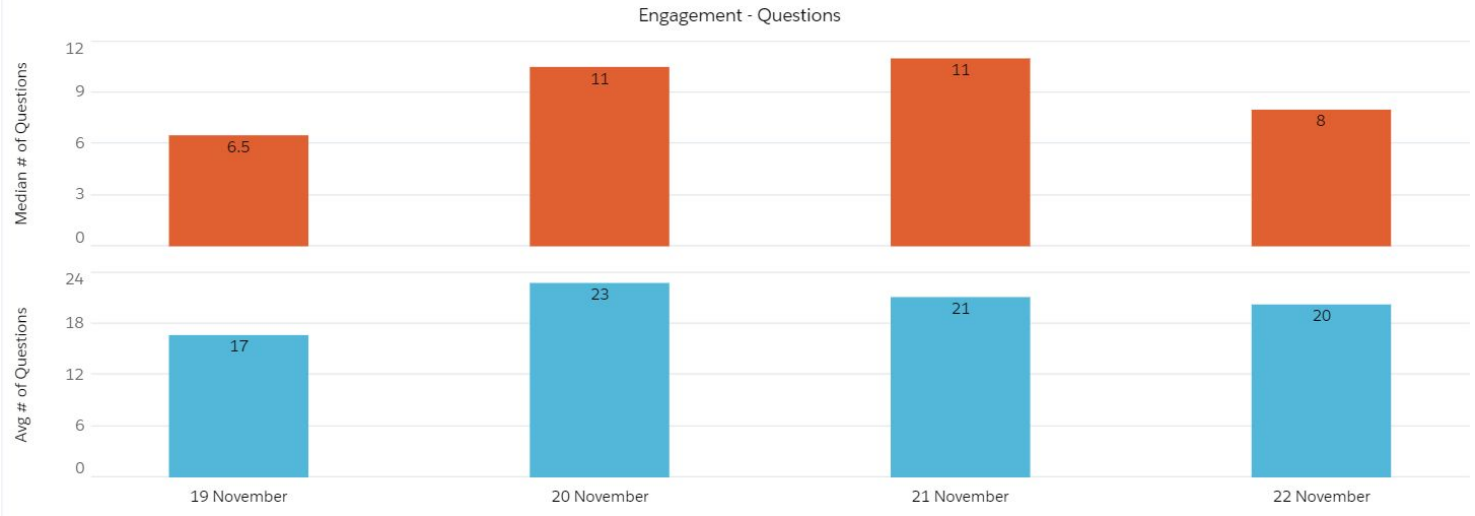
https://pxhere.com/en/photo/1437922

https://www.flickr.com/photos/andrewhurley/6254409229

https://www.flickr.com/photos/70267096@N00/8234628909

https://engineering.salesforce.com/play-games-learn-better-fc782757c884





Conclusion

- Why
- What
- How

- Next week you should:
  - Identify teams that will benefit from CTF style training
  - Identify SMEs to build a pilot CTF
- In the first three months following this presentation you should:
  - Have run a CTF and iterated on the design, challenges and goals
  - Run retrospectives of both CTF builders and CTF players
  - Gathered usage data into a repository
- Within six months you should:
  - Have an active, ongoing CTF based training program
  - Run regular retrospectives and incorporate feedback
  - Report KPIs and regularly survey program effectiveness

Resources

- https://github.com/salesforce/integrated_challenge
- https://github.com/apsdehal/awesome-ctf
- https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/Multimodal-Learning-Through-Media.pdf
- https://engineering.salesforce.com/capture-the-flag-secure-your-knowledge-37b43180e55a
- https://engineering.salesforce.com/play-games-learn-better-fc782757c884
- https://github.com/CTFd/CTFd
- https://github.com/jkuemerle/blueteam-2022-ctf

https://www.flickr.com/photos/88547796@N00/5716815256